CIS CentOS Linux 7 Benchmark

v4.0.0 - 12-22-2023

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This is the archive of the CIS CentOS Linux 7 Benchmark v4.0.0. CIS encourages you to migrate to a more recent, supported version of this technology.

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for CentOS Linux 7 systems running on x86_64 platforms.
This guide was developed and tested against CentOS Linux 7.9
The guidance within broadly assumes that operations are being performed as the `root` user, and executed under the default Bash version for the applicable distribution. Operations performed using `sudo` instead of the `root` user, or executed under another shell, may produce unexpected results, or fail to make the intended changes to the system. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify `root` users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.
The default prompt for the `root` user is `#`, and as such all sample commands will have `#` as an additional indication that it is to be executed as `root`.
To obtain the latest version of this guide, please visit http://workbench.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate CentOS Linux 7 on x86_64 platforms.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Server**
  Items in this profile intend to:
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

  This profile is intended for servers.
- **Level 2 - Server**
  This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:
  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers.
- **Level 1 - Workstation**
  Items in this profile intend to:
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

  This profile is intended for workstations.

- **Level 2 - Workstation**
  This profile extends the "Level 1 - Workstation" profile. Items in this profile exhibit one or more of the following characteristics:
  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for workstations.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

This benchmark is based upon previous Linux benchmarks published and would not be possible without the contributions provided over the history of all of these benchmarks. The CIS community thanks everyone who has contributed to the Linux benchmarks.

Contributor
Ron Colvin
Dave Billing
Dominic Pace
Koen Laevens
Mark Birch
Thomas Sjögren
James Trigg
Matthew Burket
Marcus Burghardt
Graham Eames
Robert McSulla
Chad Streck
Ryan Jaynes
Agustin Gonzalez
Tamas Tevesz
Cory Sherman
Simon John
Nym Coy

Editor
Jonathan Lewis Christopherson
Eric Pinnell
Justin Brown
Gokhan Lus

Recommendations

1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

1.1 Filesystem

The file system is generally a built-in layer used to handle the data management of the storage.

1.1.1 Configure Filesystem Kernel Modules

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

Note: This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment. For the current available file system modules on the system see `/usr/lib/modules/$(uname -r)/kernel/fs`

Start up scripts

Kernel modules loaded directly via `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. If modules are still being loaded after a reboot whilst having the correctly configured `blacklist` and `install` command, check for `insmod` entries in start up scripts such as `.bashrc`.

You may also want to check `/lib/modprobe.d/`. Please note that this directory should not be used for user defined module loading. Ensure that all such entries resides in `/etc/modprobe.d/*.conf` files.

Return values

Using `/bin/false` as the command in disabling a particular module serves two purposes; to convey the meaning of the entry to the user and cause a non-zero return value. The latter can be tested for in scripts. Please note that `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. The preferred way to load modules is with `modprobe`.

1.1.1.1 Ensure cramfs kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `cramfs` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="cramfs" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `cramfs` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install cramfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist cramfs` in the `/etc/modprobe.d/` directory
- Unload `cramfs` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist cramfs` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="cramfs" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.2 Ensure freevxfs kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `freevxfs` filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `freevxfs` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="freevxfs" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"
   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `freevxfs` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install freevxfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist freevxfs` in the `/etc/modprobe.d/` directory
- Unload `freevxfs` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist freevxfs` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="freevxfs" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.3 Ensure hfs kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `hfs` filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `hfs` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="hfs" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `hfs` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install hfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfs` in the `/etc/modprobe.d/` directory
- Unload `hfs` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist hfs` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="hfs" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.4 Ensure hfsplus kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `hfsplus` filesystem type is a hierarchical filesystem designed to replace `hfs` that allows you to mount Mac OS filesystems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `hfsplus` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="hfsplus" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `hfsplus` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install hfsplus /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfsplus` in the `/etc/modprobe.d/` directory
- Unload `hfsplus` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist hfsplus` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="hfsplus" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.5 Ensure jffs2 kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `jffs2` (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `jffs2` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="jffs2" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `jffs2` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install jffs2 /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist jffs2` in the `/etc/modprobe.d/` directory
- Unload `jffs2` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist jffs2` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="jffs2" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.6 Ensure squashfs kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `squashfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Impact:

As Snap packages utilizes `squashfs` as a compressed filesystem, disabling `squashfs` will cause Snap packages to fail.

`Snap` application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment.

Audit:

Run the following script to verify the `squashfs` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="squashfs" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Note: On operating systems where `squashfs` is pre-build into the kernel:

- This is considered an acceptable "passing" state
- The kernel **should not** be re-compiled to remove `squashfs`
- This audit will return as passing state with "module: "squashfs" doesn't exist in ..."

Remediation:

Run the following script to disable the `squashfs` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install squashfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory
- Unload `squashfs` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="squashfs" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.7 Ensure udf kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `udf` filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Impact:

Microsoft Azure requires the usage of `udf`.

`udf` **should not** be disabled on systems run on Microsoft Azure.

Audit:

Run the following script to verify the `udf` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="udf" # set module name
   l_mtype="fs" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `udf` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install udf /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist udf` in the `/etc/modprobe.d/` directory
- Unload `udf` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist udf` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="udf" # set module name
   l_mtype="fs" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0005	M1050

1.1.1.8 Ensure usb-storage kernel module is not available (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

USB storage provides a means to transfer and store files ensuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

Rationale:

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

Impact:

Disabling the `usb-storage` module will disable any usage of USB storage devices.

If requirements and local site policy allow the use of such devices, other solutions should be configured accordingly instead. One example of a commonly used solution is `USBGuard`.

Audit:

Run the following script to verify the `usb-storage` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="usb-storage" # set module name
   l_mtype="drivers" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `usb-storage` module:
-IF- the module is available in the running kernel:

- Create a file ending in `.conf` with `install usb-storage /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist usb-storage` in the `/etc/modprobe.d/` directory
- Unload `usb-storage` from the kernel

-IF- available in ANY installed kernel:

- Create a file ending in `.conf` with `blacklist usb-storage` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="usb-storage" # set module name
   l_mtype="drivers" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: SI-3

Additional Information:

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	13.7 Manage USB Devices If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1052, T1052.001, T1091, T1091.000, T1200, T1200.000	TA0001, TA0010	M1034

1.1.2 Configure Filesystem Partitions

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

Note:

- The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system
- **-IF-** you are repartitioning a system that has already been installed (This may require the system to be in single-user mode):
    - Mount the new partition to a temporary mountpoint e.g. `mount /dev/sda2 /mnt`
    - Copy data from the original partition to the new partition. e.g. `cp -a /var/tmp/* /mnt`
    - Verify that all data is present on the new partition. e.g. `ls -la /mnt`
    - Unmount the new partition. e.g. `umount /mnt`
    - Remove the data from the original directory that was in the old partition. e.g. `rm -Rf /var/tmp/*` Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted.
    - Mount the new partition to the desired mountpoint. e.g. `mount /dev/sda2 /var/tmp`
    - Update `/etc/fstab` with the new mountpoint. e.g. `/dev/sda2 /var/tmp xfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`

1.1.2.1 Configure /tmp

The `/tmp` directory is a world-writable directory used to store data used by the system and user applications for a short period of time. This data should have no expectation of surviving a reboot, as this directory is intended to be emptied after each reboot.

1.1.2.1.1 Ensure /tmp is a separate partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

-IF- an entry for `/tmp` exists in `/etc/fstab` it will take precedence over entries in systemd default unit file.

Note: In an environment where the main system is diskless and connected to iSCSI, entries in `/etc/fstab` may not take precedence.

`/tmp` can be configured to use `tmpfs`.

`tmpfs` puts everything into the kernel internal caches and grows and shrinks to accommodate the files it contains and is able to swap unneeded pages out to swap space. It has maximum size limits which can be adjusted on the fly via `mount -o remount`.

Since tmpfs lives completely in the page cache and on swap, all tmpfs pages will be shown as "Shmem" in `/proc/meminfo` and "Shared" in `free`. Notice that these counters also include shared memory. The most reliable way to get the count is using `df` and `du`.

tmpfs has three mount options for sizing:

- `size`: The limit of allocated bytes for this tmpfs instance. The default is half of your physical RAM without swap. If you oversize your tmpfs instances the machine will deadlock since the OOM handler will not be able to free that memory.
- `nr_blocks`: The same as size, but in blocks of PAGE_SIZE.
- `nr_inodes`: The maximum number of inodes for this instance. The default is half of the number of your physical RAM pages, or (on a machine with highmem) the number of lowmem RAM pages, whichever is the lower.

These parameters accept a suffix k, m or g and can be changed on remount. The size parameter also accepts a suffix % to limit this tmpfs instance to that percentage of your physical RAM. The default, when neither `size` nor `nr_blocks` is specified, is `size=50%`.

Rationale:

Making `/tmp` its own file system allows an administrator to set additional mount options such as the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard link would be broken, and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by either mounting `tmpfs` to `/tmp`, or creating a separate partition for `/tmp`.

Impact:

By design files saved to `/tmp` should have no expectation of surviving a reboot of the system. `tmpfs` is ram based and all files stored to `tmpfs` will be lost when the system is rebooted.

If files need to be persistent through a reboot, they should be saved to `/var/tmp` not `/tmp`.

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to `tmpfs` or a separate partition.

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a configuration where `/tmp` is not a separate file system it will essentially have the whole disk available, as the default installation only creates a single `/` partition. On the other hand, a RAM-based `/tmp` (as with `tmpfs`) will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily. Another alternative is to create a dedicated partition for `/tmp` from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than `tmpfs` which is RAM-based.

Audit:

Run the following command and verify the output shows that `/tmp` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt -nk /tmp
```

Example output:

```
/tmp   tmpfs  tmpfs  rw,nosuid,nodev,noexec
```

Remediation:

Create or update an entry for `/tmp` in `/etc/fstab`:
_ Example:_

```
tmpfs   /tmp    tmpfs     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp`

```
# mount -o remount,noexec,nodev,nosuid /tmp
```

- OR - if `/tmp` is not already mounted, run the following command to mount `/tmp`:

```
# mount /tmp
```

References:

1. https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
2. https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html
3. https://www.kernel.org/doc/Documentation/filesystems/tmpfs.txt
4. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.1.2 Ensure nodev option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/tmp`.

Audit:

- IF - a separate partition exists for `/tmp`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -kn /tmp | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/tmp` partition.
Example:

```
<device> /tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

```
# mount -o remount /tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/tmp`.

Audit:

- IF - a separate partition exists for `/tmp`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -kn /tmp | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/tmp` partition.
Example:

```
<device> /tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

```
# mount -o remount /tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/tmp`.

Impact:

Setting the `noexec` option on `/tmp` may prevent installation and/or updating of some 3rd party software.

Audit:

- IF - a separate partition exists for `/tmp`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# findmnt -kn /tmp | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition.
Example:

```
<device> /tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

```
# mount -o remount /tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.2.2 Configure /dev/shm

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC)

1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC).

Rationale:

Making `/dev/shm` its own file system allows an administrator to set additional mount options such as the `noexec` option on the mount, making `/dev/shm` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by mounting `tmpfs` to `/dev/shm`.

Impact:

Since the `/dev/shm` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.

`/dev/shm` utilizing `tmpfs` can be resized using the `size={size}` parameter in the relevant entry in `/etc/fstab`.

Audit:

-IF- `/dev/shm` is to be used on the system, run the following command and verify the output shows that `/dev/shm` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt -kn /dev/shm
```

Example output:

```
/dev/shm   tmpfs   tmpfs   rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For specific configuration requirements of the `/dev/shm` mount for your environment, modify `/etc/fstab`.
Example:

```
tmpfs   /dev/shm        tmpfs
defaults,rw,nosuid,nodev,noexec,relatime,size=2G  0 0
```

References:

1. https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/
2. https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html
3. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.2.2 Ensure nodev option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/dev/shm` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in `/dev/shm` partitions.

Audit:

- IF - a separate partition exists for `/dev/shm`, verify that the `nodev` option is set.

```
# findmnt -kn /dev/shm | grep -v 'nodev'

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/dev/shm`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.
Example:

```
tmpfs /dev/shm    tmpfs     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/dev/shm` with the configured options:

```
# mount -o remount /dev/shm
```

Note: It is recommended to use `tmpfs` as the device/filesystem type as `/dev/shm` is used as shared memory space by applications.

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.2.2.3 Ensure nosuid option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

- IF - a separate partition exists for `/dev/shm`, verify that the `nosuid` option is set.

```
# findmnt -kn /dev/shm | grep -v 'nosuid'

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/dev/shm`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.
Example:

```
tmpfs /dev/shm    tmpfs     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/dev/shm` with the configured options:

```
# mount -o remount /dev/shm
```

Note: It is recommended to use `tmpfs` as the device/filesystem type as `/dev/shm` is used as shared memory space by applications.

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1038

1.1.2.2.4 Ensure noexec option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Audit:

- IF - a separate partition exists for `/dev/shm`, verify that the `noexec` option is set.

```
# findmnt -kn /dev/shm | grep -v 'noexec'

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/dev/shm`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition.
Example:

```
tmpfs /dev/shm    tmpfs     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/dev/shm` with the configured options:

```
# mount -o remount /dev/shm
```

Note: It is recommended to use `tmpfs` as the device/filesystem type as `/dev/shm` is used as shared memory space by applications.

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.2.3 Configure /home

Please note that home directories could be mounted anywhere and are not necessarily restricted to `/home`, nor restricted to a single location, nor is the name restricted in any way.

Checks can be made by looking in `/etc/passwd`, looking over the mounted file systems with `mount` or querying the relevant database with `getent`.

1.1.2.3.1 Ensure separate partition exists for /home (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/home` directory is used to support disk storage needs of local users.

Rationale:

The reasoning for mounting `/home` on a separate partition is as follows.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/home` directory contains user generated data, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/home` and impact all local users.

Fine grained control over the mount

Configuring `/home` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system. In the case of `/home` options such as `usrquota/grpquota` may be considered to limit the impact that users can have on each other with regards to disk resource exhaustion. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of user data

As `/home` contains user data, care should be taken to ensure the security and integrity of the data and mount point.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/home` is mounted:

```
# findmnt -nk /home

/home   /dev/sdb  ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/home`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

When modifying `/home` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1038

1.1.2.3.2 Ensure nodev option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/home` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/home`.

Audit:

- IF - a separate partition exists for `/home`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -nk /home | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/home`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/home` partition.
Example:

```
<device> /home    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

```
# mount -o remount /home
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1038

1.1.2.3.3 Ensure nosuid option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/home` filesystem is only intended for user file storage, set this option to ensure that users cannot create `setuid` files in `/home`.

Audit:

- IF - a separate partition exists for `/home`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -nk /home | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/home`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/home` partition.
Example:

```
<device> /home    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

```
# mount -o remount /home
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.4 Configure /var

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

1.1.2.4.1 Ensure separate partition exists for /var (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

Rationale:

The reasoning for mounting `/var` on a separate partition is as follows.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var` and cause unintended behavior across the system as the disk is full. See `man auditd.conf` for details.

Fine grained control over the mount

Configuring `/var` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection from exploitation

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var` is mounted.
Example:

```
# findmnt -nk /var

/var  /dev/sdb  ext4   rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

When modifying `/var` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0006	M1022

1.1.2.4.2 Ensure nodev option set on /var partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var`.

Audit:

- IF - a separate partition exists for `/var`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -nk /var | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var` partition.
Example:

```
<device> /var    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

```
# mount -o remount /var
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.2.4.3 Ensure nosuid option set on /var partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var`.

Audit:

- IF - a separate partition exists for `/var`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -nk /var | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var` partition.
Example:

```
<device> /var    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

```
# mount -o remount /var
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.5 Configure /var/tmp

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary files residing in `/var/tmp` are to be preserved between reboots.

1.1.2.5.1 Ensure separate partition exists for /var/tmp (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary files residing in `/var/tmp` are to be preserved between reboots.

Rationale:

The reasoning for mounting `/var/tmp` on a separate partition is as follows.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/tmp` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/tmp` and cause potential disruption to daemons as the disk is full.

Fine grained control over the mount

Configuring `/var/tmp` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection from exploitation

An example of exploiting `/var/tmp` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/tmp` is mounted.
Example:

```
# findmnt -nk /var/tmp

/var/tmp   /dev/sdb ext4   rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

When modifying `/var/tmp` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.5.2 Ensure nodev option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/tmp`.

Audit:

- IF - a separate partition exists for `/var/tmp`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -nk /var/tmp | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/tmp`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/tmp` partition.
Example:

```
<device> /var/tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.5.3 Ensure nosuid option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/var/tmp`.

Audit:

- IF - a separate partition exists for `/var/tmp`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -nk /var/tmp | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/tmp`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/tmp` partition.
Example:

```
<device> /var/tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.5.4 Ensure noexec option set on /var/tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/var/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/var/tmp`.

Audit:

- IF - a separate partition exists for `/var/tmp`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# findmnt -nk /var/tmp | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/tmp`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/tmp` partition.
Example:

```
<device> /var/tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.2.6 Configure /var/log

The `/var/log` directory is used by system services to store log data.

1.1.2.6.1 Ensure separate partition exists for /var/log (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/var/log` directory is used by system services to store log data.

Rationale:

The reasoning for mounting `/var/log` on a separate partition is as follows.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/log` directory contains log files which can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole.

Fine grained control over the mount

Configuring `/var/log` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of log data

As `/var/log` contains log files, care should be taken to ensure the security and integrity of the data and mount point.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/log` is mounted:

```
# findmnt -nk /var/log

/var/log /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log` .
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

When modifying `/var/log` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.6.2 Ensure nodev option set on /var/log partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var/log` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/log`.

Audit:

- IF - a separate partition exists for `/var/log`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -nk /var/log | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log` partition.
Example:

```
<device> /var/log    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1038

1.1.2.6.3 Ensure nosuid option set on /var/log partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot create `setuid` files in `/var/log`.

Audit:

- IF - a separate partition exists for `/var/log`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -nk /var/log | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log` partition.
Example:

```
<device> /var/log    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.6.4 Ensure noexec option set on /var/log partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot run executable binaries from `/var/log`.

Audit:

- IF - a separate partition exists for `/var/log`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# findmnt -nk /var/log | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/log` partition.
Example:

```
<device> /var/log    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.1.2.7 Configure /var/log/audit

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

1.1.2.7.1 Ensure separate partition exists for /var/log/audit (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

Rationale:

The reasoning for mounting `/var/log/audit` on a separate partition is as follows.

Protection from resource exhaustion

The default installation only creates a single `/` partition. Since the `/var/log/audit` directory contains the `audit.log` file which can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/log/audit` and cause `auditd` to trigger it's `space_left_action` as the disk is full. See `man auditd.conf` for details.

Fine grained control over the mount

Configuring `/var/log/audit` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

Protection of audit data

As `/var/log/audit` contains audit logs, care should be taken to ensure the security and integrity of the data and mount point.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Audit:

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# findmnt -nk /var/log/audit

/var/log/audit /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

When modifying `/var/log/audit` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

1.1.2.7.2 Ensure nodev option set on /var/log/audit partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var/log/audit` filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in `/var/log/audit`.

Audit:

- IF - a separate partition exists for `/var/log/audit`, verify that the `nodev` option is set.
Run the following command to verify that the `nodev` mount option is set.
Example:

```
# findmnt -nk /var/log/audit | grep -v nodev

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log/audit`.
Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log/audit` partition.
Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1200, T1200.000	TA0005	M1022

1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var/log/audit` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var/log/audit`.

Audit:

- IF - a separate partition exists for `/var/log/audit`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# findmnt -nk /var/log/audit | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log/audit`.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log/audit` partition.
Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0005	M1022

1.1.2.7.4 Ensure noexec option set on /var/log/audit partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/var/log/audit` filesystem is only intended for audit logs, set this option to ensure that users cannot run executable binaries from `/var/log/audit`.

Audit:

- IF - a separate partition exists for `/var/log/audit`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# findmnt -nk /var/log/audit | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/var/log/audit`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/log/audit` partition.
Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0005	M1022

1.2 Configure Software and Patch Management

Fedora 19/CentOS 7 stream derived Linux distributions use `yum` to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Organizations may prefer to test patches against their environment on a non-production system before rolling out to production.

Outdated software is vulnerable to cyber criminals and hackers. Software updates help reduce the risk to your organization. The release of software update notes often reveal the patched exploitable entry points to the public. Public knowledge of these exploits cans your organization more vulnerable to malicious actors attempting to gain entry to your system's data.

Software updates often offer new and improved features and speed enhancements

For the purpose of this benchmark, the requirement is to ensure that a patch management process is defined and maintained, the specifics of which are left to the organization.

1.2.1 Ensure GPG keys are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The RPM Package Manager implements GPG key signing to verify package integrity during and after installation.

Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system. To this end, verify that GPG keys are configured correctly for your system.

Audit:

List all GPG key URLs
Each repository should have a `gpgkey` with a URL pointing to the location of the GPG key, either local or remote.

```
# grep -r gpgkey /etc/yum.repos.d/*
```

List installed GPG keys
Run the following command to list the currently installed keys. These are the active keys used for verification and installation of RPMs. The packages are fake, they are generated on the fly by `yum` or `rpm` during the import of keys from the URL specified in the repository configuration.

```
#!/usr/bin/env bash

{
   for RPM_PACKAGE in $(rpm -q gpg-pubkey); do
      echo "RPM: ${RPM_PACKAGE}"
      RPM_SUMMARY=$(rpm -q --queryformat "%{SUMMARY}" "${RPM_PACKAGE}")
      RPM_PACKAGER=$(rpm -q --queryformat "%{PACKAGER}" "${RPM_PACKAGE}")
      RPM_DATE=$(date +%Y-%m-%d -d "1970-1-1+$((0x$(rpm -q --queryformat
"%{RELEASE}" "${RPM_PACKAGE}") ))sec")
      RPM_KEY_ID=$(rpm -q --queryformat "%{VERSION}" "${RPM_PACKAGE}")
      echo -e "Packager: ${RPM_PACKAGER}\nSummary: ${RPM_SUMMARY}\nCreation
date: ${RPM_DATE}\nKey ID: ${RPM_KEY_ID}"
   done
}
```

Example Output:

```
RPM: gpg-pubkey-f4a80eb5-53a7ff4b
Packager: CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>
Summary: gpg(CentOS-7 Key (CentOS 7 Official Signing Key)
<security@centos.org>)
Creation date: 2014-06-23
Key ID: f4a80eb5
```

The format of the package (`gpg-pubkey-f4a80eb5-53a7ff4b`) is important to understand for verification. Using the above example, it consists of three parts:

1. The general prefix name for all imported GPG keys: `gpg-pubkey-`
2. The version, which is the GPG key ID: `f4a80eb5`
3. The release is the date of the key in UNIX timestamp in hexadecimal: `53a7ff4b`

With both the date and the GPG key ID, check the relevant repositories public key page to confirm that the keys are indeed correct.

Query locally available GPG keys

Repositories that store their respective GPG keys on disk should do so in `/etc/pki/rpm-gpg/`. These keys are available for immediate import either when `yum` is asked to install a relevant package from the repository or when an administrator imports the key directly with the `rpm --import` command.

To find where these keys come from run:

```
# for PACKAGE in $(find /etc/pki/rpm-gpg/ -type f -exec rpm -qf {} \; | sort
-u); do rpm -q --queryformat "%{NAME}-%{VERSION} %{PACKAGER} %{SUMMARY}\\n"
"${PACKAGE}"; done
```

Remediation:

Update your package manager GPG keys in accordance with site policy.

References:

1. NIST SP 800-53 Rev. 5: SI-2

Additional Information:

Fedora public keys: https://getfedora.org/security/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1195, T1195.001	TA0001	M1051

1.2.2 Ensure gpgcheck is globally activated (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `gpgcheck` option, found in the main section of the `/etc/yum.conf` and individual `/etc/yum.repos.d/*` files, determines if an RPM package's signature is checked prior to its installation.

Rationale:

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

Audit:

Global configuration. Run the following command and verify that `gpgcheck` is set to `1`:

```
# grep -P -- '^\h*gpgcheck\b' /etc/yum.conf

gpgcheck=1
```

Configuration in `/etc/yum.repos.d/` takes precedence over the global configuration. Run the following command and verify that there are no instances of entries starting with `gpgcheck` returned set to `0`. Nor should there be any invalid (non-boolean) values. When `yum` encounters such invalid entries they are ignored and the global configuration is applied.

```
# grep -Prs -- '^\h*gpgcheck\h*=\h*(0|[2-9]|[1-9][0-9]+|[a-zA-Z_]+)\b'
/etc/yum.repos.d/
```

Remediation:

Edit `/etc/yum.conf` and set `gpgcheck=1` in the `[main]` section.
Example:

```
# sed -i 's/^gpgcheck\s*=\s*.*/gpgcheck=1/' /etc/yum.conf
```

Edit any failing files in `/etc/yum.repos.d/*` and set all instances starting with `gpgcheck` to `1`.
Example:

```
# find /etc/yum.repos.d/ -name "*.repo" -exec echo "Checking:" {} \; -exec
sed -ri 's/^gpgcheck\s*=\s*.*/gpgcheck=1/' {} \;
```

References:

1. NIST SP 800-53 Rev. 5: SI-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1195, T1195.001	TA0005	

1.2.3 Ensure repo_gpgcheck is globally activated (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `repo_gpgcheck` option, found in the main section of the `/etc/yum.conf` and individual `/etc/yum.repos.d/*` files, will perform a GPG signature check on the repodata.

Rationale:

It is important to ensure that the repository data signature is always checked prior to installation to ensure that the software is not tampered with in any way.

Impact:

Not all repositories, notably RedHat, support `repo_gpgcheck`. Take care to set this value to false (default) for particular repositories that do not support it. If enabled on repositories that do not support `repo_gpgcheck` installation of packages will fail.

Research is required by the user to determine which repositories is configured on the local system and, from that list, which support `repo_gpgcheck`.

Audit:

Global configuration
Run the following command:

```
grep ^repo_gpgcheck /etc/yum.conf
```

Verify that `repo_gpgcheck` is set to `1`
Per repository configuration
Configuration in `/etc/yum.repos.d/` takes precedence over the global configuration.
As an example, to list all the configured repositories, excluding "fedoraproject.org", that specifically disables `repo_gpgcheck`, run the following script:

```
#!/usr/bin/env bash

{
   REPO_URL="fedoraproject.org"
   for repo in $(grep -l "repo_gpgcheck=0" /etc/yum.repos.d/* ); do
      if ! grep "${REPO_URL}" "${repo}" &>/dev/null; then
         echo "${repo}"
      fi
   done
}
```

Per the research that was done on which repositories does not support `repo_gpgcheck`, change the `REPO_URL` variable and run the test.

Remediation:

Global configuration
Edit `/etc/yum.conf` and set `repo_gpgcheck=1` in the `[main]` section.
Example:

```
[main]
repo_gpgcheck=1
```

Per repository configuration
First check that the particular repository support GPG checking on the repodata.
Edit any failing files in `/etc/yum.repos.d/*` and set all instances starting with `repo_gpgcheck` to `1`.

References:

1. NIST SP 800-53 Rev. 5: SI-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1195, T1195.001	TA0005	

1.2.4 Ensure package manager repositories are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Systems need to have the respective package manager repositories configured to ensure that the system is able to receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured, important patches may not be identified or a rogue repository could introduce compromised software.

Audit:

Run the following command to verify repositories are configured correctly. The output may vary depending on which repositories are currently configured on the system.
Example:

```
# yum repolist
```

For the repositories in use, inspect the configuration file to ensure all settings are correctly applied according to site policy.
Example:
Depending on the distribution being used the repo file name might differ.

```
cat /etc/yum.repos.d/*.repo
```

Remediation:

Configure your package manager repositories according to site policy.

References:

1. NIST SP 800-53 Rev. 5: SI-2

Additional Information:

For further information about Fedora repositories see: https://docs.fedoraproject.org/en-US/quick-docs/repositories/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1195, T1195.001	TA0001	M1051

1.2.5 Ensure updates, patches, and additional security software are installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Rationale:

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Audit:

Run the following command and verify there are no updates or patches to install:

```
# yum check-update
```

Check to make sure no system reboot is required

```
needs-restarting -r
```

Remediation:

Use your package manager to update all packages on the system according to site policy.
The following command will install all available updates:

```
# yum update
```

Once the update process is complete, verify if reboot is required to load changes.

```
needs-restarting -r
```

References:

1. NIST SP 800-53 Rev. 5: SI-2

Additional Information:

Site policy may mandate a testing period before install onto production systems for available updates.

```
# yum check-update
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1211, T1211.000	TA0004, TA0008	M1051

1.3 Configure Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

Note:

- In Fedora 28 based distributions, the kernel command-line parameters for systems using the GRUB2 bootloader were defined in the `kernelopts` environment variable. This variable was stored in the `/boot/grub2/grubenv` file for each kernel boot entry. However, storing the kernel command-line parameters using `kernelopts` was not robust. Therefore, the `kernelopts` has been removed and the kernel command-line parameters are now stored in the Boot Loader Specification (BLS) snippet, instead of in the `/boot/loader/entries/<KERNEL_BOOT_ENTRY>.conf` file.
- Boot loader configuration files are unified across CPU architectures
    - Configuration files for the GRUB boot loader are now stored in the `/boot/grub2/` directory on all supported CPU architectures. The `/boot/efi/EFI/redhat/grub.cfg` file, which GRUB previously used as the main configuration file on UEFI systems, now simply loads the `/boot/grub2/grub.cfg` file.
    - This change simplifies the layout of the GRUB configuration file, improves user experience, and provides the following notable benefits:
        - You can boot the same installation with either EFI or legacy BIOS.
        - You can use the same documentation and commands for all architectures.
        - GRUB configuration tools are more robust, because they no longer rely on symbolic links and they do not have to handle platform-specific cases.
        - The usage of the GRUB configuration files is aligned with images generated by CoreOS Assembler (COSA) and OSBuild.
        - The usage of the GRUB configuration files is aligned with other Linux distributions.
        - Fedora 28 based distributions no longer boot on 32-bit UEFI
- Support for the 32-bit UEFI firmware was removed from the GRUB and shim boot loaders. As a consequence, Fedora 28 based distributions require a 64-bit UEFI, and can no longer boot on 64-bit systems that use a 32-bit UEFI.
    - The following packages have been removed as part of this change:
    - `grub2-efi-ia32`
    - `grub2-efi-ia32-cdboot`
    - `grub2-efi-ia32-modules`
    - `shim-ia32`

Reference: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/considerations_in_adopting_rhel_8/index#kernel_considerations-in-adopting-RHEL-8

1.3.1 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters.

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing `e` or access the GRUB 2 command line by pressing `c`

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

Audit:

Run the following script to verify the bootloader password has been set:

```
#!/usr/bin/env bash

{
   l_grub_password_file="$(find /boot -type f -name 'user.cfg' ! -empty)"
   if [ -f "$l_grub_password_file" ]; then
      awk -F. '/^\s*GRUB2_PASSWORD=\S+/ {print $1"."$2"."$3}'
"$l_grub_password_file"
   fi
}
```

Output should be similar to:

```
GRUB2_PASSWORD=grub.pbkdf2.sha512
```

Note: Requires version 7.2 or later

Remediation:

Create an encrypted password with `grub2-setpassword`:

```
# grub2-setpassword

Enter password: <password>
Confirm password: <password>
```

Note: Requires version 7.2 or later

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

This recommendation is designed around the grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

`grub2-setpassword` outputs the `user.cfg` file which contains the hashed GRUB bootloader password. This utility only supports configurations where there is a single root user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0003	M1046

1.3.2 Ensure permissions on bootloader config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub files contain information on boot settings and passwords for unlocking boot options.

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Audit:

Run the following script to verify grub configuration files:

- For systems using UEFI (Files located in `/boot/efi/EFI/*`):
  - Mode is `0700` or more restrictive
- For systems using BIOS (Files located in `/boot/grub2/*`):
  - Mode is `0600` or more restrictive
- Owner is the user `root`
- Group owner is group `root`

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   file_mug_chk()
   {
      l_out="" l_out2=""
      [[ "$(dirname "$l_file")" =~ ^\/boot\/efi\/EFI ]] && l_pmask="0077" ||
l_pmask="0177"
      l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
      if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
         l_out2="$l_out2\n   - Is mode \"$l_mode\" and should be mode:
\"$l_maxperm\" or more restrictive"
      else
         l_out="$l_out\n   - Is correctly mode: \"$l_mode\" which is mode:
\"$l_maxperm\" or more restrictive"
      fi
      if [ "$l_user" = "root" ]; then
         l_out="$l_out\n   - Is correctly owned by user: \"$l_user\""
      else
         l_out2="$l_out2\n   - Is owned by user: \"$l_user\" and should be
owned by user: \"root\""
      fi
      if [ "$l_group" = "root" ]; then
         l_out="$l_out\n   - Is correctly group-owned by group: \"$l_user\""
      else
         l_out2="$l_out2\n   - Is group-owned by group: \"$l_user\" and
should be group-owned by group: \"root\""
      fi
      [ -n "$l_out" ] && l_output="$l_output\n  - File: \"$l_file\"$l_out\n"
      [ -n "$l_out2" ] && l_output2="$l_output2\n  - File:
\"$l_file\"$l_out2\n"
   }
   while IFS= read -r -d $'\0' l_gfile; do
      while read -r l_file l_mode l_user l_group; do
         file_mug_chk
      done <<< "$(stat -Lc '%n %#a %U %G' "$l_gfile")"
   done < <(find /boot -type f \( -name 'grub*' -o -name 'user.cfg' \) -
print0)
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  *** PASS ***\n- * Correctly set *
:\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
      [ -n "$l_output" ] && echo -e " - * Correctly set * :\n$l_output\n"
   fi
}
```

Remediation:

Run the following to update the mode, ownership, and group ownership of the grub configuration files:
-IF- the system uses UEFI (Files located in `/boot/efi/EFI/*`)
Edit `/etc/fstab` and add the `fmask=0077`, `uid=0`, and `gid=0` options:
Example:

```
<device> /boot/efi vfat defaults,umask=0027,fmask=0077,uid=0,gid=0 0 0
```

Note: This may require a re-boot to enable the change
-OR-
-IF- the system uses BIOS (Files located in `/boot/grub2/*`)
Run the following commands to set ownership and permissions on your grub configuration file(s):

```
# [ -f /boot/grub2/grub.cfg ] && chown root:root /boot/grub2/grub.cfg
# [ -f /boot/grub2/grub.cfg ] && chmod u-x,go-rwx /boot/grub2/grub.cfg

# [ -f /boot/grub2/grubenv ] && chown root:root /boot/grub2/grubenv
# [ -f /boot/grub2/grubenv ] && chmod u-x,go-rwx /boot/grub2/grubenv

# [ -f /boot/grub2/user.cfg ] && chown root:root /boot/grub2/user.cfg
# [ -f /boot/grub2/user.cfg ] && chmod u-x,go-rwx /boot/grub2/user.cfg
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1542, T1542.000	TA0005, TA0007	M1022

1.3.3 Ensure authentication required for single user mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Note: The systemctl option `--fail` is synonymous with `--job-mode=fail`. Using either is acceptable.

Rationale:

Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Run the following commands and verify that `/sbin/sulogin` or `/usr/sbin/sulogin` is used as shown:

```
# grep /sbin/sulogin /usr/lib/systemd/system/rescue.service

ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
# grep /sbin/sulogin /usr/lib/systemd/system/emergency.service

ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

Remediation:

Edit `/usr/lib/systemd/system/rescue.service` and `/usr/lib/systemd/system/emergency.service` and set `ExecStart` to use `/sbin/sulogin` or `/usr/sbin/sulogin`:

```
ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.4 Configure Additional Process Hardening

1.4.1 Ensure address space layout randomization (ASLR) is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale:

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.randomize_va_space` is set to `2`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("kernel.randomize_va_space=2")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.randomize_va_space = 2`

Example:

```
# printf '%s\n' "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

kernel.randomize_va_space = 2

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 Rev. 5: CM-6
3. NIST SP 800-53A :: CM-6.1 (iv)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 Enable Anti-Exploitation Features Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0002	M1050

1.4.2 Ensure ptrace_scope is restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `ptrace()` system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

Rationale:

If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

Enabling restricted mode will limit the ability of a compromised process to PTRACE_ATTACH on other processes running under the same user. With restricted mode, ptrace will continue to work with root user.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.yama.ptrace_scope` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("kernel.yama.ptrace_scope=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.yama.ptrace_scope = 1`

Example:

```
# printf '%s\n' "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.yama.ptrace_scope=1
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

References:

1. https://www.kernel.org/doc/Documentation/security/Yama.txt
2. https://github.com/raj3shp/termspy

Additional Information:

Ptrace is very rarely used by regular applications and is mostly used by debuggers such as `gdb` and `strace`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1055.008		

1.4.3 Ensure core dump backtraces are disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems, increasing the risk to the system.

Audit:

Run the following command to verify `ProcessSizeMax` is set to `0` in `/etc/systemd/coredump.conf`:

```
# grep -Pi -- '^\h*ProcessSizeMax\b' /etc/systemd/coredump.conf

ProcessSizeMax=0
```

Remediation:

Create or edit the file `/etc/systemd/coredump.conf` and edit or add the following line:

```
ProcessSizeMax=0
```

Default Value:

ProcessSizeMax=2G

References:

1. https://www.freedesktop.org/software/systemd/man/coredump.conf.html
2. NIST SP 800-53 Rev. 5: CM-6b

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0007	M1057

1.4.4 Ensure core dump storage is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Run the following command to verify `Storage` is set to `none` in `/etc/systemd/coredump.conf`:

```
# grep -Pi -- '^\h*Storage\b' /etc/systemd/coredump.conf

Storage=none
```

Remediation:

Create or edit the file `/etc/systemd/coredump.conf` and edit or add the following line:

```
Storage=none
```

Default Value:

Storage=external

References:

1. https://www.freedesktop.org/software/systemd/man/coredump.conf.html

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000	TA0007	M1057

1.5 Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

Impact: Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

1.5.1 Configure SELinux

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called an SELinux context. A SELinux context, sometimes referred to as an SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods. For example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.

In Fedora 28 Family Linux distributions, system services are controlled by the systemd daemon; systemd starts and stops all services, and users and processes communicate with systemd using the systemctl utility. The systemd daemon can consult the SELinux policy and check the label of the calling process and the label of the unit file that the caller tries to manage, and then ask SELinux whether or not the caller is allowed the access. This approach strengthens access control to critical system capabilities, which include starting and stopping system services.

This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation.

Two such policies have been designed for use with Fedora 28 Family Linux distributions and are included with the system:

- `targeted` - Targeted processes run in their own domain, called a confined domain. In a confined domain, the files that a targeted process has access to are limited. If a confined process is compromised by an attacker, the attacker’s access to resources and the possible damage they can do is also limited. SELinux denies access to these resources and logs the denial.
- `mls` - Implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the `targeted` policy.

Note:

- Remember that SELinux policy rules are checked after DAC rules. SELinux policy rules are not used if DAC rules deny access first, which means that no SELinux denial is logged if the traditional DAC rules prevent the access.
- This section only applies if SELinux is in use on the system. Additional Mandatory Access Control systems exist.
- To avoid incorrect SELinux labeling and subsequent problems, ensure that you start services using a systemctl start command.

References:

- NSA SELinux resources:
  - https://www.nsa.gov/Research/Technical-Papers-Brochures/smdsearch14229/selinux
- Fedora SELinux resources:
  - Getting started with SELinux: https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux
  - User Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/using_selinux/index
- SELinux Project web page and wiki:
  - http://www.selinuxproject.org

1.5.1.1 Ensure SELinux is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

SELinux provides Mandatory Access Control.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Audit:

Verify SELinux is installed.
Run the following command:

```
# rpm -q libselinux

libselinux-<version>
```

Remediation:

Run the following command to install `SELinux`:

```
# yum install libselinux
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0003	M1026

1.5.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.

Rationale:

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

Impact:

Files created while SELinux is disabled are not labeled at all. This behavior causes problems when changing to enforcing mode because files are labeled incorrectly or are not labeled at all. To prevent incorrectly labeled and unlabeled files from causing problems, file systems are automatically relabeled when changing from the disabled state to permissive or enforcing mode. This can be a long running process that should be accounted for as it may extend downtime during initial re-boot.

Audit:

Run the following command to verify that neither the `selinux=0` or `enforcing=0` parameters have been set:

```
# grubby --info=ALL | grep -Po '(selinux|enforcing)=0\b'
```

Nothing should be returned
Note: `/etc/default/grub` should be checked because the `grub2-mkconfig -o` command will overwrite `grub.cfg` with parameters listed in `/etc/default/grub`.
Run the following command to verify that the `selinux=0` and `enforcing=0` parameters have not been set in `/etc/default/grub`:

```
# grep -Psi --
'^\h*GRUB_CMDLINE_LINUX(_DEFAULT)?=\"([^#\n\r]+\h+)?(selinux|enforcing)=[^1\n
\r]\d*\b' /etc/default/grub
```

Nothing should be returned

Remediation:

Run the following command to remove the `selinux=0` and `enforcing=0` parameters:

```
grubby --update-kernel ALL --remove-args "selinux=0 enforcing=0"
```

Edit `/etc/default/grub` and remove `selinux=0` and `enforcing=0` from all lines beginning with `GRUB_CMDLINE_LINUX=` or `GRUB_CMDLINE_LINUX_DEFAULT=`:
Example:

```
# sed -ri 's/\s*(selinux|enforcing)=0\s*//g' /etc/default/grub
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2
2. GRUBBY(8)

Additional Information:

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

`grubby` is a command line tool used to configure bootloader menu entries across multiple architectures. It is used for updating and displaying information about the configuration files for various architecture specific bootloaders.

It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

The grubby executable has full support for the grub2 bootloader on x86_64 systems using legacy BIOS or modern UEFI firmware and ppc64 and ppc64le hardware using OPAL or SLOF as firmware.

Legacy s390 and the current s390x architectures and their zipl bootloader are fully supported.

Support for yaboot has been deprecated as all ppc architecture hardware since the Power8 uses grub2 or petitboot which both use the grub2 configuration file format.

Legacy bootloaders LILO, SILO, and ELILO are deprecated and no longer receiving active support in favor of previously mentioned bootloaders.

The default bootloader target is primarily determined by the architecture for which grubby has been built. Each architecture has a preferred bootloader, and each bootloader has its own configuration file. If no bootloader is selected on the command line, grubby will use these default settings to search for an existing configuration. If no bootloader configuration file is found, grubby will use the default value for that architecture.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0003	M1026

1.5.1.3 Ensure SELinux policy is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Audit:

Run the following commands and ensure output matches either " `targeted` " or " `mls` ":

```
# grep -E '^\s*SELINUXTYPE=(targeted|mls)\b' /etc/selinux/config

SELINUXTYPE=targeted
# sestatus | grep Loaded

Loaded policy name:             targeted
```

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

If your organization requires stricter policies, ensure that they are set in the `/etc/selinux/config` file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000	TA0005	

1.5.1.4 Ensure the SELinux mode is not disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- `Enforcing` - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- `Permissive` - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- `Disabled` - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

Note: You can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd_t domain permissive:

```
# semanage permissive -a httpd_t
```

Rationale:

Running SELinux in disabled mode is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

Audit:

Run the following command to verify SELinux's current mode:

```
# getenforce

Enforcing
-OR-
Permissive
```

Run the following command to verify SELinux's configured mode:

```
# grep -Ei '^\s*SELINUX=(enforcing|permissive)' /etc/selinux/config

SELINUX=enforcing
-OR-
SELINUX=permissive
```

Remediation:

Run one of the following commands to set SELinux's running mode:
To set SELinux mode to `Enforcing`:

```
# setenforce 1
```

-OR-
To set SELinux mode to `Permissive`:

```
# setenforce 0
```

Edit the `/etc/selinux/config` file to set the SELINUX parameter:
For Enforcing mode:

```
SELINUX=enforcing
```

-OR-
For Permissive mode:

```
SELINUX=permissive
```

References:

1. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-introduction-selinux_modes
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0003	M1026

1.5.1.5 Ensure the SELinux mode is enforcing (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- `Enforcing` - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- `Permissive` - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- `Disabled` - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

Note: You can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd_t domain permissive:

```
# semanage permissive -a httpd_t
```

Rationale:

Running SELinux in disabled mode the system not only avoids enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

Running SELinux in Permissive mode, though helpful for developing SELinux policy, only logs access denial entries, but does not deny any operations.

Impact:

Running SELinux in Enforcing mode may block intended access to files or processes if the SELinux policy is not correctly configured. If this occurs, review the system logs for details and update labels or policy as appropriate.

Audit:

Run the following command to verify SELinux's current mode:

```
# getenforce

Enforcing
```

Run the following command to verify SELinux's configured mode:

```
# grep -i SELINUX=enforcing /etc/selinux/config

SELINUX=enforcing
```

Remediation:

Run the following command to set SELinux's running mode:

```
# setenforce 1
```

Edit the `/etc/selinux/config` file to set the SELINUX parameter:
For Enforcing mode:

```
SELINUX=enforcing
```

References:

1. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-introduction-selinux_modes
2. CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
3. NIST SP 800-53 Revision 4 :: AC-3 (4)
4. CCI-002696: The information system verifies correct operation of organization-defined security functions.
5. NIST SP 800-53 Revision 4 :: SI-6 a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0005	

1.5.1.6 Ensure no unconfined services exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Unconfined processes run in unconfined domains

Rationale:

For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. SELinux is a security enhancement on top of DAC rules – it does not replace them

Audit:

Run the following command and verify no output is produced:

```
# ps -eZ | grep unconfined_service_t
```

Remediation:

Investigate any unconfined processes found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1565, T1565.001, T1565.003	TA0004	M1022

1.5.1.7 Ensure the MCS Translation Service (mcstrans) is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`

Rationale:

Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.

Audit:

Verify `mcstrans` is not installed.
Run the following command:

```
# rpm -q mcstrans

package mcstrans is not installed
```

Remediation:

Run the following command to uninstall `mcstrans`:

```
# yum remove mcstrans
```

References:

1. NIST SP 800-53 Rev. 5: SI-4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1543, T1543.002	TA0005	M1033

1.5.1.8 Ensure SETroubleshoot is not installed (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

Rationale:

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.

Audit:

Verify `setroubleshoot` is not installed.
Run the following command:

```
# rpm -q setroubleshoot

package setroubleshoot is not installed
```

Remediation:

Run the following command to uninstall `setroubleshoot`:

```
# yum remove setroubleshoot
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1543, T1543.002	TA0005	M1033

1.6 Configure Command Line Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

1.6.1 Ensure message of the day is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/motd
```

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
-OR-
-IF- the `motd` is not used, this file can be removed.
Run the following command to remove the `motd` file:

```
# rm /etc/motd
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.2 Ensure local login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue
```

Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
Example:

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.3 Ensure remote login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue.net
```

Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
Example:

```
# echo "Authorized users only. All activity may be monitored and reported." >
/etc/issue.net
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1018, T1018.000, T1082, T1082.000, T1592, T1592.004	TA0007	

1.6.4 Ensure access to /etc/motd is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Rationale:

-IF- the `/etc/motd` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify that if `/etc/motd` exists, `Access` is `644` or more restrictive, `Uid` and `Gid` are both `0/root`:

```
# [ -e /etc/motd ] && stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/
%G)' /etc/motd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
  -- OR --
Nothing is returned
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/motd`:

```
# chown root:root $(readlink -e /etc/motd)
# chmod u-x,go-wx $(readlink -e /etc/motd)
```

-OR-
Run the following command to remove the `/etc/motd` file:

```
# rm /etc/motd
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.6.5 Ensure access to /etc/issue is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Rationale:

-IF- the `/etc/issue` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Access` is `644` or more restrictive and `Uid` and `Gid` are both `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/issue

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue`:

```
# chown root:root $(readlink -e /etc/issue)
# chmod u-x,go-wx $(readlink -e /etc/issue)
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.6.6 Ensure access to /etc/issue.net is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Rationale:

-IF- the `/etc/issue.net` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Access` is `644` or more restrictive and `Uid` and `Gid` are both `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/issue.net

Access: (0644/-rw-r--r--)  Uid: ( 0/ root)   Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue.net`:

```
# chown root:root $(readlink -e /etc/issue.net)
# chmod u-x,go-wx $(readlink -e /etc/issue.net)
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

1.7 Configure GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Note: If GDM is not installed on the system, this section can be skipped

1.7.1 Ensure GNOME Display Manager is removed (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Rationale:

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

Impact:

Removing the GNOME Display manager will remove the Graphical User Interface (GUI) from the system.

Audit:

Run the following command and verify the output:

```
# rpm -q gdm

package gdm is not installed
```

Remediation:

Run the following command to remove the `gdm` package

```
# yum remove gdm
```

References:

1. https://wiki.gnome.org/Projects/GDM
2. NIST SP 800-53 Rev. 5: CM-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1543, T1543.002	TA0002	M1033

1.7.2 Ensure GDM login banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Audit:

Run the following script to verify that the text banner on the login screen is enabled and set:

```
#!/usr/bin/env bash

{
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   if [ -n "$l_pkgoutput" ]; then
      l_output="" l_output2=""
      echo -e "$l_pkgoutput"
      # Look for existing settings and set variables if they exist
      l_gdmfile="$(grep -Prils '^\h*banner-message-enable\b' /etc/dconf/db/*.d)"
      if [ -n "$l_gdmfile" ]; then
         # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
         l_gdmprofile="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_gdmfile")"
         # Check if banner message is enabled
         if grep -Pisq '^\h*banner-message-enable=true\b' "$l_gdmfile"; then
            l_output="$l_output\n - The \"banner-message-enable\" option is enabled in
\"$l_gdmfile\""
         else
            l_output2="$l_output2\n - The \"banner-message-enable\" option is not enabled"
         fi
         l_lsbt="$(grep -Pios '^\h*banner-message-text=.*$' "$l_gdmfile")"
         if [ -n "$l_lsbt" ]; then
            l_output="$l_output\n - The \"banner-message-text\" option is set in \"$l_gdmfile\"\n
- banner-message-text is set to:\n  - \"$l_lsbt\""
         else
            l_output2="$l_output2\n - The \"banner-message-text\" option is not set"
         fi
         if grep -Pq "^\h*system-db:$l_gdmprofile" /etc/dconf/profile/"$l_gdmprofile"; then
            l_output="$l_output\n - The \"$l_gdmprofile\" profile exists"
         else
            l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist"
         fi
         if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
            l_output="$l_output\n - The \"$l_gdmprofile\" profile exists in the dconf database"
         else
            l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist in the dconf
database"
         fi
      else
         l_output2="$l_output2\n - The \"banner-message-enable\" option isn't configured"
      fi
   else
      echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n- Audit result:\n  *** PASS ***\n"
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to verify that the banner message is enabled and set:

```
#!/usr/bin/env bash

{
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   if [ -n "$l_pkgoutput" ]; then

      l_gdmprofile="gdm" # Set this to desired profile name IaW Local site policy
      l_bmessage="'Authorized uses only. All activity may be monitored and reported'" # Set to
desired banner message
      if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
         echo "Creating profile \"$l_gdmprofile\""
         echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" > /etc/dconf/profile/$l_gdmprofile
      fi
      if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
         echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/\""
         mkdir /etc/dconf/db/$l_gdmprofile.d/
      fi
      if ! grep -Piq '^\h*banner-message-enable\h*=\h*true\b' /etc/dconf/db/$l_gdmprofile.d/*;
then
         echo "creating gdm keyfile for machine-wide settings"
         if ! grep -Piq -- '^\h*banner-message-enable\h*=\h*' /etc/dconf/db/$l_gdmprofile.d/*;
then
            l_kfile="/etc/dconf/db/$l_gdmprofile.d/01-banner-message"
            echo -e "\n[org/gnome/login-screen]\nbanner-message-enable=true" >> "$l_kfile"
         else
            l_kfile="$(grep -Pil -- '^\h*banner-message-enable\h*=\h*'
/etc/dconf/db/$l_gdmprofile.d/*)"
            ! grep -Pq '^\h*\[org\/gnome\/login-screen\]' "$l_kfile" && sed -ri '/^\s*banner-
message-enable/ i\[org/gnome/login-screen]' "$l_kfile"
            ! grep -Pq '^\h*banner-message-enable\h*=\h*true\b' "$l_kfile" && sed -ri
's/^\s*(banner-message-enable\s*=\s*)(\S+)(\s*.*$)/\1true \3//' "$l_kfile"
 #           sed -ri '/^\s*\[org\/gnome\/login-screen\]/ a\\nbanner-message-enable=true'
"$l_kfile"
         fi
      fi
      if ! grep -Piq "^\h*banner-message-text=[\'\"]+\S+" "$l_kfile"; then
         sed -ri "/^\s*banner-message-enable/ a\banner-message-text=$l_bmessage" "$l_kfile"
      fi
      dconf update
   else
      echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n - No remediation required\n"
   fi
}
```

Note:

- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.
  OR

Run the following command to remove the gdm package:

```
# yum remove gdm
```

Default Value:

disabled

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

Additional options and sections may appear in the `/etc/dconf/db/gdm.d/01-banner-message` file.

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002	TA0007	M1028

1.7.3 Ensure GDM disable-user-list option is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

The `disable-user-list` option controls if a list of users is displayed on the login screen

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Audit:

Run the following script and to verify that the `disable-user-list` option is enabled or GNOME isn't installed:

```
#!/usr/bin/env bash

{
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   if [ -n "$l_pkgoutput" ]; then
      output="" output2=""
      l_gdmfile="$(grep -Pril '^\h*disable-user-list\h*=\h*true\b' /etc/dconf/db)"
      if [ -n "$l_gdmfile" ]; then
         output="$output\n - The \"disable-user-list\" option is enabled in \"$l_gdmfile\""
         l_gdmprofile="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<< "$l_gdmfile")"
         if grep -Pq "^\h*system-db:$l_gdmprofile" /etc/dconf/profile/"$l_gdmprofile"; then
            output="$output\n - The \"$l_gdmprofile\" exists"
         else
            output2="$output2\n - The \"$l_gdmprofile\" doesn't exist"
         fi
         if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
            output="$output\n - The \"$l_gdmprofile\" profile exists in the dconf database"
         else
            output2="$output2\n - The \"$l_gdmprofile\" profile doesn't exist in the dconf
database"
         fi
      else
         output2="$output2\n - The \"disable-user-list\" option is not enabled"
      fi
      if [ -z "$output2" ]; then
         echo -e "$l_pkgoutput\n- Audit result:\n   *** PASS: ***\n$output\n"
      else
         echo -e "$l_pkgoutput\n- Audit Result:\n   *** FAIL: ***\n$output2\n"
         [ -n "$output" ] && echo -e "$output\n"
      fi
   else
      echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n- Audit result:\n  *** PASS ***\n"
   fi
}
```

Remediation:

Run the following script to enable the `disable-user-list` option:
Note: the `l_gdm_profile` variable in the script can be changed if a different profile name is desired in accordance with local site policy.

```
#!/usr/bin/env bash

{
   l_gdmprofile="gdm"
   if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
      echo "Creating profile \"$l_gdmprofile\""
      echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" >
/etc/dconf/profile/$l_gdmprofile
   fi
   if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
      echo "Creating dconf database directory
\"/etc/dconf/db/$l_gdmprofile.d/\""
      mkdir /etc/dconf/db/$l_gdmprofile.d/
   fi
   if ! grep -Piq '^\h*disable-user-list\h*=\h*true\b'
/etc/dconf/db/$l_gdmprofile.d/*; then
      echo "creating gdm keyfile for machine-wide settings"
      if ! grep -Piq -- '^\h*\[org\/gnome\/login-screen\]'
/etc/dconf/db/$l_gdmprofile.d/*; then
         echo -e "\n[org/gnome/login-screen]\n# Do not show the user
list\ndisable-user-list=true" >> /etc/dconf/db/$l_gdmprofile.d/00-login-
screen
      else
         sed -ri '/^\s*\[org\/gnome\/login-screen\]/ a\# Do not show the user
list\ndisable-user-list=true' $(grep -Pil -- '^\h*\[org\/gnome\/login-
screen\]' /etc/dconf/db/$l_gdmprofile.d/*)
      fi
   fi
   dconf update
}
```

Note: When the user profile is created or changed, the user will need to log out and log in again before the changes will be applied.
OR
Run the following command to remove the GNOME package:

```
# yum remove gdm
```

Default Value:

false

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/login-userlist-disable.html.en
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the user list

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002	TA0007	M1028

1.7.4 Ensure GDM screen locks when the user is idle (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

- `idle-delay=uint32 {n}` - Number of seconds of inactivity before the screen goes blank
- `lock-delay=uint32 {n}` - Number of seconds after the screen is blank before locking the screen

Example key file:

```
# Specify the dconf path
[org/gnome/desktop/session]

# Number of seconds of inactivity before the screen goes blank
# Set to 0 seconds if you want to deactivate the screensaver.
idle-delay=uint32 900

# Specify the dconf path
[org/gnome/desktop/screensaver]

# Number of seconds after the screen is blank before locking the screen
lock-delay=uint32 5
```

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Audit:

Run the following script to verify that the screen locks when the user is idle:

```
#!/usr/bin/env bash

{
   # Check if GNMOE Desktop Manager is installed.  If package isn't
installed, recommendation is Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      l_output="" l_output2=""
      l_idmv="900" # Set for max value for idle-delay in seconds
      l_ldmv="5" # Set for max value for lock-delay in seconds
      # Look for idle-delay to determine profile in use, needed for remaining
tests
      l_kfile="$(grep -Psril '^\h*idle-delay\h*=\h*uint32\h+\d+\b'
/etc/dconf/db/*/)" # Determine file containing idle-delay key
      if [ -n "$l_kfile" ]; then
         # set profile name (This is the name of a dconf database)
         l_profile="$(awk -F'/' '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")" #Set the key profile name
         l_pdbdir="/etc/dconf/db/$l_profile.d" # Set the key file dconf db
directory
         # Confirm that idle-delay exists, includes unit32, and value is
between 1 and max value for idle-delay
         l_idv="$(awk -F 'uint32' '/idle-delay/{print $2}' "$l_kfile" |
xargs)"
         if [ -n "$l_idv" ]; then
            [ "$l_idv" -gt "0" -a "$l_idv" -le "$l_idmv" ] &&
l_output="$l_output\n - The \"idle-delay\" option is set to \"$l_idv\"
seconds in \"$l_kfile\""
            [ "$l_idv" = "0" ] && l_output2="$l_output2\n - The \"idle-
delay\" option is set to \"$l_idv\" (disabled) in \"$l_kfile\""
            [ "$l_idv" -gt "$l_idmv" ] && l_output2="$l_output2\n - The
\"idle-delay\" option is set to \"$l_idv\" seconds (greater than $l_idmv) in
\"$l_kfile\""
         else
            l_output2="$l_output2\n - The \"idle-delay\" option is not set in
\"$l_kfile\""
         fi
         # Confirm that lock-delay exists, includes unit32, and value is
between 0 and max value for lock-delay
         l_ldv="$(awk -F 'uint32' '/lock-delay/{print $2}' "$l_kfile" |
xargs)"
         if [ -n "$l_ldv" ]; then
            [ "$l_ldv" -ge "0" -a "$l_ldv" -le "$l_ldmv" ] &&
l_output="$l_output\n - The \"lock-delay\" option is set to \"$l_ldv\"
```

```
seconds in \"$l_kfile\""
            [ "$l_ldv" -gt "$l_ldmv" ] && l_output2="$l_output2\n - The
\"lock-delay\" option is set to \"$l_ldv\" seconds (greater than $l_ldmv) in
\"$l_kfile\""
         else
            l_output2="$l_output2\n - The \"lock-delay\" option is not set in
\"$l_kfile\""
         fi
         # Confirm that dconf profile exists
         if grep -Psq "^\h*system-db:$l_profile" /etc/dconf/profile/*; then
            l_output="$l_output\n - The \"$l_profile\" profile exists"
         else
            l_output2="$l_output2\n - The \"$l_profile\" doesn't exist"
         fi
         # Confirm that dconf profile database file exists
         if [ -f "/etc/dconf/db/$l_profile" ]; then
            l_output="$l_output\n - The \"$l_profile\" profile exists in the
dconf database"
         else
            l_output2="$l_output2\n - The \"$l_profile\" profile doesn't
exist in the dconf database"
         fi
      else
         l_output2="$l_output2\n - The \"idle-delay\" option doesn't exist,
remaining tests skipped"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n  - Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Note:

- `idle-delay=uint32` Should be 900 seconds (15 minutes) or less, not `0` (disabled) and follow local site policy
- `lock-delay=uint32` should be 5 seconds or less and follow local site policy

Remediation:

Create or edit a file in the `/etc/dconf/profile/` and verify it includes the following:

```
user-db:user
system-db:{NAME_OF_DCONF_DATABASE}
```

Note: `local` is the name of a dconf database used in the examples.
Example:

```
# echo -e '\nuser-db:user\nsystem-db:local' >> /etc/dconf/profile/user
```

Create the directory `/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/` if it doesn't already exist:
Example:

```
# mkdir /etc/dconf/db/local.d
```

Create the key file `/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME} to provide information for the {NAME_OF_DCONF_DATABASE} database:
Example script:

```
#!/usr/bin/env bash

{
   l_key_file="/etc/dconf/db/local.d/00-screensaver"
   l_idmv="900" # Set max value for idle-delay in seconds (between 1 and 900)
   l_ldmv="5" # Set max value for lock-delay in seconds (between 0 and 5)
   {
      echo '# Specify the dconf path'
      echo '[org/gnome/desktop/session]'
      echo ''
      echo '# Number of seconds of inactivity before the screen goes blank'
      echo '# Set to 0 seconds if you want to deactivate the screensaver.'
      echo "idle-delay=uint32 $l_idmv"
      echo ''
      echo '# Specify the dconf path'
      echo '[org/gnome/desktop/screensaver]'
      echo ''
      echo '# Number of seconds after the screen is blank before locking the
screen'
      echo "lock-delay=uint32 $l_ldmv"
   } > "$l_key_file"
}
```

Note: You must include the uint32 along with the integer key values as shown.
Run the following command to update the system databases:

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1461	TA0027	

1.7.5 Ensure GDM screen locks cannot be overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Example Lock File:

```
# Lock desktop screensaver settings
/org/gnome/desktop/session/idle-delay
/org/gnome/desktop/screensaver/lock-delay
```

Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Without locking down the system settings, user settings take precedence over the system settings.

Audit:

Run the following script to verify that the screen lock cannot be overridden:

```
#!/usr/bin/env bash

{
   # Check if GNOME Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      l_output="" l_output2=""
      # Look for idle-delay to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*idle-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/ |
awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*lock-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/
| awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Prilq '\/org\/gnome\/desktop\/session\/idle-delay\b' "$l_kfd"; then
            l_output="$l_output\n - \"idle-delay\" is locked in \"$(grep -Pril
'\/org\/gnome\/desktop\/session\/idle-delay\b' "$l_kfd")\""
         else
            l_output2="$l_output2\n - \"idle-delay\" is not locked"
         fi
      else
         l_output2="$l_output2\n - \"idle-delay\" is not set so it can not be locked"
      fi
      if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Prilq '\/org\/gnome\/desktop\/screensaver\/lock-delay\b' "$l_kfd2"; then
            l_output="$l_output\n - \"lock-delay\" is locked in \"$(grep -Pril
'\/org\/gnome\/desktop\/screensaver\/lock-delay\b' "$l_kfd2")\""
         else
            l_output2="$l_output2\n - \"lock-delay\" is not locked"
         fi
      else
         l_output2="$l_output2\n - \"lock-delay\" is not set so it can not be locked"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
         [ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to ensure screen locks cannot be overridden:

```
#!/usr/bin/env bash

{
   # Check if GNMOE Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\"
exists on the system\n - remediating configuration if needed"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      # Look for idle-delay to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*idle-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/ |
awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      # Look for lock-delay to determine profile in use, needed for remaining tests
      l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*lock-delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/*/
| awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Prilq '^\h*\/org\/gnome\/desktop\/session\/idle-delay\b' "$l_kfd"; then
            echo " - \"idle-delay\" is locked in \"$(grep -Pril
'^\h*\/org\/gnome\/desktop\/session\/idle-delay\b' "$l_kfd")\""
         else
            echo "creating entry to lock \"idle-delay\""
            [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir
"$l_kfd"/locks
            {
               echo -e '\n# Lock desktop screensaver idle-delay setting'
               echo '/org/gnome/desktop/session/idle-delay'
            } >> "$l_kfd"/locks/00-screensaver
         fi
      else
         echo -e " - \"idle-delay\" is not set so it can not be locked\n - Please follow
Recommendation \"Ensure GDM screen locks when the user is idle\" and follow this Recommendation
again"
      fi
      if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Prilq '^\h*\/org\/gnome\/desktop\/screensaver\/lock-delay\b' "$l_kfd2"; then
            echo " - \"lock-delay\" is locked in \"$(grep -Pril
'^\h*\/org\/gnome\/desktop\/screensaver\/lock-delay\b' "$l_kfd2")\""
         else
            echo "creating entry to lock \"lock-delay\""
            [ ! -d "$l_kfd2"/locks ] && echo "creating directory $l_kfd2/locks" && mkdir
"$l_kfd2"/locks
            {
               echo -e '\n# Lock desktop screensaver lock-delay setting'
               echo '/org/gnome/desktop/screensaver/lock-delay'
            } >> "$l_kfd2"/locks/00-screensaver
         fi
      else
         echo -e " - \"lock-delay\" is not set so it can not be locked\n - Please follow
Recommendation \"Ensure GDM screen locks when the user is idle\" and follow this Recommendation
again"
      fi
   else
      echo -e " - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
}
```

Run the following command to update the system databases:

```
# dconf update
```

Note: Users must log out and back in again before the system-wide settings take effect.

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en
2. https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1456	TA0027	

1.7.6 Ensure GDM automatic mounting of removable media is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Audit:

Run the following script to verify automatic mounting is disabled:

```
#!/usr/bin/env bash

{
   l_pkgoutput="" l_output="" l_output2=""
   # Check if GNOME Desktop Manager is installed.  If package isn't
installed, recommendation is Not Applicable\n
   # determine system's package manager
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      echo -e "$l_pkgoutput"
      # Look for existing settings and set variables if they exist
      l_kfile="$(grep -Prils -- '^\h*automount\b' /etc/dconf/db/*.d)"
      l_kfile2="$(grep -Prils -- '^\h*automount-open\b' /etc/dconf/db/*.d)"
      # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
      if [ -f "$l_kfile" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
      elif [ -f "$l_kfile2" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")"
      fi
      # If the profile name exist, continue checks
      if [ -n "$l_gpname" ]; then
         l_gpdir="/etc/dconf/db/$l_gpname.d"
         # Check if profile file exists
         if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*;
then
            l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\" exists"
         else
            l_output2="$l_output2\n - dconf database profile isn't set"
         fi
         # Check if the dconf database file exists
         if [ -f "/etc/dconf/db/$l_gpname" ]; then
            l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
         else
            l_output2="$l_output2\n - The dconf database \"$l_gpname\"
doesn't exist"
         fi
         # check if the dconf database directory exists
         if [ -d "$l_gpdir" ]; then
            l_output="$l_output\n - The dconf directory \"$l_gpdir\" exitst"
         else
            l_output2="$l_output2\n - The dconf directory \"$l_gpdir\"
doesn't exist"
         fi
```

```
         # check automount setting
         if grep -Pqrs -- '^\h*automount\h*=\h*false\b' "$l_kfile"; then
            l_output="$l_output\n - \"automount\" is set to false in:
\"$l_kfile\""
         else
            l_output2="$l_output2\n - \"automount\" is not set correctly"
         fi
         # check automount-open setting
         if grep -Pqs -- '^\h*automount-open\h*=\h*false\b' "$l_kfile2"; then
            l_output="$l_output\n - \"automount-open\" is set to false in:
\"$l_kfile2\""
         else
            l_output2="$l_output2\n - \"automount-open\" is not set
correctly"
         fi
      else
         # Setings don't exist. Nothing further to check
         l_output2="$l_output2\n - neither \"automount\" or \"automount-
open\" is set"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n  - Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable automatic mounting of media for all GNOME users:

```
#!/usr/bin/env bash

{
   l_pkgoutput=""
   l_gpname="local" # Set to desired dconf profile name (default is local)
   # Check if GNOME Desktop Manager is installed.  If package isn't
installed, recommendation is Not Applicable\n
   # determine system's package manager
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      echo -e "$l_pkgoutput"
      # Look for existing settings and set variables if they exist
      l_kfile="$(grep -Prils -- '^\h*automount\b' /etc/dconf/db/*.d)"
      l_kfile2="$(grep -Prils -- '^\h*automount-open\b' /etc/dconf/db/*.d)"
      # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
      if [ -f "$l_kfile" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
         echo " - updating dconf profile name to \"$l_gpname\""
      elif [ -f "$l_kfile2" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")"
         echo " - updating dconf profile name to \"$l_gpname\""
      fi
      # check for consistency (Clean up configuration if needed)
      if [ -f "$l_kfile" ] && [ "$(awk -F\/ '{split($(NF-1),a,".");print
a[1]}' <<< "$l_kfile")" != "$l_gpname" ]; then
         sed -ri "/^\s*automount\s*=/s/^/# /" "$l_kfile"
         l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"
      fi
      if [ -f "$l_kfile2" ] && [ "$(awk -F\/ '{split($(NF-1),a,".");print
a[1]}' <<< "$l_kfile2")" != "$l_gpname" ]; then
         sed -ri "/^\s*automount-open\s*=/s/^/# /" "$l_kfile2"
      fi
      [ -z "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-
automount"
      # Check if profile file exists
      if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
         echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\""
      else
         if [ ! -f "/etc/dconf/profile/user" ]; then
            l_gpfile="/etc/dconf/profile/user"
         else
            l_gpfile="/etc/dconf/profile/user2"
         fi
```

```
         echo -e " - creating dconf database profile"
         {
            echo -e "\nuser-db:user"
            echo "system-db:$l_gpname"
         } >> "$l_gpfile"
      fi
      # create dconf directory if it doesn't exists
      l_gpdir="/etc/dconf/db/$l_gpname.d"
      if [ -d "$l_gpdir" ]; then
         echo " - The dconf database directory \"$l_gpdir\" exists"
      else
         echo " - creating dconf database directory \"$l_gpdir\""
         mkdir "$l_gpdir"
      fi
      # check automount-open setting
      if grep -Pqs -- '^\h*automount-open\h*=\h*false\b' "$l_kfile"; then
         echo " - \"automount-open\" is set to false in: \"$l_kfile\""
      else
         echo " - creating \"automount-open\" entry in \"$l_kfile\""
         ! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
         sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a
\\nautomount-open=false' "$l_kfile"
      fi
      # check automount setting
      if grep -Pqs -- '^\h*automount\h*=\h*false\b' "$l_kfile"; then
         echo " - \"automount\" is set to false in: \"$l_kfile\""
      else
         echo " - creating \"automount\" entry in \"$l_kfile\""
         ! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
         sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a
\\nautomount=false' "$l_kfile"
      fi
      # update dconf database
      dconf update
   else
      echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n  - Recommendation is not applicable"
   fi
}
```

OR

Run the following command to uninstall the GNOME desktop Manager package:

```
# yum remove gdm
```

References:

1. https://access.redhat.com/solutions/20107

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

By default GNOME automatically mounts removable media when inserted as a convenience to the user

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Example Lock File:

```
# Lock automount settings
/org/gnome/desktop/media-handling/automount
/org/gnome/desktop/media-handling/automount-open
```

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users

Audit:

Run the following script to verify disable automatic mounting is locked:

```
#!/usr/bin/env bash

{
   # Check if GNOME Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      l_output="" l_output2=""
      echo -e "$l_pkgoutput\n"
      # Look for idle-delay to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*automount\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*automount-open\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount\b' "$l_kfd"; then
            l_output="$l_output\n - \"automount\" is locked in \"$(grep -Pril
'^\h*\/org/gnome\/desktop\/media-handling\/automount\b' "$l_kfd")\""
         else
            l_output2="$l_output2\n - \"automount\" is not locked"
         fi
      else
         l_output2="$l_output2\n - \"automount\" is not set so it can not be locked"
      fi
      if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount-open\b' "$l_kfd2";
then
            l_output="$l_output\n - \"lautomount-open\" is locked in \"$(grep -Pril
'^\h*\/org/gnome\/desktop\/media-handling\/automount-open\b' "$l_kfd2")\""
         else
            l_output2="$l_output2\n - \"automount-open\" is not locked"
         fi
      else
         l_output2="$l_output2\n - \"automount-open\" is not set so it can not be locked"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to lock disable automatic mounting of media for all GNOME users:

```
#!/usr/bin/env bash

{
   # Check if GNMOE Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space seporated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\"
exists on the system\n - remediating configuration if needed"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      # Look for automount to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*automount\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      # Look for automount-open to determine profile in use, needed for remaining tests
      l_kfd2="/etc/dconf/db/$(grep -Psril '^\h*automount-open\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount\b' "$l_kfd"; then
            echo " - \"automount\" is locked in \"$(grep -Pril '^\h*\/org/gnome\/desktop\/media-
handling\/automount\b' "$l_kfd")\""
         else
            echo " - creating entry to lock \"automount\""
            [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir
"$l_kfd"/locks
            {
               echo -e '\n# Lock desktop media-handling automount setting'
               echo '/org/gnome/desktop/media-handling/automount'
            } >> "$l_kfd"/locks/00-media-automount
         fi
      else
         echo -e " - \"automount\" is not set so it can not be locked\n - Please follow
Recommendation \"Ensure GDM automatic mounting of removable media is disabled\" and follow this
Recommendation again"
      fi
      if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/automount-open\b' "$l_kfd2";
then
            echo " - \"automount-open\" is locked in \"$(grep -Pril
'^\h*\/org/gnome\/desktop\/media-handling\/automount-open\b' "$l_kfd2")\""
         else
            echo " - creating entry to lock \"automount-open\""
            [ ! -d "$l_kfd2"/locks ] && echo "creating directory $l_kfd2/locks" && mkdir
"$l_kfd2"/locks
            {
               echo -e '\n# Lock desktop media-handling automount-open setting'
               echo '/org/gnome/desktop/media-handling/automount-open'
            } >> "$l_kfd2"/locks/00-media-automount
         fi
      else
         echo -e " - \"automount-open\" is not set so it can not be locked\n - Please follow
Recommendation \"Ensure GDM automatic mounting of removable media is disabled\" and follow this
Recommendation again"
      fi
      # update dconf database
      dconf update
   else
      echo -e " - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
}
```

References:

1. https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091, T1091.000	TA0001, TA0008	M1042

1.7.8 Ensure GDM autorun-never is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `autorun-never` setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

Rationale:

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

Audit:

Run the following script to verify that `autorun-never` is set to `true` for GDM:

```
#!/usr/bin/env bash

{
   l_pkgoutput="" l_output="" l_output2=""
   # Check if GNOME Desktop Manager is installed.  If package isn't
installed, recommendation is Not Applicable\n
   # determine system's package manager
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space separated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
      echo -e "$l_pkgoutput"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      echo -e "$l_pkgoutput"
      # Look for existing settings and set variables if they exist
      l_kfile="$(grep -Prils -- '^\h*autorun-never\b' /etc/dconf/db/*.d)"
      # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
      if [ -f "$l_kfile" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
      fi
      # If the profile name exist, continue checks
      if [ -n "$l_gpname" ]; then
         l_gpdir="/etc/dconf/db/$l_gpname.d"
         # Check if profile file exists
         if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*;
then
            l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\" exists"
         else
            l_output2="$l_output2\n - dconf database profile isn't set"
         fi
         # Check if the dconf database file exists
         if [ -f "/etc/dconf/db/$l_gpname" ]; then
            l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
         else
            l_output2="$l_output2\n - The dconf database \"$l_gpname\"
doesn't exist"
         fi
         # check if the dconf database directory exists
         if [ -d "$l_gpdir" ]; then
            l_output="$l_output\n - The dconf directory \"$l_gpdir\" exitst"
         else
            l_output2="$l_output2\n - The dconf directory \"$l_gpdir\"
doesn't exist"
         fi
         # check autorun-never setting
         if grep -Pqrs -- '^\h*autorun-never\h*=\h*true\b' "$l_kfile"; then
            l_output="$l_output\n - \"autorun-never\" is set to true in:
```

```
\"$l_kfile\""
         else
            l_output2="$l_output2\n - \"autorun-never\" is not set correctly"
         fi
      else
         # Settings don't exist. Nothing further to check
         l_output2="$l_output2\n - \"autorun-never\" is not set"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n  - Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to set `autorun-never` to `true` for GDM users:

```
#!/usr/bin/env bash

{
   l_pkgoutput="" l_output="" l_output2=""
   l_gpname="local" # Set to desired dconf profile name (default is local)
   # Check if GNOME Desktop Manager is installed.  If package isn't
installed, recommendation is Not Applicable\n
   # determine system's package manager
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space separated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
   done
   echo -e "$l_pkgoutput"
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      echo -e "$l_pkgoutput"
      # Look for existing settings and set variables if they exist
      l_kfile="$(grep -Prils -- '^\h*autorun-never\b' /etc/dconf/db/*.d)"
      # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
      if [ -f "$l_kfile" ]; then
         l_gpname="$(awk -F\/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
         echo " - updating dconf profile name to \"$l_gpname\""
      fi
      [ ! -f "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-
autorun"
      # Check if profile file exists
      if grep -Pq -- "^\h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
         echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^\h*system-db:$l_gpname\b" /etc/dconf/profile/*)\""
      else
         [ ! -f "/etc/dconf/profile/user" ] &&
l_gpfile="/etc/dconf/profile/user" || l_gpfile="/etc/dconf/profile/user2"
         echo -e " - creating dconf database profile"
         {
            echo -e "\nuser-db:user"
            echo "system-db:$l_gpname"
         } >> "$l_gpfile"
      fi
      # create dconf directory if it doesn't exists
      l_gpdir="/etc/dconf/db/$l_gpname.d"
      if [ -d "$l_gpdir" ]; then
         echo " - The dconf database directory \"$l_gpdir\" exists"
      else
         echo " - creating dconf database directory \"$l_gpdir\""
         mkdir "$l_gpdir"
      fi
      # check autorun-never setting
      if grep -Pqs -- '^\h*autorun-never\h*=\h*true\b' "$l_kfile"; then
         echo " - \"autorun-never\" is set to true in: \"$l_kfile\""
```

```
      else
         echo " - creating or updating \"autorun-never\" entry in
\"$l_kfile\""
         if grep -Psq -- '^\h*autorun-never' "$l_kfile"; then
            sed -ri 's/(^\s*autorun-never\s*=\s*)(\S+)(\s*.*)$/\1true \3/'
"$l_kfile"
         else
            ! grep -Psq -- '\^\h*\[org\/gnome\/desktop\/media-handling\]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
            sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a
\\nautorun-never=true' "$l_kfile"
         fi
      fi
   else
      echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n  - Recommendation is not applicable"
   fi
   # update dconf database
   dconf update
}
```

Default Value:

false

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091		

1.7.9 Ensure GDM autorun-never is not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Example Lock File:

```
# Lock desktop media-handling settings
/org/gnome/desktop/media-handling/autorun-never
```

Rationale:

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

Audit:

Run the following script to verify that `autorun-never=true` cannot be overridden:

```
#!/usr/bin/env bash

{
   # Check if GNOME Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space separated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      l_output="" l_output2=""
      echo -e "$l_pkgoutput\n"
      # Look for idle-delay to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*autorun-never\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/autorun-never\b' "$l_kfd"; then
            l_output="$l_output\n - \"autorun-never\" is locked in \"$(grep -Pril
'^\h*\/org/gnome\/desktop\/media-handling\/autorun-never\b' "$l_kfd")\""
         else
            l_output2="$l_output2\n - \"autorun-never\" is not locked"
         fi
      else
         l_output2="$l_output2\n - \"autorun-never\" is not set so it can not be locked"
      fi
   else
      l_output="$l_output\n - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to ensure that `autorun-never=true` cannot be overridden:

```
#!/usr/bin/env bash

{
   # Check if GNOME Desktop Manager is installed.  If package isn't installed, recommendation is
Not Applicable\n
   # determine system's package manager
   l_pkgoutput=""
   if command -v dpkg-query > /dev/null 2>&1; then
      l_pq="dpkg-query -W"
   elif command -v rpm > /dev/null 2>&1; then
      l_pq="rpm -q"
   fi
   # Check if GDM is installed
   l_pcl="gdm gdm3" # Space separated list of packages to check
   for l_pn in $l_pcl; do
      $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n - Package: \"$l_pn\"
exists on the system\n - remediating configuration if needed"
   done
   # Check configuration (If applicable)
   if [ -n "$l_pkgoutput" ]; then
      # Look for autorun to determine profile in use, needed for remaining tests
      l_kfd="/etc/dconf/db/$(grep -Psril '^\h*autorun-never\b' /etc/dconf/db/*/ | awk -F'/'
'{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
      if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
         if grep -Priq '^\h*\/org/gnome\/desktop\/media-handling\/autorun-never\b' "$l_kfd"; then
            echo " - \"autorun-never\" is locked in \"$(grep -Pril
'^\h*\/org/gnome\/desktop\/media-handling\/autorun-never\b' "$l_kfd")\""
         else
            echo " - creating entry to lock \"autorun-never\""
            [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks" && mkdir
"$l_kfd"/locks
            {
               echo -e '\n# Lock desktop media-handling autorun-never setting'
               echo '/org/gnome/desktop/media-handling/autorun-never'
            } >> "$l_kfd"/locks/00-media-autorun
         fi
      else
         echo -e " - \"autorun-never\" is not set so it can not be locked\n - Please follow
Recommendation \"Ensure GDM autorun-never is enabled\" and follow this Recommendation again"
      fi
      # update dconf database
      dconf update
   else
      echo -e " - GNOME Desktop Manager package is not installed on the system\n  -
Recommendation is not applicable"
   fi
}
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1091	TA0001, TA0008	

1.7.10 Ensure XDMCP is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

Rationale:

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

Audit:

Run the following command and verify the output:

```
# grep -Eis '^\s*Enable\s*=\s*true' /etc/gdm/custom.conf

Nothing should be returned
```

Remediation:

Edit the file `/etc/gdm/custom.conf` and remove the line:

```
Enable=true
```

Default Value:

false (This is denoted by no Enabled= entry in the file `/etc/gdm/custom.conf` in the [xdmcp] section

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1056, T1056.001, T1557, T1557.000	TA0002	M1050

2 Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

2.1 Configure Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as NTP or chrony.

2.1.1 Ensure time synchronization is in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Note: If another method for time synchronization is being used, this section may be skipped.

Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

Run the following commands to verify that chrony is installed:

```
# rpm -q chrony

chrony-<version>
```

Remediation:

Run the following command to install `chrony`:

```
# yum install chrony
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

Additional Information:

On systems where host based time synchronization is not available, verify that chrony is installed.

On systems where host based time synchronization is available consult your documentation and verify that host based synchronization is in use.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.001	TA0005	M1022

2.1.2 Ensure chrony is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on `chrony` can be found at http://chrony.tuxfamily.org/. `chrony` can be configured to be a client and/or a server.

Rationale:

If `chrony` is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Audit:

Run the following command and verify remote server is configured properly:

```
# grep -Prs -- '^\h*(server|pool)\h+[^#\n\r]+' /etc/chrony.conf

server <remote-server>
```

Multiple servers may be configured.

Remediation:

Add or edit server or pool lines to `/etc/chrony.conf` as appropriate:
Example:

```
server <remote-server>
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

Additional Information:

On systems where host based time synchronization is not available, verify that `chrony` is installed.

On systems where host based time synchronization is available consult your documentation and verify that host based synchronization is in use.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0002	M1022

2.1.3 Ensure chrony is not run as the root user (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The file `/etc/sysconfig/chronyd` allows configuration of options for `chrony` to include the user `chrony` is run as. By default this is set to the user `chrony`

Rationale:

Services should not be set to run as the root user

Audit:

Run the following command to verify that `chrony` isn't configured to run as the `root` user:

```
# grep -Psi -- '^\h*OPTIONS=\"?\h+-u\h+root\b' /etc/sysconfig/chronyd

Nothing should be returned
```

Remediation:

Edit the file `/etc/sysconfig/chronyd` and add or modify the following line:

```
OPTIONS="-u chrony"
```

Run the following command to reload the `chronyd.service` configuration:

```
# systemctl try-reload-or-restart chronyd.service
```

Default Value:

OPTIONS="-u chrony"

2.2 Configure Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that the package be removed.

-IF- the package is required for a dependency:

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy
- Stop and mask the service and/or socket to reduce the potential attack surface

The following commands can be used to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service
# systemctl mask <service_name>.socket <service_name>.service
```

Note: This should not be considered a comprehensive list of services not required for normal system operation. You may wish to consider additions to those listed here for your environment

2.2.1 Ensure autofs services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

`autofs` allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

There may be packages that are dependent on the `autofs` package. If the `autofs` package is removed, these dependent packages will be removed as well. Before removing the `autofs` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `autofs.service` leaving the `autofs` package installed.

Audit:

As a preference `autofs` should not be installed unless other packages depend on it.
Run the following command to verify `autofs` is not installed:

```
# rpm -q autofs

package autofs is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `autofs.service` is not enabled:

```
# systemctl is-enabled autofs.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `autofs.service` is not active:

```
# systemctl is-active autofs.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `autofs.service` and remove `autofs` package:

```
# systemctl stop autofs.service
# yum remove autofs
```

-OR-
-IF- the `autofs` package is required as a dependency:
Run the following commands to stop and mask `autofs.service`:

```
# systemctl stop autofs.service
# systemctl mask autofs.service
```

References:

1. NIST SP 800-53 Rev. 5: SI-3, MP-7

Additional Information:

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 Disable Autorun and Autoplay for Removable Media Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	8.5 Configure Devices Not To Auto-run Content Configure devices to not auto-run content from removable media.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1203, T1203.000, T1211, T1211.000, T1212, T1212.000	TA0002	M1038

2.2.2 Ensure avahi daemon services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `avahi` package. If the `avahi` package is removed, these dependent packages will be removed as well. Before removing the `avahi` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `avahi-daemon.socket` and `avahi-daemon.service` leaving the `avahi` package installed.

Audit:

Run the following command to verify the `avahi` package is not installed:

```
# rpm -q avahi

package avahi is not installed
```

-OR-
-IF- the `avahi` package is required as a dependency:
Run the following command to verify `avahi-daemon.socket` and `avahi-daemon.service` are not enabled:

```
# systemctl is-enabled avahi-daemon.socket avahi-daemon.service 2>/dev/null |
grep 'enabled'

Nothing should be returned
```

Run the following command to verify `avahi-daemon.socket` and `avahi-daemon.service` are not active:

```
# systemctl is-active avahi-daemon.socket avahi-daemon.service 2>/dev/null |
grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `avahi-daemon.socket` and `avahi-daemon.service`, and remove the `avahi` package:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# yum remove avahi
```

-OR-
-IF- the `avahi` package is required as a dependency:
Run the following commands to stop and mask the `avahi-daemon.socket` and `avahi-daemon.service`:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# systemctl mask avahi-daemon.socket avahi-daemon.service
```

References:

1. NIST SP 800-53 Rev. 5: SI-4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.3 Ensure dhcp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. There are two versions of the DHCP protocol `DHCPv4` and `DHCPv6`. At startup the server may be started for one or the other via the `-4` or `-6` arguments.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that the `dhcp-server` package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `dhcp-server` package. If the `dhcp-server` package is removed, these dependent packages will be removed as well. Before removing the `dhcp-server` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `dhcpd.service` and `dhcpd6.service` leaving the `dhcp-server` package installed.

Audit:

Run the following command to verify `dhcp-server` is not installed:

```
# rpm -q dhcp

package dhcp is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `dhcpd.service` and `dhcpd6.service` are not enabled:

```
# systemctl is-enabled dhcpd.service dhcpd6.service 2>/dev/null | grep
'enabled'

Nothing should be returned
```

Run the following command to verify `dhcpd.service` and `dhcpd6.service` are not active:

```
# systemctl is-active dhcpd.service dhcpd6.service 2>/dev/null | grep
'^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `dhcpd.service` and `dhcpd6.service` and remove `dhcp` package:

```
# systemctl stop dhcpd.service dhcpd6.service
# yum remove dhcp
```

-OR-
-IF- the `dhcp` package is required as a dependency:
Run the following commands to stop and mask `dhcpd.service` and `dhcpd6.service`:

```
# systemctl stop dhcpd.service dhcpd6.service
# systemctl mask dhcpd.service dhcpd6.service
```

References:

1. dhcpd(8)
2. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.4 Ensure dns server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `bind` package. If the `bind` package is removed, these dependent packages will be removed as well. Before removing the `bind` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `named.service` leaving the `bind` package installed.

Audit:

Run one of the following commands to verify `bind` is not installed:

```
# rpm -q bind

package bind is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `named.service` is not enabled:

```
# systemctl is-enabled named.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `named.service` is not active:

```
# systemctl is-active named.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `named.service` and remove `bind` package:

```
# systemctl stop named.service
# yum remove bind
```

-OR-
-IF- the `bind` package is required as a dependency:
Run the following commands to stop and mask `named.service`:

```
# systemctl stop named.service
# systemctl mask named.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.5 Ensure dnsmasq services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dnsmasq` is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.

Rationale:

Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `dnsmasq` package. If the `dnsmasq` package is removed, these dependent packages will be removed as well. Before removing the `dnsmasq` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `dnsmasq.service` leaving the `dnsmasq` package installed.

Audit:

Run one of the following commands to verify `dnsmasq` is not installed:

```
# rpm -q dnsmasq

package dnsmasq is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `dnsmasq.service` is not enabled:

```
# systemctl is-enabled dnsmasq.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `dnsmasq.service` is not active:

```
# systemctl is-active dnsmasq.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `dnsmasq.service` and remove `dnsmasq` package:

```
# systemctl stop dnsmasq.service
# yum remove dnsmasq
```

-OR-
-IF- the `dnsmasq` package is required as a dependency:
Run the following commands to stop and mask the `dnsmasq.service`:

```
# systemctl stop dnsmasq.service
# systemctl mask dnsmasq.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.6 Ensure samba file server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this package can be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `samba` package. If the `samba` package is removed, these dependent packages will be removed as well. Before removing the `samba` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `smb.service` leaving the `samba` package installed.

Audit:

Run the following command to verify `samba` package is not installed:

```
# rpm -q samba

package samba is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `smb.service` is not enabled:

```
# systemctl is-enabled smb.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `smb.service` is not active:

```
# systemctl is-active smb.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following command to stop `smb.service` and remove `samba` package:

```
# systemctl stop smb.service
# yum remove samba
```

-OR-
-IF- the `samba` package is required as a dependency:
Run the following commands to stop and mask the `smb.service`:

```
# systemctl stop smb.service
# systemctl mask smb.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.7 Ensure ftp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

Rationale:

Unless there is a need to run the system as a FTP server, it is recommended that the package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the `vsftpd` package. If the `vsftpd` package is removed, these dependent packages will be removed as well. Before removing the `vsftpd` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `vsftpd.service` leaving the `vsftpd` package installed.

Audit:

Run the following command to verify `vsftpd` is not installed:

```
# rpm -q vsftpd

package vsftpd is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `vsftpd` service is not enabled:

```
# systemctl is-enabled vsftpd.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `vsftpd` service is not active:

```
# systemctl is-active vsftpd.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note:

- Other ftp server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `vsftpd.service` and remove `vsftpd` package:

```
# systemctl stop vsftpd.service
# yum remove vsftpd
```

-OR-
-IF- the `vsftpd` package is required as a dependency:
Run the following commands to stop and mask the `vsftpd.service`:

```
# systemctl stop vsftpd.service
# systemctl mask vsftpd.service
```

Note: Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.8 Ensure message access server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot` and `cyrus-imapd` are open source IMAP and POP3 server packages for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

Impact:

There may be packages that are dependent on `dovecot` and `cyrus-imapd` packages. If `dovecot` and `cyrus-imapd` packages are removed, these dependent packages will be removed as well. Before removing `dovecot` and `cyrus-imapd` packages, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask `dovecot.socket`, `dovecot.service` and `cyrus-imapd.service` leaving `dovecot` and `cyrus-imapd` packages installed.

Audit:

Run the following command to verify `dovecot` and `cyrus-imapd` are not installed:

```
# rpm -q dovecot cyrus-imapd

package dovecot is not installed
package cyrus-imapd is not installed
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to verify `dovecot.socket`, `dovecot.service`, and `cyrus-imapd.service` are not enabled:

```
# systemctl is-enabled dovecot.socket dovecot.service cyrus-imapd.service
2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify `dovecot.socket`, `dovecot.service`, and `cyrus-imapd.service` are not active:

```
# systemctl is-active dovecot.socket dovecot.service cyrus-imapd.service
2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `dovecot.socket`, `dovecot.service`, and `cyrus-imapd.service`, and remove `dovecot` and `cyrus-imapd` packages:

```
# systemctl stop dovecot.socket dovecot.service cyrus-imapd.service
# yum remove dovecot cyrus-imapd
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to stop and mask `dovecot.socket`, `dovecot.service`, and `cyrus-imapd.service`:

```
# systemctl stop dovecot.socket dovecot.service cyrus-imapd.service
# systemctl mask dovecot.socket dovecot.service cyrus-imapd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.9 Ensure network file system services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not require access to network shares or the ability to provide network file system services for other host's network shares, it is recommended that the `nfs-utils` package be removed to reduce the attack surface of the system.

Impact:

Many of the `libvirt` packages used by Enterprise Linux virtualization are dependent on the `nfs-utils` package. If the `nfs-utils` package is removed, these dependent packages will be removed as well. Before removing the `nfs-utils` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `nfs-server.service` leaving the `nfs-utils` package installed.

Audit:

Run the following command to verify `nfs-utils` is not installed:

```
# rpm -q nfs-utils

package nfs-utils is not installed
```

-OR- If package is required for dependencies:
Run the following command to verify that the `nfs-server.service` is not enabled:

```
# systemctl is-enabled nfs-server.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `nfs-server.service` is not active:

```
# systemctl is-active nfs-server.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following command to stop `nfs-server.service` and remove `nfs-utils` package:

```
# systemctl stop nfs-server.service
# yum remove nfs-utils
```

-OR-
-IF- the `nfs-utils` package is required as a dependency:
Run the following commands to stop and mask the `nfs-server.service`:

```
# systemctl stop nfs-server.service
# systemctl mask nfs-server.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

Additional Information:

Many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-utils package is required as a dependency, the nfs-server service should be disabled and masked to reduce the attack surface of the system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1210, T1210.000	TA0008	M1042

2.2.10 Ensure nis server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

There may be packages that are dependent on the `ypserv` package. If the `ypserv` package is removed, these dependent packages will be removed as well. Before removing the `ypserv` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `ypserv.service` leaving the `ypserv` package installed.

Audit:

Run the following command to verify `ypserv` is not installed:

```
# rpm -q ypserv

package ypserv is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `ypserv.service` is not enabled:

```
# systemctl is-enabled ypserv.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify `ypserv.service` is not active:

```
# systemctl is-active ypserv.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `ypserv.service` and remove `ypserv` package:

```
# systemctl stop ypserv.service
# yum remove ypserv
```

-OR-
-IF- the `ypserv` package is required as a dependency:
Run the following commands to stop and mask `ypserv.service`:

```
# systemctl stop ypserv.service
# systemctl mask ypserv.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.11 Ensure print server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

Impact:

Removing the cups package, or disabling `cups.socket` and/or `cups.service` will prevent printing from the system, a common task for workstation systems.

There may be packages that are dependent on the `cups` package. If the `cups` package is removed, these dependent packages will be removed as well. Before removing the `cups` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask `cups.socket` and `cups.service` leaving the `cups` package installed.

Audit:

Run the following command to verify `cups` is not installed:

```
# rpm -q cups

package cups is not installed
```

-OR-
-IF- the `cups` package is required as a dependency:
Run the following command to verify the `cups.socket` and `cups.service` are not enabled:

```
# systemctl is-enabled cups.socket cups.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `cups.socket` and `cups.service` are not active:

```
# systemctl is-active cups.socket cups.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `cups.socket` and `cups.service`, and remove the `cups` package:

```
# systemctl stop cups.socket cups.service
# yum remove cups
```

-OR-
-IF- the `cups` package is required as a dependency:
Run the following commands to stop and mask the `cups.socket` and `cups.service`:

```
# systemctl stop cups.socket cups.service
# systemctl mask cups.socket cups.service
```

References:

1. http://www.cups.org
2. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.12 Ensure rpcbind services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rpcbind` utility maps RPC services to the ports on which they listen. RPC processes notify `rpcbind` when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts `rpcbind` on the server with a particular RPC program number. The `rpcbind.service` redirects the client to the proper port number so it can communicate with the requested service.

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

Rationale:

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If `rpcbind` is not required, it is recommended to remove `rpcbind` package to reduce the potential attack surface.

Impact:

Many of the libvirt packages used by Enterprise Linux virtualization, and the `nfs-utils` package used for The Network File System (NFS), are dependent on the `rpcbind` package. If the `rpcbind` package is removed, these dependent packages will be removed as well. Before removing the `rpcbind` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `rpcbind.socket` and `rpcbind.service` leaving the `rpcbind` package installed.

Audit:

Run the following command to verify `rpcbind` package is not installed:

```
# rpm -q rpcbind

package rpcbind is not installed
```

-OR-
-IF- the `rpcbind` package is required as a dependency:
Run the following command to verify `rpcbind.socket` and `rpcbind.service` are not enabled:

```
# systemctl is-enabled rpcbind.socket rpcbind.service 2>/dev/null | grep
'enabled'

Nothing should be returned
```

Run the following command to verify `rpcbind.socket` and `rpcbind.service` are not active:

```
# systemctl is-active rpcbind.socket rpcbind.service 2>/dev/null | grep
'^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `rpcbind.socket` and `rpcbind.service`, and remove the `rpcbind` package:

```
# systemctl stop rpcbind.socket rpcbind.service
# yum remove rpcbind
```

-OR-
-IF- the `rpcbind` package is required as a dependency:
Run the following commands to stop and mask the `rpcbind.socket` and `rpcbind.service`:

```
# systemctl stop rpcbind.socket rpcbind.service
# systemctl mask rpcbind.socket rpcbind.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1498, T1498.002, T1543, T1543.002	TA0008	M1042

2.2.13 Ensure rsync services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyncd.service` can be used to synchronize files between systems over network links.

Rationale:

Unless required, the `rsync` package should be removed to reduce the potential attack surface.

The `rsyncd.service` presents a security risk as it uses unencrypted protocols for communication.

Impact:

There may be packages that are dependent on the `rsync` package. If the `rsync` package is removed, these dependent packages will be removed as well. Before removing the `rsync` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `rsyncd.socket` and `rsyncd.service` leaving the `rsync` package installed.

Audit:

Run the following command to verify the `rsync-daemon` package is not installed:

```
# rpm -q rsync

package rsync is not installed
```

-OR-
-IF- the `rsync` package is required as a dependency:
Run the following command to verify `rsyncd.socket` and `rsyncd.service` are not enabled:

```
# systemctl is-enabled rsyncd.socket rsyncd.service 2>/dev/null | grep
'enabled'

Nothing should be returned
```

Run the following command to verify `rsyncd.socket` and `rsyncd.service` are not active:

```
# systemctl is-active rsyncd.socket rsyncd.service 2>/dev/null | grep
'^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `rsyncd.socket` and `rsyncd.service`, and remove the `rsync` package:

```
# systemctl stop rsyncd.socket rsyncd.service
# yum remove rsync
```

-OR-
-IF- the `rsync` package is required as a dependency:
Run the following commands to stop and mask the `rsyncd.socket` and `rsyncd.service`:

```
# systemctl stop rsyncd.socket rsyncd.service
# systemctl mask rsyncd.socket rsyncd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1105, T1105.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002, T1570, T1570.000	TA0008	M1042

2.2.14 Ensure snmp services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using `SNMPv1`, which transmits data in the clear and does not require authentication to execute commands. `SNMPv3` replaces the simple/clear text password sharing used in `SNMPv2` with more securely encoded parameters. If the the SNMP service is not required, the `net-snmp` package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- The server should be configured for `SNMP v3` only. `User Authentication` and `Message Encryption` should be configured.
- If `SNMP v2` is **absolutely** necessary, modify the community strings' values.

Impact:

There may be packages that are dependent on the `net-snmp` package. If the `net-snmp` package is removed, these packages will be removed as well.

Before removing the `net-snmp` package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the `snmpd.service` leaving the `net-snmp` package installed.

Audit:

Run the following command to verify `net-snmp` package is not installed:

```
# rpm -q net-snmp

package net-snmp is not installed
```

-OR- If the package is required for dependencies:
Run the following command to verify the `snmpd.service` is not enabled:

```
# systemctl is-enabled snmpd.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `snmpd.service` is not active:

```
# systemctl is-active snmpd.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `snmpd.service` and remove `net-snmp` package:

```
# systemctl stop snmpd.service
# yum remove net-snmp
```

-OR- If the package is required for dependencies:
Run the following commands to stop and mask the `snmpd.service`:

```
# systemctl stop snmpd.service
# systemctl mask snmpd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.15 Ensure telnet server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `telnet-server` package contains the `telnet` daemon, which accepts connections from users from other systems via the `telnet` protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh` package provides an encrypted session and stronger security.

Impact:

There may be packages that are dependent on the `telnet-server` package. If the `telnet-server` package is removed, these dependent packages will be removed as well. Before removing the `telnet-server` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `telnet.socket` leaving the `telnet-server` package installed.

Audit:

Run the following command to verify the `telnet-server` package is not installed:

```
rpm -q telnet-server

package telnet-server is not installed
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following command to verify `telnet.socket` is not enabled:

```
# systemctl is-enabled telnet.socket 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify `telnet.socket` is not active:

```
# systemctl is-active telnet.socket 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `telnet.socket` and remove the `telnet-server` package:

```
# systemctl stop telnet.socket
# yum remove telnet-server
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to stop and mask `telnet.socket`:

```
# systemctl stop telnet.socket
# systemctl mask telnet.socket
```

References:

1. NIST SP 800-53 Rev. 5: CM-7, CM-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.16 Ensure tftp server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

Rationale:

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

Impact:

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

There may be packages that are dependent on the `tftp-server` package. If the `tftp-server` package is removed, these dependent packages will be removed as well. Before removing the `tftp-server` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `tftp.socket` and `tftp.service` leaving the `tftp-server` package installed.

Audit:

Run the following command to verify `tftp-server` is not installed:

```
# rpm -q tftp-server

package tftp-server is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `tftp.socket` and `tftp.service` are not enabled:

```
# systemctl is-enabled tftp.socket tftp.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `tftp.socket` and `tftp.service` are not active:

```
# systemctl is-active tftp.socket tftp.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `tftp.socket` and `tftp.service`, and remove the `tftp-server` package:

```
# systemctl stop tftp.socket tftp.service
# yum remove tftp-server
```

-OR-
-IF- the `tftp-server` package is required as a dependency:
Run the following commands to stop and mask `tftp.socket` and `tftp.service`:

```
# systemctl stop tftp.socket tftp.service
# systemctl mask tftp.socket tftp.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.17 Ensure web proxy server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Squid is a standard proxy server used in many distributions and environments.

Rationale:

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

Impact:

There may be packages that are dependent on the `squid` package. If the `squid` package is removed, these dependent packages will be removed as well. Before removing the `squid` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `squid.service` leaving the `squid` package installed.

Audit:

Run the following command to verify `squid` package is not installed:

```
# rpm -q squid

package squid is not installed
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `squid.service` is not enabled:

```
# systemctl is-enabled squid.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify the `squid.service` is not active:

```
# systemctl is-active squid.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `squid.service` and remove the `squid` package:

```
# systemctl stop squid.service
# yum remove squid
```

-OR- If the `squid` package is required as a dependency:
Run the following commands to stop and mask the `squid.service`:

```
# systemctl stop squid.service
# systemctl mask squid.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

Additional Information:

Several HTTP proxy servers exist. These and other services should be checked.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.18 Ensure web server services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Web servers provide the ability to host web site content.

Rationale:

Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

Impact:

Removal of web server packages will remove that ability for the server to host web services.

-IF- the web server package is required for a dependency, any related service or socket should be stopped and masked.

Note: If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

Audit:

Run the following command to verify `httpd` and `nginx` are not installed:

```
# rpm -q httpd nginx

package httpd is not installed
package nginx is not installed
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following command to verify `httpd.socket`, `httpd.service`, and `nginx.service` are not enabled:

```
# systemctl is-enabled httpd.socket httpd.service nginx.service 2>/dev/null |
grep 'enabled'

Nothing should be returned
```

Run the following command to verify `httpd.socket`, `httpd.service`, and `nginx.service` are not active:

```
# systemctl is-active httpd.socket httpd.service nginx.service 2>/dev/null |
grep '^active'

Nothing should be returned
```

Note:

- Other web server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `httpd.socket`, `httpd.service`, and `nginx.service`, and remove `httpd` and `nginx` packages:

```
# systemctl stop httpd.socket httpd.service nginx.service
# yum remove httpd nginx
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to stop and mask `httpd.socket`, `httpd.service`, and `nginx.service`:

```
# systemctl stop httpd.socket httpd.service nginx.service
# systemctl mask httpd.socket httpd.service nginx.service
```

Note: Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.19 Ensure xinetd services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The eXtended InterNET Daemon (`xinetd`) is an open source super daemon that replaced the original `inetd` daemon. The `xinetd` daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

Unless your organization specifically requires xinetd services, it is recommended that the package be removed to reduce the attack surface are of the system.

Impact:

There may be packages that are dependent on the `xinetd` package. If the `xinetd` package is removed, these dependent packages will be removed as well. Before removing the `xinetd` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the avahi-daemon.socket and avahi-daemon.service leaving the avahi package installed.

Audit:

Run the following command to verify the `xinetd` package is not installed:

```
# rpm -q xinetd

package xinetd is not installed
```

-OR-
-IF- the `xinetd` package is required as a dependency:
Run the following command to verify `xinetd.service` is not enabled:

```
# systemctl is-enabled xinetd.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify `xinetd.service` is not active:

```
# systemctl is-active xinetd.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `xinetd.service`, and remove the `xinetd` package:

```
# systemctl stop xinetd.service
# yum remove xinetd
```

-OR-
-IF- the `xinetd` package is required as a dependency:
Run the following commands to stop and mask the `xinetd.service`:

```
# systemctl stop xinetd.service
# systemctl mask xinetd.service
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.20 Ensure X window server services are not in use (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Impact:

If a Graphical Desktop Manager (GDM) is in use on the system, there may be a dependency on the `xorg-x11-server-common` package. If the GDM is required and approved by local site policy, the package should **not** be removed.

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime.

Audit:

-IF- a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:
Run the following command to Verify X Windows Server is not installed.

```
# rpm -q xorg-x11-server-common

package xorg-x11-server-common is not installed
```

Remediation:

-IF- a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:
Run the following command to remove the X Windows Server packages:

```
# yum remove xorg-x11-server-common
```

References:

1. NIST SP 800-53 Rev. 5: CM-11

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.2.21 Ensure mail transfer agents are configured for local-only mode (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Audit:

Run the following commands to verify that the MTA is not listening on any non-loopback address (`127.0.0.1` or `::1`)

```
#  ss -plntu | grep -P -- ':25\b' | grep -Pv --
'\h+(127\.0\.0\.1|\[?::1\]?):25\b'
#  ss -plntu | grep -P -- ':465\b' | grep -Pv --
'\h+(127\.0\.0\.1|\[?::1\]?):465\b'
#  ss -plntu | grep -P -- ':587\b' | grep -Pv --
'\h+(127\.0\.0\.1|\[?::1\]?):587\b'
```

Nothing should be returned

Remediation:

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart `postfix`:

```
# systemctl restart postfix
```

Note:

- This remediation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1018, T1018.000, T1210, T1210.000	TA0008	M1042

2.2.22 Ensure only approved services are listening on a network interface (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

Rationale:

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

Impact:

There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the `<service_name>.socket` and `<service_name>.service` leaving the service's package installed.

Audit:

Run the following command:

```
# ss -plntu
```

Review the output to ensure:

- All services listed are required on the system and approved by local site policy.
- Both the port and interface the service is listening on are approved by local site policy.
- If a listed service is not required:
  - Remove the package containing the service
  - **-IF-** the service's package is required for a dependency, stop and mask the service and/or socket

Remediation:

Run the following commands to stop the service and remove the package containing the service:

```
# systemctl stop <service_name>.socket <service_name>.service
# yum remove <package_name>
```

-OR- If required packages have a dependency:
Run the following commands to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service
# systemctl mask <service_name>.socket <service_name>.service
```

Note: replace `<service_name>` with the appropriate service name.

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1210, T1210.000, T1543, T1543.002	TA0008	M1042

2.3 Configure Service Clients

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

Note: This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

2.3.1 Ensure ftp client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

Audit:

Run the following command to verify `ftp` is not installed:

```
# rpm -q ftp

package ftp is not installed
```

Remediation:

Run the following command to remove `ftp`:

```
# yum remove ftp
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3.2 Ensure ldap client is not installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Audit:

Run the following command to verify that the `openldap-clients` package is not installed:

```
# rpm -q openldap-clients

package openldap-clients is not installed
```

Remediation:

Run the following command to remove the `openldap-clients` package:

```
# yum remove openldap-clients
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3.3 Ensure nis client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Run the following command to verify that the `ypbind` package is not installed:

```
# rpm -q ypbind

package ypbind is not installed
```

Remediation:

Run the following command to remove the ypbind package:

```
# yum remove ypbind
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

2.3.4 Ensure telnet client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Linux distributions.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Run the following command to verify that the `telnet` package is not installed:

```
# rpm -q telnet

package telnet is not installed
```

Remediation:

Run the following command to remove the `telnet` package:

```
# yum remove telnet
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1203, T1203.000, T1543, T1543.002	TA0006, TA0008	M1041, M1042

2.3.5 Ensure tftp client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

Rationale:

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

Audit:

Run the following command to verify `tftp` is not installed:

```
# rpm -q tftp

package tftp is not installed
```

Remediation:

Run the following command to remove `tftp`:

```
# yum remove tftp
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1203, T1203.000, T1543, T1543.002	TA0008	M1042

3 Network

This section provides guidance on for securing the network configuration of the system

3.1 Configure Network Devices

To reduce the attack surface of a system, unused devices should be disabled.

Note: This should not be considered a comprehensive list, you may wish to consider additions to those listed here for your environment.

3.1.1 Ensure IPv6 status is identified (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340 trillion3 addresses.

Features of IPv6

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

Rationale:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations.

-IF- dual stack and IPv6 are not used in your environment, IPv6 may be disabled to reduce the attack surface of the system, and recommendations pertaining to IPv6 can be skipped.

Note: It is recommended that IPv6 be enabled and configured unless this is against local site policy

Impact:

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

When enabled, IPv6 will require additional configuration to reduce risk to the system.

Audit:

Run the following to identify if IPv6 is enabled on the system:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Enable or disable IPv6 in accordance with system requirements and local site policy

Default Value:

IPv6 is enabled

References:

1. NIST SP 800-53 Rev. 5: CM-7

Additional Information:

Having more addresses has grown in importance with the expansion of smart devices and connectivity. IPv6 provides more than enough globally unique IP addresses for every networked device currently on the planet, helping ensure providers can keep pace with the expected proliferation of IP-based devices.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000, T1595, T1595.001, T1595.002	TA0008	M1042

3.1.2 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Wireless networking is used when wired networks are unavailable.

Rationale:

-IF- wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

Audit:

Run the following script to verify no wireless interfaces are active on the system:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   module_chk()
   {
      # Check how module will be loaded
      l_loadable="$(modprobe -n -v "$l_mname")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
      # Check is the module currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
      # Check if the module is deny listed
      if modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mname\b"; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pl --
"^\h*blacklist\h+$l_mname\b" /etc/modprobe.d/*)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
      l_dname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0
dirname); do basename "$(readlink -f "$driverdir"/device/driver/module)";done | sort -u)
      for l_mname in $l_dname; do
         module_chk
      done
   fi
   # Report results. If no failures output in l_output2, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **"
      if [ -z "$l_output" ]; then
         echo -e "\n - System has no wireless NICs installed"
      else
         echo -e "\n$l_output\n"
      fi
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable any wireless interfaces:

```
#!/usr/bin/env bash

{
   module_fix()
   {
      if ! modprobe -n -v "$l_mname" | grep -P -- '^\h*install
\/bin\/(true|false)'; then
         echo -e " - setting module: \"$l_mname\" to be un-loadable"
         echo -e "install $l_mname /bin/false" >>
/etc/modprobe.d/"$l_mname".conf
      fi
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e " - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
      if ! grep -Pq -- "^\h*blacklist\h+$l_mname\b" /etc/modprobe.d/*; then
         echo -e " - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf
      fi
   }
   if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
      l_dname=$(for driverdir in $(find /sys/class/net/*/ -type d -name
wireless | xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver/module)";done | sort -u)
      for l_mname in $l_dname; do
         module_fix
      done
   fi
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	15.4 Disable Wireless Access on Devices if Not Required Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	15.5 Limit Wireless Access on Client Devices Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1011, T1011.000, T1595, T1595.001, T1595.002	TA0010	M1028

3.1.3 Ensure bluetooth services are not in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

Rationale:

An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is `bluesnarfing`, which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

Impact:

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

There may be packages that are dependent on the `bluez` package. If the `bluez` package is removed, these dependent packages will be removed as well. Before removing the `bluez` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask `bluetooth.service` leaving the `bluez` package installed.

Audit:

Run the following command to verify the `bluez` package is not installed:

```
# rpm -q bluez

package bluez is not installed
```

-OR-
-IF- the `bluez` package is required as a dependency:
Run the following command to verify `bluetooth.service` is not enabled:

```
# systemctl is-enabled bluetooth.service 2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify `bluetooth.service` is not active:

```
# systemctl is-active bluetooth.service 2>/dev/null | grep '^active'

Nothing should be returned
```

Note: If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

Remediation:

Run the following commands to stop `bluetooth.service`, and remove the `bluez` package:

```
# systemctl stop bluetooth.service
# yum remove bluez
```

-OR-
-IF- the `bluez` package is required as a dependency:
Run the following commands to stop and mask `bluetooth.service`:

```
# systemctl stop bluetooth.service
# systemctl mask bluetooth.service
```

Note: A reboot may be required

References:

1. https://www.cisa.gov/tips/st05-015
2. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1011, T1011.001	TA0010	M1042

3.2 Configure Network Kernel Modules

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

3.2.1 Ensure dccp kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

Rationale:

-IF- the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Audit:

Run the following script to verify the `dccp` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="dccp" # set module name
   l_mtype="net" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `dccp` module:
-IF- the module is available in the running kernel:

- Create a file with `install dccp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist dccp` in the `/etc/modprobe.d/` directory
- Unload `dccp` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist dccp` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="dccp" # set module name
   l_mtype="net" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

3.2.2 Ensure tipc kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

Rationale:

-IF- the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following script to verify the `tipc` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="tipc" # set module name
   l_mtype="net" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `tipc` module:
-IF- the module is available in the running kernel:

- Create a file with `install tipc /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist tipc` in the `/etc/modprobe.d/` directory
- Unload `tipc` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist tipc` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="tipc" # set module name
   l_mtype="net" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

3.2.3 Ensure rds kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.

Rationale:

-IF- the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following script to verify the `rds` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="rds" # set module name
   l_mtype="net" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `rds` module:
-IF- the module is available in the running kernel:

- Create a file with `install rds /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist rds` in the `/etc/modprobe.d/` directory
- Unload `rds` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist rds` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="rds" # set module name
   l_mtype="net" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

3.2.4 Ensure sctp kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

Rationale:

-IF- the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Run the following script to verify the `sctp` module is disabled:
-IF- the module is available in the running kernel:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the kernel

-IF- available in ANY installed kernel:

- The module is deny listed in a file within the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system, or pre-compiled into the kernel:

- No additional configuration is necessary

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3="" l_dl="" # Unset output variables
   l_mname="sctp" # set module name
   l_mtype="net" # set module type
   l_searchloc="/lib/modprobe.d/*.conf /usr/local/lib/modprobe.d/*.conf /run/modprobe.d/*.conf
/etc/modprobe.d/*.conf"
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_chk()
   {
      # Check if the module is currently loadable
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         l_output="$l_output\n - module: \"$l_mname\" is not loadable: \"$l_loadable\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loadable: \"$l_loadable\""
      fi
   }
   module_loaded_chk()
   {
      # Check if the module is currently loaded
      if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
         l_output="$l_output\n - module: \"$l_mname\" is not loaded"
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
      fi
   }
   module_deny_chk()
   {
      # Check if the module is deny listed
      l_dl="y"
      if modprobe --showconfig | grep -Pq -- '^\h*blacklist\h+'"$l_mpname"'\b'; then
         l_output="$l_output\n - module: \"$l_mname\" is deny listed in: \"$(grep -Pls --
"^\h*blacklist\h+$l_mname\b" $l_searchloc)\""
      else
         l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         l_output3="$l_output3\n  - \"$l_mdir\""
         [ "$l_dl" != "y" ] && module_deny_chk
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_chk
            module_loaded_chk
         fi
      else
         l_output="$l_output\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\""
      fi
   done
   # Report results. If no failures output in l_output2, we pass
   [ -n "$l_output3" ] && echo -e "\n\n -- INFO --\n - module: \"$l_mname\" exists in:$l_output3"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to disable the `sctp` module:
-IF- the module is available in the running kernel:

- Create a file with `install sctp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file with `blacklist sctp` in the `/etc/modprobe.d/` directory
- Unload `sctp` from the kernel

-IF- available in ANY installed kernel:

- Create a file with `blacklist sctp` in the `/etc/modprobe.d/` directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

- No remediation is necessary

```
#!/usr/bin/env bash

{
   l_mname="sctp" # set module name
   l_mtype="net" # set module type
   l_mpath="/lib/modules/**/kernel/$l_mtype"
   l_mpname="$(tr '-' '_' <<< "$l_mname")"
   l_mndir="$(tr '-' '/' <<< "$l_mname")"

   module_loadable_fix()
   {
      # If the module is currently loadable, add "install {MODULE_NAME} /bin/false" to a file in
"/etc/modprobe.d"
      l_loadable="$(modprobe -n -v "$l_mname")"
      [ "$(wc -l <<< "$l_loadable")" -gt "1" ] && l_loadable="$(grep -P --
"(^\h*install|\b$l_mname)\b" <<< "$l_loadable")"
      if ! grep -Pq -- '^\h*install \/bin\/(true|false)' <<< "$l_loadable"; then
         echo -e "\n - setting module: \"$l_mname\" to be not loadable"
         echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   module_loaded_fix()
   {
      # If the module is currently loaded, unload the module
      if lsmod | grep "$l_mname" > /dev/null 2>&1; then
         echo -e "\n - unloading module \"$l_mname\""
         modprobe -r "$l_mname"
      fi
   }
   module_deny_fix()
   {
      # If the module isn't deny listed, denylist the module
      if ! modprobe --showconfig | grep -Pq -- "^\h*blacklist\h+$l_mpname\b"; then
         echo -e "\n - deny listing \"$l_mname\""
         echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mpname".conf
      fi
   }
   # Check if the module exists on the system
   for l_mdir in $l_mpath; do
      if [ -d "$l_mdir/$l_mndir" ] && [ -n "$(ls -A $l_mdir/$l_mndir)" ]; then
         echo -e "\n - module: \"$l_mname\" exists in \"$l_mdir\"\n - checking if disabled..."
         module_deny_fix
         if [ "$l_mdir" = "/lib/modules/$(uname -r)/kernel/$l_mtype" ]; then
            module_loadable_fix
            module_loaded_fix
         fi
      else
         echo -e "\n - module: \"$l_mname\" doesn't exist in \"$l_mdir\"\n"
      fi
   done
   echo -e "\n - remediation of module: \"$l_mname\" complete\n"
}
```

References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068, T1068.000, T1210, T1210.000	TA0008	M1042

3.3 Configure Network Kernel Parameters

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

Note:

- sysctl settings are defined through files in `/usr/local/lib`, `/usr/lib/`, `/lib/`, `/run/`, and `/etc/`
- Files are typically placed in the `sysctl.d` directory within the parent directory
- The paths where sysctl preload files usually exist
    - `/run/sysctl.d/*.conf`
    - `/etc/sysctl.d/*.conf`
    - `/usr/local/lib/sysctl.d/*.conf`
    - `/usr/lib/sysctl.d/*.conf`
    - `/lib/sysctl.d/*.conf`
    - `/etc/sysctl.conf`
- Files must have the "`.conf`" extension
- Vendors settings usually live in `/usr/lib/` or `/usr/local/lib/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
    - Entries listed latter in the file take precedence over the same settings listed earlier in the file
    - Files containing kernel parameters that are over-ridden by other files with the same name will not be listed
    - On systems running UncomplicatedFirewall, the kernel parameters may be set or over-written. This will not be visible in the output of the command
- On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`
    - The settings in `/etc/ufw/sysctl.conf` will override settings other settings
    - This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

3.3.1 Ensure ip forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` to `0` ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Impact:

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

Many Cloud Service Provider (CSP) hosted systems require IP forwarding to be enabled. If the system is running on a CSP platform, this requirement should be reviewed before disabling IP forwarding.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.ip_forward` is set to `0`
- `net.ipv6.conf.all.forwarding` is set to `0`

Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.ip_forward=0" "net.ipv6.conf.all.forwarding=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.ip_forward = 0`

Example:

```
# printf '%s\n' "net.ipv4.ip_forward = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.ip_forward=0
   sysctl -w net.ipv4.route.flush=1
}
```

-IF- IPv6 is enabled on the system:
Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.forwarding = 0`

Example:

```
# printf '%s\n' "net.ipv6.conf.all.forwarding = 0" >> /etc/sysctl.d/60-
netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv6.conf.all.forwarding=0
   sysctl -w net.ipv6.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

3.3.2 Ensure packet redirect sending is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Impact:

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.send_redirects` is set to `0`
- `net.ipv4.conf.default.send_redirects` is set to `0`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.send_redirects=0"
"net.ipv4.conf.default.send_redirects=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
```

```
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.send_redirects = 0`
- `net.ipv4.conf.default.send_redirects = 0`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.send_redirects = 0"
"net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.send_redirects=0
   sysctl -w net.ipv4.conf.default.send_redirects=0
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

3.3.3 Ensure bogus icmp responses are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting `net.ipv4.icmp_ignore_bogus_error_responses` to `1` prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_ignore_bogus_error_responses` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.icmp_ignore_bogus_error_responses=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.icmp_ignore_bogus_error_responses = 1`

Example:

```
# printf '%s\n' "net.ipv4.icmp_ignore_bogus_error_responses = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.icmp_ignore_bogus_error_responses = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1053

3.3.4 Ensure broadcast icmp requests are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting `net.ipv4.icmp_echo_ignore_broadcasts` to `1` will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_echo_ignore_broadcasts` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.icmp_echo_ignore_broadcasts=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.icmp_echo_ignore_broadcasts = 1`

Example:

```
# printf '%s\n' "net.ipv4.icmp_echo_ignore_broadcasts = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.default.log_martians = 0

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1498, T1498.001	TA0040	M1037

3.3.5 Ensure icmp redirects are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

Rationale:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects`, `net.ipv4.conf.default.accept_redirects`, `net.ipv6.conf.all.accept_redirects`, and `net.ipv6.conf.default.accept_redirects` to `0`, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.accept_redirects` is set to `0`
- `net.ipv4.conf.default.accept_redirects` is set to `0`
- `net.ipv6.conf.all.accept_redirects` is set to `0`
- `net.ipv6.conf.default.accept_redirects` is set to `0`

Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.accept_redirects=0"
"net.ipv4.conf.default.accept_redirects=0"
"net.ipv6.conf.all.accept_redirects=0"
"net.ipv6.conf.default.accept_redirects=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
```

```
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.accept_redirects = 0`
- `net.ipv4.conf.default.accept_redirects = 0`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.accept_redirects = 0"
"net.ipv4.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.accept_redirects=0
   sysctl -w net.ipv4.conf.default.accept_redirects=0
   sysctl -w net.ipv4.route.flush=1
}
```

-IF- IPv6 is enabled on the system:
Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_redirects = 0`
- `net.ipv6.conf.default.accept_redirects = 0`

Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_redirects = 0"
"net.ipv6.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-
netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv6.conf.all.accept_redirects=0
   sysctl -w net.ipv6.conf.default.accept_redirects=0
   sysctl -w net.ipv6.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

3.3.6 Ensure secure icmp redirects are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` and `net.ipv4.conf.default.secure_redirects` to `0` protects the system from routing table updates by possibly compromised known gateways.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.secure_redirects` is set to `0`
- `net.ipv4.conf.default.secure_redirects` is set to `0`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.secure_redirects=0"
"net.ipv4.conf.default.secure_redirects=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
```

```
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.secure_redirects = 0`
- `net.ipv4.conf.default.secure_redirects = 0`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.secure_redirects = 0"
"net.ipv4.conf.default.secure_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.secure_redirects=0
   sysctl -w net.ipv4.conf.default.secure_redirects=0
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0009	M1030, M1042

3.3.7 Ensure reverse path filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.rp_filter` is set to `1`
- `net.ipv4.conf.default.rp_filter` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.rp_filter=1"
"net.ipv4.conf.default.rp_filter=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
```

```
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.rp_filter = 1`
- `net.ipv4.conf.default.rp_filter = 1`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.rp_filter = 1"
"net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.rp_filter=1
   sysctl -w net.ipv4.conf.default.rp_filter=1
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1498, T1498.001	TA0006, TA0040	M1030, M1042

3.3.8 Ensure source routed packets are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting `net.ipv4.conf.all.accept_source_route`, `net.ipv4.conf.default.accept_source_route`, `net.ipv6.conf.all.accept_source_route` and `net.ipv6.conf.default.accept_source_route` to `0` disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.accept_source_route` is set to `0`
- `net.ipv4.conf.default.accept_source_route` is set to `0`
- `net.ipv6.conf.all.accept_source_route` is set to `0`
- `net.ipv6.conf.default.accept_source_route` is set to `0`

Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.accept_source_route=0"
"net.ipv4.conf.default.accept_source_route=0"
"net.ipv6.conf.all.accept_source_route=0"
"net.ipv6.conf.default.accept_source_route=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
```

```
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.accept_source_route = 0`
- `net.ipv4.conf.default.accept_source_route = 0`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.accept_source_route = 0"
"net.ipv4.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.accept_source_route=0
   sysctl -w net.ipv4.conf.default.accept_source_route=0
   sysctl -w net.ipv4.route.flush=1
}
```

-IF- IPv6 is enabled on the system:
Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_source_route = 0`
- `net.ipv6.conf.default.accept_source_route = 0`

Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_source_route = 0"
"net.ipv6.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-
netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv6.conf.all.accept_source_route=0
   sysctl -w net.ipv6.conf.default.accept_source_route=0
   sysctl -w net.ipv6.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1590, T1590.005	TA0007	

3.3.9 Ensure suspicious packets are logged (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Setting `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians to 1` enables this feature. Logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.log_martians` is set to `1`
- `net.ipv4.conf.default.log_martians` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.conf.all.log_martians=1"
"net.ipv4.conf.default.log_martians=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
```

```
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`

Example:

```
# printf '%s\n' "net.ipv4.conf.all.log_martians = 1"
"net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.conf.all.log_martians=1
   sysctl -w net.ipv4.conf.default.log_martians=1
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

References:

1. NIST SP 800-53 Rev. 5: AU-3

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

3.3.10 Ensure tcp syn cookies is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting `net.ipv4.tcp_syncookies` to `1` enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.tcp_syncookies` is set to `1`

Note: kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv4.tcp_syncookies=1")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
then
```

```
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.tcp_syncookies = 1`

Example:

```
# printf '%s\n' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv4.tcp_syncookies=1
   sysctl -w net.ipv4.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv4.tcp_syncookies = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0040	M1037

3.3.11 Ensure ipv6 router advertisements are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. Setting `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` to `0` disables the system's ability to accept IPv6 router advertisements.

Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv6.conf.all.accept_ra` is set to `0`
- `net.ipv6.conf.default.accept_ra` is set to `0`

Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_parlist=("net.ipv6.conf.all.accept_ra=0"
"net.ipv6.conf.default.accept_ra=0")
   l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
   a_searchpath=("/run/sysctl.d/" "/etc/sysctl.d/" "/usr/local/lib/sysctl.d/"
"/usr/lib/sysctl.d/" "/lib/sysctl.d/")
   unset A_files
   declare -A A_files # Array of "valid" files
   A_files+=(["sysctl.conf"]="/etc/sysctl.conf")
   for l_searchpath in "${a_searchpath[@]}"; do
      if [ -d "$l_searchpath" ]; then
         while IFS= read -r -d $'\0' l_filename; do
            if [ -f "$l_filename" ]; then
               l_basename="$(basename "$l_filename")"
               if [ -z "${A_files["$l_basename"]}" ]; then
                  A_files+=(["$l_basename"]="$l_filename")
               fi
            fi
         done < <(find "$l_searchpath" -type f -name '*.conf' -print0)
      fi
   done
   a_sorted=()
   while IFS= read -rd '' l_key; do
      a_sorted+=( "$l_key" )
   done < <(printf '%s\0' "${!A_files[@]}" | sort -rz)
   kernel_parameter_chk()
   {
      l_var="" l_var2=""
      l_krp="$(sysctl "$l_kpname" | awk -F= '{print $2}' | xargs)" # Check
running configuration
      if [ "$l_krp" = "$l_kpvalue" ]; then
         l_output="$l_output\n - \"$l_kpname\" is correctly set to \"$l_krp\"
in the running configuration"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set to
\"$l_krp\" in the running configuration and should have a value of:
\"$l_kpvalue\""
      fi
      if [ -n "$l_ufwscf" ]; then # Check UFW kernel parameter file first
         if grep -Pqs -- "^\h*$l_kpname\b" "$l_$l_ufwscf"; then
            l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" "$l_$l_ufwscf"
| tail -n 1)"
         fi
      fi
      if grep -Pqs -- "^\h*$l_kpname\b" /etc/sysctl.conf; then # Check
/etc/sysctl.conf parameter file next
         l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b" /etc/sysctl.conf |
tail -n 1)"
      fi
      if [ -z "$l_var" ]; then # If non found yet, now we loop find actual
conf file parameter setting based on presence
         for l_keyname in "${a_sorted[@]}";do
            if grep -Pqs -- "^\h*$l_kpname\b" "${A_files["$l_keyname"]}";
```

```
then
               l_var="$(grep -PHo -- "^\h*$l_kpname\h*=\h*\H+\b"
"${A_files["$l_keyname"]}" | tail -n 1)"
               break
            fi
         done
      fi
      if [ -n "$l_var" ]; then
         while IFS=":" read -r l_conf_file l_var2; do
            while IFS="=" read -r l_fkpname l_fkpvalue; do
            l_fkpname="${l_fkpname// /}"; l_fkpvalue="${l_fkpvalue// /}"
               if [ "$l_fkpvalue" = "$l_kpvalue" ]; then
                  l_output="$l_output\n - \"$l_kpname\" is correctly set to
\"$l_fkpvalue\" in \"$l_conf_file\"\n"
               else
                  l_output2="$l_output2\n - \"$l_kpname\" is incorrectly set
to \"$l_fkpvalue\" in \"$l_conf_file\" and should have a value of:
\"$l_kpvalue\"\n"
               fi
            done <<< "$l_var2"
         done <<< "$l_var"
      else
         l_output2="$l_output2\n - \"$l_kpname\" is not set in an included
file\n   ** Note: \"$l_kpname\" May be set in a file that's ignored by load
procedure **\n"
      fi
   }
   while IFS="=" read -r l_kpname l_kpvalue; do # Assess and check parameters
      l_kpname="${l_kpname// /}"; l_kpvalue="${l_kpvalue// /}"
      if ! grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && grep -q
'^net.ipv6.' <<< "$l_kpname"; then
         l_output="$l_output\n - IPv6 is disabled on the system,
\"$l_kpname\" is not applicable"
      else
         kernel_parameter_chk
      fi
   done < <(printf '%s\n' "${a_parlist[@]}")
   unset A_files; unset a_sorted # Remove arrays
   if [ -z "$l_output2" ]; then # Provide output from checks
      echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
   fi
}
```

Remediation:

-IF- IPv6 is enabled on the system:
Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_ra = 0`
- `net.ipv6.conf.default.accept_ra = 0`

Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_ra = 0"
"net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl -w net.ipv6.conf.all.accept_ra=0
   sysctl -w net.ipv6.conf.default.accept_ra=0
   sysctl -w net.ipv6.route.flush=1
}
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

References:

1. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0006, TA0040	M1030, M1042

3.4 Configure Host Based Firewall

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through

To provide a Host Based Firewall, the Linux kernel includes support for:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem. **Is available in Linux kernels 3.13 and newer**.

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- FirewallD - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules.

Note:

- Only **one** method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.
- This section is intended only to ensure the resulting firewall rules are in place, not how they are configured.

3.4.1 Configure firewall utility

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- `FirewallD:`
  - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
  - Use the firewalld utility for simple firewall use cases. The utility is easy to use and covers the typical use cases for these scenarios.
- `NFTables:`
  - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
  - Use the nftables utility to set up complex and performance critical firewalls, such as for a whole network.
- `IPTables services:`
  - The iptables-services package contains the iptables service and the ip6tables service.
  - With the iptables service, every single change means flushing all the old rules and reading all the new rules from `/etc/sysconfig/iptables`

CAUTION: Only **one** method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.

3.4.1.1 Ensure iptables is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall

Rationale:

IPTables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Impact:

Changing firewall settings while connected over the network can result in being locked out of the system.

Audit:

Run the following command to verify that `iptables` is installed:

```
# rpm -q iptables

iptables-<version>
```

Remediation:

Run the following command to install `nftables`

```
# yum install nftables
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.1.2 Ensure a single firewall configuration utility is in use (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

FirewallD - Is a firewall service daemon that provides a dynamic customizable host-based firewall with a D-Bus interface. Being dynamic, it enables creating, changing, and deleting the rules without the necessity to restart the firewall daemon each time the rules are changed

NFTables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel

IPTables Services - Contains the iptables service and the ip6tables service which store their configurations in `/etc/sysconfig/iptables` and `/etc/sysconfig/ip6tables`

Note: firewalld with nftables backend does not support passing custom nftables rules to firewalld, using the `--direct` option.

Rationale:

In order to configure firewall rules, a firewall utility needs to be installed and active of the system. The use of more than one firewall utility may produce unexpected results.

Audit:

Run the following script to verify that a single firewall utility is in use on the system:

```
#!/usr/bin/env bash

{
   l_output=""
   if rpm -q firewalld &>/dev/null; then
      l_output="$l_output\n - FirewallD is installed"
      if systemctl is-enabled firewalld.service | grep -q '^enabled'; then
         l_output="$l_output\n   - firewalld.service is enabled"
      else
         l_output="$l_output\n   - firewalld.service is not enabled"
      fi
      if systemctl is-active firewalld.service | grep -q '^active'; then
         l_output="$l_output\n   - firewalld.service is active"
      else
         l_output="$l_output\n   - firewalld.service is not active"
      fi
   else
      l_output="$l_output\n - FirewallD is not installed"
   fi
   if rpm -q nftables &>/dev/null; then
      l_output="$l_output\n - nftables is installed"
      if systemctl is-enabled nftables.service | grep -q '^enabled'; then
         l_output="$l_output\n   - nftables.service is enabled"
      else
         l_output="$l_output\n   - nftables.service is not enabled"
      fi
      if systemctl is-active nftables.service | grep -q '^active'; then
         l_output="$l_output\n   - nftables.service is active"
      else
         l_output="$l_output\n   - nftables.service is not active"
      fi
   else
      l_output="$l_output\n - nftables is not installed"
   fi
   if rpm -q iptables-services &>/dev/null; then
      l_output="$l_output\n - iptables-services is installed"
      if systemctl is-enabled iptables.service | grep -q '^enabled'; then
         l_output="$l_output\n   - iptables.service is enabled"
      else
         l_output="$l_output\n   - iptables.service is not enabled"
      fi
      if systemctl is-active iptables.service | grep -q '^active'; then
         l_output="$l_output\n   - iptables.service is active"
      else
         l_output="$l_output\n   - iptables.service is not active"
      fi
      if grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable; then
         if systemctl is-enabled ip6tables.service | grep -q '^enabled'; then
            l_output="$l_output\n   - ip6tables.service is enabled"
         else
            l_output="$l_output\n   - ip6tables.service is not enabled"
         fi
         if systemctl is-active ip6tables.service | grep -q '^active'; then
            l_output="$l_output\n   - ip6tables.service is active"
         else
            l_output="$l_output\n   - ip6tables.service is not active"
         fi
      fi
   else
      l_output="$l_output\n - iptables-services is not installed"
   fi
   echo -e "$l_output"
}
```

Review the output and verify that one, and only one utilities' service(s) are enabled and active
Example output for a system using FirewallD:

```
 - FirewallD is installed
   - firewalld.service is enabled
   - firewalld.service is active
 - nftables is installed
   - nftables.service is not enabled
   - nftables.service is not active
 - iptables-services is installed
   - iptables.service is not enabled
   - iptables.service is not active
   - ip6tables.service is not enabled
   - ip6tables.service is not active
```

Note: In the example both nftables and iptables are not enabled and not active. Not installed is also acceptable for the utilities that are not being used

Remediation:

Determine which firewall utility to use in your environment. Ensure it also follows local site policy, and follow the guidance for that option:
OPTION 1 - FirewallD:
Run the following command to uninstall `nftables` and `iptables-services`

```
# yum remove nftables iptables-services
```

- OR - If the package is required for a dependency and is authorized by local sight policy, run the following commands to stop and mask `nftables.service`, `iptables.service`, and `ip6tables.service`:

```
# systemctl stop nftables.service iptables.service ip6tables.service
# systemctl mask nftables.service iptables.service ip6tables.service
```

Follow the guidance in subsection "Configure firewalld. Skip sections "Configure nftables" and "Configure iptables"
OPTION 2 - NFTables:
Run the following command to uninstall `firewalld` and `iptables-services`

```
# yum remove firewalld iptables-services
```

- OR - If the package is required for a dependency and is authorized by local sight policy, run the following commands to stop and mask `firewalld.service`, `iptables.service`, and `ip6tables.service`:

```
# systemctl stop firewalld.service iptables.service ip6tables.service
# systemctl mask firewalld.service iptables.service ip6tables.service
```

Follow the guidance in subsection "Configure nftables". Skip sections "Configure firewalld" and "Configure iptables"

OPTION 3 - IPTables:
Run the following command to uninstall `nftables` and `iptables-services`

```
# yum remove firewalld nftables
```

- OR - If the package is required for a dependency and is authorized by local sight policy, run the following commands to stop and mask `firewalld.service` and `nftables.service`:

```
# systemctl stop firewalld.service nftables.service
# systemctl mask firewalld.service nftables.service
```

Follow the guidance in subsection "Configure iptables" skip sections "Configure firewalld" and "Configure nftables"

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.2 Configure firewalld

CAUTION: - IF - nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options. It also provides an interface for services or applications to add iptables, ip6tables and ebtables rules directly. This interface can also be used by advanced users.

In the v0.6.0 release, firewalld gained support for using nftables as a firewall back-end.

The following example will create a FirewallD Zone called `securezone` to implement the firewall rules of this section leveraging the firewalld utility included with the firewalld package. This example will open port 22(ssh) from anywhere. Opening service `SSH` should be updated in accordance with local site policy. If another name for the zone is preferred, replace `securezone` with the name to be used.

Sample FirewallD securezone zone xml file

```
<?xml version="1.0" encoding="utf-8"?>
<zone target="DROP">
  <short>securezone</short>
  <description>For use with CIS Linux Benchmark. You do not trust the other
computers on networks to not harm your computer. Only selected incoming
connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <icmp-block name="destination-unreachable"/>
  <icmp-block name="packet-too-big"/>
  <icmp-block name="time-exceeded"/>
  <icmp-block name="parameter-problem"/>
  <icmp-block name="neighbour-advertisement"/>
  <icmp-block name="neighbour-solicitation"/>
  <icmp-block name="router-advertisement"/>
  <icmp-block name="router-solicitation"/>
  <rule family="ipv4">
    <source address="127.0.0.1"/>
    <destination address="127.0.0.1" invert="True"/>
    <drop/>
  </rule>
  <rule family="ipv6">
    <source address="::1"/>
    <destination address="::1" invert="True"/>
    <drop/>
  </rule>
  <icmp-block-inversion/>
</zone>
```

To use this zone, save this as `/etc/firewalld/zones/securezone.xml` and run the following commands:

```
# firewall-cmd --reload
# firewall-cmd --permanent --zone=securezone --change-interface={NAME OF
NETWORK INTERFACE}
```

To make this zone the default zone, runt the following command:

```
# firewall-cmd --set-default-zone=securezone
```

Note: Configuration of a live system's firewall directly over a remote connection will often result in being locked out.

3.4.2.1 Ensure firewalld is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewalld is a firewall management tool for Linux operating systems. It provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend or provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables utility.

firewalld replaces iptables as the default firewall management tool. Use the firewalld utility to configure a firewall for less complex firewalls. The utility is easy to use and covers the typical use cases scenario. FirewallD supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.

Note: Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program.

Rationale:

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Note: Only **one** firewall utility should be installed and configured. `FirewallD` is dependent on the `iptables` package.

Impact:

Changing firewall settings while connected over the network can result in being locked out of the system.

Audit:

Run the following command to verify that `FirewallD` and `iptables` are installed:

```
# rpm -q firewalld iptables

firewalld-<version>
iptables-<version>
```

Remediation:

Run the following command to install `FirewallD` and `iptables`:

```
# yum install firewalld iptables
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.2.2 Ensure firewalld service enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`firewalld.service` enables the enforcement of firewall rules configured through `firewalld`

Rationale:

Ensure that the `firewalld.service` is enabled and running to enforce firewall rules configured through `firewalld`

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command to verify that `firewalld` is enabled:

```
# systemctl is-enabled firewalld

enabled
```

Run the following command to verify that `firewalld` is running

```
# firewall-cmd --state

running
```

Remediation:

Run the following command to unmask `firewalld`

```
# systemctl unmask firewalld
```

Run the following command to enable and start `firewalld`

```
# systemctl --now enable firewalld
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.2.3 Ensure firewalld drops unnecessary services and ports (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Services and ports can be accepted or explicitly rejected or dropped by a zone.

For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

- ACCEPT - you accept all incoming packets except those disabled by a specific rule.
- REJECT - you disable all incoming packets except those that you have allowed in specific rules and the source machine is informed about the rejection.
- DROP - you disable all incoming packets except those that you have allowed in specific rules and no information sent to the source machine.

Rationale:

To reduce the attack surface of a system, all services and ports should be blocked unless required

Audit:

Run the following command and review output to ensure that listed services and ports follow site policy.

```
# systemctl is-enabled firewalld.service | grep -q 'enabled' && firewall-cmd
--list-all --zone="$(firewall-cmd --list-all | awk '/\(active\)/ { print $1
}')" | grep -P -- '^\h*(services:|ports:)'
```

Remediation:

If Firewalld is in use on the system:
Run the following command to remove an unnecessary service:

```
# firewall-cmd --remove-service=<service>
```

Example:

```
# firewall-cmd --remove-service=cockpit
```

Run the following command to remove an unnecessary port:

```
# firewall-cmd --remove-port=<port-number>/<port-type>
```

Example:

```
# firewall-cmd --remove-port=25/tcp
```

Run the following command to make new settings persistent:

```
# firewall-cmd --runtime-to-permanent
```

References:

1. firewalld.service(5)
2. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring-firewalls_securing-networks
3. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.4.2.4 Ensure network interfaces are assigned to appropriate zone (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewall zones define the trust level of network connections or interfaces.

Rationale:

A network interface not assigned to the appropriate zone can allow unexpected or undesired network traffic to be accepted on the interface.

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following and verify that the interface(s) follow site policy for zone assignment

```
# find /sys/class/net/* -maxdepth 1 | awk -F"/" '{print $NF}' | while read -r
netint; do [ "$netint" != "lo" ] && firewall-cmd --get-active-zones | grep -
B1 $netint; done
```

Example output:

```
<custom zone>
   eth0
```

Remediation:

Run the following command to assign an interface to the approprate zone.

```
# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>
```

Example:

```
# firewall-cmd --zone=customezone --change-interface=eth0
```

Default Value:

default zone defined in the firewalld configuration

References:

1. https://firewalld.org/documentation/zone/connections-interfaces-and-sources.html
2. NIST SP 800-53 Rev. 5: CA-9, SC-7

Additional Information:

The firewall in the Linux kernel is not able to handle network connections with the name shown by NetworkManager, it can only handle the network interfaces used by the connection. Because of this NetworkManager tells firewalld to assign the network interface that is used for this connection to the zone defined in the configuration of that connection. This assignment happens before the interface is used. The configuration of the connection can either be the NetworkManager configuration or also an `ifcfg`.

Example: If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration. If a connection has more than one interface, all of them will be supplied to firewalld. Also changes in the names of interfaces will be handled by NetworkManager and supplied to firewalld.

If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	M1031, M1037

3.4.3 Configure nftables

If firewalld or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. It is available in Linux kernels >= 3.13. **Please ensure that your kernel supports nftables before choosing this option.**

This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. **Configuration of a live systems firewall directly over a remote connection will often result in being locked out**. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

***Note**: Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*

The following will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.

Save the script bellow as `/etc/nftables/nftables.rules`

```
#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/nftables/nftables.rules

# flush nftables rulesset
flush ruleset

# Load nftables ruleset

# nftables config with inet table named filter

table inet filter {
        # Base chain for input hook named input (Filters inbound network packets)
        chain input {
                type filter hook input priority 0; policy drop;

                # Ensure loopback traffic is configured
                iif "lo" accept
                ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
                ip6 saddr ::1 counter packets 0 bytes 0 drop

                # Ensure established connections are configured
                ip protocol tcp ct state established accept
                ip protocol udp ct state established accept
                ip protocol icmp ct state established accept

                # Accept port 22(SSH) traffic from anywhere
                tcp dport ssh accept

                # Accept ICMP and IGMP from anywhere
                icmpv6 type { destination-unreachable, packet-too-big, time-exceeded, parameter-
problem, mld-listener-query, mld-listener-report, mld-listener-done, nd-router-solicit, nd-
router-advert, nd-neighbor-solicit, nd-neighbor-advert, ind-neighbor-solicit, ind-neighbor-
advert, mld2-listener-report } accept
                icmp type { destination-unreachable, router-advertisement, router-solicitation,
time-exceeded, parameter-problem } accept
                ip protocol igmp accept
        }

        # Base chain for hook forward named forward (Filters forwarded network packets)
        chain forward {
                type filter hook forward priority 0; policy drop;
        }

        # Base chain for hook output named output (Filters outbount network packets)
        chain output {
                type filter hook output priority 0; policy drop;
                # Ensure outbound and established connections are configured
                ip protocol tcp ct state established,related,new accept
                ip protocol udp ct state established,related,new accept
                ip protocol icmp ct state established,related,new accept
        }
}
```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables/nftables.rules
```

All changes in the nftables subsections are temporary

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables/nftables.rules
```

Add the following line to `/etc/sysconfig/nftables.conf`

```
include "/etc/nftables/nftables.rules"
```

3.4.3.1 Ensure nftables is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Note:

- *nftables is available in Linux kernel 3.13 and newer.*
- *Only **one** firewall utility should be installed and configured.*

Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Impact:

Changing firewall settings while connected over the network can result in being locked out of the system.

Audit:

Run the following command to verify that `nftables` is installed:

```
# rpm -q nftables

nftables-<version>
```

Remediation:

Run the following command to install `nftables`

```
# yum install nftables
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.3.2 Ensure iptables are flushed with nftables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Audit:

Run the following commands to ensure not iptables rules exist
For iptables:

```
# iptables -L

No rules should be returned
```

For ip6tables:

```
# ip6tables -L

No rules should be returned
```

Remediation:

Run the following commands to flush iptables:
For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.3.3 Ensure an nftables table exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Audit:

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:
Example:

```
table inet filter
```

Remediation:

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.3.4 Ensure nftables base chains exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Impact:

If configuring nftables over ssh, `creating` a `base chain` with a policy of `drop` will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains exist for `INPUT`, `FORWARD`, and `OUTPUT`.

```
# nft list ruleset | grep 'hook input'

type filter hook input priority 0;

# nft list ruleset | grep 'hook forward'

type filter hook forward priority 0;

# nft list ruleset | grep 'hook output'

type filter hook output priority 0;
```

Remediation:

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook
<(input|forward|output)> priority 0 \; }
```

Example:

```
# nft create chain inet filter input { type filter hook input priority 0 \; }
# nft create chain inet filter forward { type filter hook forward priority 0
\; }
# nft create chain inet filter output { type filter hook output priority 0 \;
}
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.3.5 Ensure nftables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands to verify that the loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'

iif "lo" accept

# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'

ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
```

- IF - IPv6 is enabled, run the following command to verify that the IPv6 loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'

ip6 saddr ::1 counter packets 0 bytes 0 drop
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept
# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

- IF - IPv6 is enabled:
Run the following command to implement the IPv6 loopback rules:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.3.6 Ensure nftables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound and established connections

Rationale:

If rules are not in place for new outbound and established connections, all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following commands and verify all rules for established incoming connections match site policy: site policy:

```
# nft list ruleset | awk '/hook input/,/}/' | grep -E 'ip protocol
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept
```

Run the following command and verify all rules for new and established outbound connections match site policy

```
# nft list ruleset | awk '/hook output/,/}/' | grep -E 'ip protocol
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established,related,new accept
ip protocol udp ct state established,related,new accept
ip protocol icmp ct state established,related,new accept
```

Remediation:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# nft add rule inet filter input ip protocol tcp ct state established accept
# nft add rule inet filter input ip protocol udp ct state established accept
# nft add rule inet filter input ip protocol icmp ct state established accept
# nft add rule inet filter output ip protocol tcp ct state
new,related,established accept
# nft add rule inet filter output ip protocol udp ct state
new,related,established accept
# nft add rule inet filter output ip protocol icmp ct state
new,related,established accept
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

3.4.3.7 Ensure nftables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to `accept`, the firewall will accept any packet that is not configured to be denied and the packet will continue traversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over the network can result in being locked out of the system.

Impact:

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing `ssh` has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains contain a policy of `DROP`.

```
# nft list ruleset | grep 'hook input'

type filter hook input priority 0; policy drop;

# nft list ruleset | grep 'hook forward'

type filter hook forward priority 0; policy drop;

# nft list ruleset | grep 'hook output'

type filter hook output priority 0; policy drop;
```

Remediation:

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

```
# nft chain <table family> <table name> <chain name> { policy drop \; }
```

Example:

```
# nft chain inet filter input { policy drop \; }
# nft chain inet filter forward { policy drop \; }
# nft chain inet filter output { policy drop \; }
```

Default Value:

accept

References:

1. Manual Page nft
2. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.3.8 Ensure nftables service is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the `/etc/sysconfig/nftables.conf` file during boot or the starting of the nftables service

Audit:

Run the following command and verify that the `nftables.service` is enabled:

```
# systemctl is-enabled nftables.service | grep '^enabled'

enabled
```

Run the following command to verive `nftables.service` is active:

```
# systemctl is-active nftables.service | grep '^active'

active
```

Remediation:

Run the following commands to unmask, enable and start `nftables.service`:

```
# systemctl unmask nftables.service
# systemctl --now enable nftables.service
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.3.9 Ensure nftables rules are permanent (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/sysconfig/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Audit:

Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot:
Run the following command to verify the input base chain:

```
# awk '/hook input/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print
$2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
                type filter hook input priority 0; policy drop;

                # Ensure loopback traffic is configured
                iif "lo" accept
                ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
                ip6 saddr ::1 counter packets 0 bytes 0 drop

                # Ensure established connections are configured
                ip protocol tcp ct state established accept
                ip protocol udp ct state established accept
                ip protocol icmp ct state established accept

                # Accept port 22(SSH) traffic from anywhere
                tcp dport ssh accept

                # Accept ICMP and IGMP from anywhere
                icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept
```

Note: Review the input base chain to ensure that it follows local site policy
Run the following command to verify the forward base chain:

```
# awk '/hook forward/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print
$2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
        # Base chain for hook forward named forward (Filters forwarded
network packets)
        chain forward {
                type filter hook forward priority 0; policy drop;
        }
```

Note: Review the forward base chain to ensure that it follows local site policy.
Run the following command to verify the forward base chain:

```
# awk '/hook output/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print
$2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
        # Base chain for hook output named output (Filters outbound network
packets)
        chain output {
                type filter hook output priority 0; policy drop;
                # Ensure outbound and established connections are configured
                ip protocol tcp ct state established,related,new accept
                ip protocol tcp ct state established,related,new accept
                ip protocol udp ct state established,related,new accept
                ip protocol icmp ct state established,related,new accept
        }
```

Note: Review the output base chain to ensure that it follows local site policy.

Remediation:

Edit the `/etc/sysconfig/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot:
Example:

```
include "/etc/nftables/nftables.rules"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	M1031

3.4.4 Configure iptables

If firewalld or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPtables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note: *Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.*

3.4.4.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

3.4.4.1.1 Ensure iptables packages are installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Audit:

Run the following command to verify that `iptables` and `iptables-services` are installed:

```
rpm -q iptables iptables-services

iptables-<version>
iptables-services-<version>
```

Remediation:

Run the following command to install `iptables` and `iptables-services`

```
# yum install iptables iptables-services
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.2 Configure iptables

IPTables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note:

- This section broadly assumes starting with an empty IPTables firewall ruleset (established by flushing the rules with iptables -F).
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out.
- It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. **This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.**

```
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.4.2.1 Ensure iptables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       127.0.0.0/8          0.0.0.0/0

 # iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.2.2 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

3.4.4.2.3 Ensure iptables rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system.
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

Audit:

Run the following command to determine open ports:

```
# ss -4tuln

Netid  State      Recv-Q Send-Q    Local Address:Port                    Peer
Address:Port
udp    UNCONN     0      0                     *:68
*:*
udp    UNCONN     0      0                     *:123
*:*
tcp    LISTEN     0      128                   *:22
*:*
```

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       127.0.0.0/8          0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.
Note: The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.2.4 Ensure iptables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify that the policy for the `INPUT` , `OUTPUT` , and `FORWARD` chains is `DROP` or `REJECT` :

```
# iptables -L

Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.2.5 Ensure iptables rules are saved (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package includes the `/etc/sysconfig/iptables` file. The `iptables` rules in this file will be loaded by the `iptables.service` during boot, or when it is started or re-loaded.

Rationale:

If the `iptables` rules are not saved and a system re-boot occurs, the `iptables` rules will be lost.

Audit:

Review the file `/etc/sysconfig/iptables` and ensure it contains the complete correct rule-set.
Example: `/etc/sysconfig/iptables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [4:463]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:23:37 2020
```

Remediation:

Run the following commands to create or update the `/etc/sysconfig/iptables` file:
Run the following command to review the current running `iptables` configuration:

```
# iptables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  loopback/8           anywhere
ACCEPT     tcp  --  anywhere             anywhere            state
ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere            state
ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere            state
ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
state NEW

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state
NEW,ESTABLISHED
ACCEPT     udp  --  anywhere             anywhere            state
NEW,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere            state
NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file `/etc/sysconfig/iptables`:

```
# service iptables save

iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.4.2.6 Ensure iptables service is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`iptables.service` is a utility for configuring and maintaining `iptables`.

Rationale:

`iptables.service` will load the iptables rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the iptables rules will be cleared during a re-boot of the system.

Audit:

Run the following commands to verify `iptables` is enabled:

```
# systemctl is-enabled iptables.service | grep '^enabled'

enabled
```

Run the following command to verify `iptables.service` is `active`:

```
# systemctl is-active iptables.service | grep '^active'

active
```

Remediation:

Run the following command to enable and start iptables:

```
# systemctl unmask iptables.service
# systemctl --now enable iptables.service
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.4.3 Configure ip6tables

If IPv6 is not enabled on the system, this section can be skipped.

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

Note:

- This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F).
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. **This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.**

```
#!/bin/bash

# Flush ip6tables rules
ip6tables -F

# Ensure default deny firewall policy
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Ensure loopback traffic is configured
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT
ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.4.4.3.1 Ensure ip6tables loopback traffic is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# ip6tables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all      lo     *       ::/0                ::/0
    0     0 DROP       all      *      *       ::1                 ::/0


# ip6tables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all      *      lo      ::/0                ::/0
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s ::1 -j DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.3.2 Ensure ip6tables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# ip6tables -L -v -n
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0011	M1031, M1037

3.4.4.3.3 Ensure ip6tables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system.
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

Audit:

Run the following command to determine open ports:

```
# ss -6tuln

Netid  State      Recv-Q Send-Q    Local Address:Port                    Peer
Address:Port
udp    UNCONN     0      0                   ::1:123
:::*
udp    UNCONN     0      0                    :::123
:::*
tcp    LISTEN     0      128                  :::22
:::*
tcp    LISTEN     0      20                  ::1:25
:::*
```

Run the following command to determine firewall rules:

```
# ip6tables -L INPUT -v -n

Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all      lo     *       ::/0                 ::/0
    0     0 DROP       all      *      *       ::1                  ::/0
    0     0 ACCEPT     tcp      *      *       ::/0                 ::/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.
- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.3.4 Ensure ip6tables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0011	M1031, M1037

3.4.4.3.5 Ensure ip6tables rules are saved (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package includes the `/etc/sysconfig/ip6tables` file. The `ip6tables` rules in this file will be loaded by the `ip6tables.service` during boot, or when it is started or re-loaded.

Rationale:

If the `ip6tables` rules are not saved and a system re-boot occurs, the `ip6tables` rules will be lost.

Audit:

Review the file `/etc/sysconfig/ip6tables` and ensure it contains the complete correct rule-set.
Example: `/etc/sysconfig/ip6tables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s ::1/128 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:58:32 2020
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Run the following commands to create or update the `/etc/sysconfig/ip6tables` file:
Run the following command to review the current running `iptables` configuration:

```
# ip6tables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all      anywhere             anywhere
DROP       all      localhost            anywhere
ACCEPT     tcp      anywhere             anywhere             state
ESTABLISHED
ACCEPT     udp      anywhere             anywhere             state
ESTABLISHED
ACCEPT     icmp     anywhere             anywhere             state
ESTABLISHED
ACCEPT     tcp      anywhere             anywhere             tcp dpt:ssh
state NEW

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all      anywhere             anywhere
ACCEPT     tcp      anywhere             anywhere             state
NEW,ESTABLISHED
ACCEPT     udp      anywhere             anywhere             state
NEW,ESTABLISHED
ACCEPT     icmp     anywhere             anywhere             state
NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file `/etc/sysconfig/ip6tables`:

```
# service ip6tables save

ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[  OK  ]
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

3.4.4.3.6 Ensure ip6tables is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`ip6tables.service` is a utility for configuring and maintaining `ip6tables`.

Rationale:

`ip6tables.service` will load the iptables rules saved in the file `/etc/sysconfig/ip6tables` at boot, otherwise the ip6tables rules will be cleared during a re-boot of the system.

Audit:

Run the following commands to verify `ip6tables` is enabled:

```
# systemctl is-enabled ip6tables.service | grep '^enabled'

enabled
```

Run the following command to verify ip6tables.service is active:

```
# systemctl is-active ip6tables | grep '^active'

active
```

- OR - verify IPv6 is not enabled:
Run the following command to confirm IPv6 is not enabled:

```
# grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n -
IPv6 is enabled\n" || echo -e "\n - IPv6 is not enabled\n"
```

Remediation:

Run the following commands to unmask, enable and start `ip6tables.service`:

```
# systemctl unmask ip6tables.service
# systemctl --now start ip6tables.service
```

References:

1. NIST SP 800-53 Rev. 5: CA-9

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.004	TA0005	

4 Access, Authentication and Authorization

4.1 Configure job schedulers

A job scheduler is used to execute jobs, commands, or shell scripts, at fixed times, dates, or intervals

4.1.1 Configure cron

`cron` is a time based job scheduler

Note:

- Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy
- **-IF-** cron is not installed on the system, this sub section can be skipped

4.1.1.1 Ensure cron daemon is enabled and active (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `cron` daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

Note: IF systemd timers are configured and used for scheduled tasks, this recommendation may be skipped

Audit:

Run the following command to verify `crond` is enabled:

```
# systemctl is-enabled crond

enabled
```

Run the following command to verify that `crond` is active:

```
# systemctl is-active crond

active
```

Remediation:

Run the following commands to unmask, enable, and start `crond`:

```
# systemctl unmask crond
# systemctl --now enable crond
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1018

4.1.1.2 Ensure permissions on /etc/crontab are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab

Access: (600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

Default Value:

Access: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.hourly/

Access: (700/drwx------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.hourly` directory:

```
# chown root:root /etc/cron.hourly/
# chmod og-rwx /etc/cron.hourly/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.daily/

Access: (700/drwx------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily/
# chmod og-rwx /etc/cron.daily/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.weekly/

Access: (700/drwx------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/
# chmod og-rwx /etc/cron.weekly/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.monthly/

Access: (700/drwx------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/
# chmod og-rwx /etc/cron.monthly/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.7 Ensure permissions on /etc/cron.d are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.d/

Access: (700/drwx------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/
# chmod og-rwx /etc/cron.d/
```

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002, TA0007	M1018

4.1.1.8 Ensure crontab is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`crontab` is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in `/var/spool/cron/crontabs`, they are not intended to be edited directly.

If the `/etc/cron.allow` file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the `/etc/cron.allow` file does not exist but the `/etc/cron.deny` file does exist, then you must not be listed in the `/etc/cron.deny` file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then `/etc/cron.allow` takes precedence. Which means that `/etc/cron.deny` is not considered and your user must be listed in `/etc/cron.allow` in order to be able to use the crontab.

Regardless of the existence of any of these files, the root administrative user is always allowed to setup a crontab.

The files `/etc/cron.allow` and `/etc/cron.deny`, if they exist, must be either world-readable, or readable by group `crontab`. If they are not, then cron will deny access to all users until the permissions are fixed.

There is one file for each user's crontab under the `/var/spool/cron/crontabs` directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the `crontab` group and configuring crontab command with the setgid bid set for that specific group.

Note:

- Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user
- The files `/etc/cron.allow` and `/etc/cron.deny`, if they exist, only controls administrative access to the crontab command for scheduling and modifying cron jobs

Rationale:

On many systems, only the system administrator is authorized to schedule `cron` jobs. Using the `cron.allow` file to control who can run `cron` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

-IF- cron is installed on the system:
Run the following command to verify `/etc/cron.allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root`
- Is group owned by the group `root`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.allow

Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Run the following command to verify `cron.deny` doesn't exist, **-OR-** is:

- Mode `0640` or more restrictive
- Owned by the user `root`
- Group owned by the group `root`

```
# [ -e "/etc/cron.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group:
(%G)' /etc/cron.deny

Access: (640/-rw-r-----) Owner: (root) Group: (root)
-OR-
Nothing is returned
```

Remediation:

-IF- cron is installed on the system:
Run the following commands to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner or user `root`
- Change group owner to group `root`
- Change mode to `640` or more restrictive

```
# [ ! -e "/etc/cron.allow" ] && touch /etc/cron.allow
# chown root:root /etc/cron.allow
# chmod u-x,g-wx,o-rwx /etc/cron.allow
```

Run the following commands to:
-IF- `/etc/cron.deny` exists:

- Change owner or user `root`
- Change group owner to group `root`
- Change mode to `640` or more restrictive

```
# [ -e "/etc/cron.deny" ] && chown root:root /etc/cron.deny
# [ -e "/etc/cron.deny" ] && chmod u-x,g-wx,o-rwx /etc/cron.deny
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

4.1.2 Configure at

`at` is a command-line utility used to schedule a job for later execution

Note: if `at` is not installed on the system, this section can be skipped

4.1.2.1 Ensure at is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`at` allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The `/etc/at.allow` and `/etc/at.deny` files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file `/etc/at.allow` exists, only usernames mentioned in it are allowed to use at. If `/etc/at.allow` does not exist, `/etc/at.deny` is checked, every username not mentioned in it is then allowed to use at. An empty `/etc/at.deny` means that every user may use at. If neither file exists, only the superuser is allowed to use at.

Rationale:

On many systems, only the system administrator is authorized to schedule `at` jobs. Using the `at.allow` file to control who can run `at` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

-IF- at is installed on the system:
Run the following command to verify `/etc/at.allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root`
- Is group owned by the group `daemon` or group `root`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.allow

Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Verify mode is `640` or more restrictive, owner is `root`, and group is `daemon` or `root`
Run the following command to verify `at.deny` doesn't exist, **-OR-** is:

- Mode `0640` or more restrictive
- Owned by the user `root`
- Group owned by the group `daemon` or group `root`

```
# [ -e "/etc/at.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)'
/etc/at.deny

Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
-OR-
Nothing is returned
```

If a value is returned, Verify mode is 640 or more restrictive, owner is `root`, and group is `daemon` or `root`

Remediation:

-IF- at is installed on the system:
Run the following script to:

- `/etc/at.allow`:
  - Create the file if it doesn't exist
  - Change owner or user `root`
  - If group `daemon` exists, change to group `daemon`, else change group to `root`
  - Change mode to `640` or more restrictive
- **-IF-** `/etc/at.deny` exists:
  - Change owner or user `root`
  - If group `daemon` exists, change to group `daemon`, else change group to `root`
  - Change mode to `640` or more restrictive

```
#!/usr/bin/env bash

{
   grep -Pq -- '^daemon\b' /etc/group && l_group="daemon" || l_group="root"
   [ ! -e "/etc/at.allow" ] && touch /etc/at.allow
   chown root:"$l_group" /etc/at.allow
   chmod u-x,g-wx,o-rwx /etc/at.allow
   [ -e "/etc/at.deny" ] && chown root:"$l_group" /etc/at.deny
   [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny
}
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1053, T1053.003	TA0002	M1018

4.2 Configure SSH Server

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note:

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- The openSSH daemon configuration option `Match`, may cause the audits in this section's recommendations to report incorrectly. It is recommended that this option only be used if it's needed and fully understood. If this option is configured in accordance with local site policy, it should be accounted for when following the recommendations in this section.
- The audits of the configuration in this section are run in the context of the root user, the local host name, and the local host's IP address. If a `Match` block exists that matches one of these criteria, the output of the audit will be from the match block. The respective matched criteria should be replaced with a non-matching substitution.
- Once all configuration changes have been made to `/etc/ssh/sshd_config` the `sshd` configuration must be reloaded
- `Match`:
    - Introduces a conditional block.
    - If all of the criteria on the Match line are satisfied, the keywords on the following lines override those set in the global section of the config file, until either another Match line or the end of the file.
    - If a keyword appears in multiple Match blocks that are satisfied, only the first instance of the keyword is applied.
    - The arguments to Match are one or more criteria-pattern pairs or the single token All which matches all criteria. The available criteria are User, Group, Host, LocalAddress, LocalPort, RDomain, and Address (with RDomain representing the rdomain(4) on which the connection was received).
    - The match patterns may consist of single entries or comma-separated lists and may use the wildcard and negation operators described in the PATTERNS section of ssh_config(5).
    - The patterns in an Address criteria may additionally contain addresses to match in CIDR address/masklen format, such as 192.0.2.0/24 or 2001:db8::/32. Note that the mask length provided must be consistent with the address - it is an error to specify a mask length that is too long for the address or one with bits set in this host portion of the address. For example, 192.0.2.0/33 and 192.0.2.0/8, respectively.

- Only a subset of keywords may be used on the lines following a Match keyword.
- Available keywords are: `AcceptEnv`, `AllowAgentForwarding`, `AllowGroups`, `AllowStreamLocalForwarding`, `AllowTcpForwarding`, `AllowUsers`, `AuthenticationMethods`, `AuthorizedKeysCommand`, `AuthorizedKeysCommandUser`, `AuthorizedKeysFile`, `AuthorizedPrincipalsCommand`, `AuthorizedPrincipalsCommandUser`, `AuthorizedPrincipalsFile`, `Banner`, `ChrootDirectory`, `ClientAliveCountMax`, `ClientAliveInterval`, `DenyGroups`, `DenyUsers`, `ForceCommand`, `GatewayPorts`, `GSSAPIAuthentication`, `HostbasedAcceptedKeyTypes`, `HostbasedAuthentication`, `HostbasedUsesNameFromPacketOnly`, `IPQoS`, `KbdInteractiveAuthentication`, `KerberosAuthentication`, `KerberosUseKuserok`, `MaxAuthTries`, `MaxSessions`, `PasswordAuthentication`, `PermitEmptyPasswords`, `PermitOpen`, `PermitRootLogin`, `PermitTTY`, `PermitTunnel`, `PermitUserRC`, `PubkeyAcceptedKeyTypes`, `PubkeyAuthentication`, `RekeyLimit`, `RevokedKeys`, `StreamLocalBindMask`, `StreamLocalBindUnlink`, `TrustedUserCAKeys`, `X11DisplayOffset`, `X11MaxDisplays`, `X11Forwarding` and `X11UseLocalhost`.

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# yum remove openssh-server
```

4.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The file `/etc/ssh/sshd_config`, and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory, contain configuration specifications for `sshd`.

Rationale:

configuration specifications for `sshd` need to be protected from unauthorized changes by non-privileged users.

Audit:

Run the following script and verify `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory are:

- Mode `0600` or more restrictive
- Owned by the `root` user
- Group owned by the group `root`.

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   unset a_sshdfiles && a_sshdfiles=()
   [ -e "/etc/ssh/sshd_config" ] && a_sshdfiles+=("$(stat -Lc '%n^%#a^%U^%G'
"/etc/ssh/sshd_config")")
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_sshdfiles+=("$(stat -Lc '%n^%#a^%U^%G'
"$l_file")")
   done < <(find /etc/ssh/sshd_config.d -type f  \( -perm /077 -o ! -user
root -o ! -group root \) -print0)
   if (( ${#a_sshdfiles[@]} != 0 )); then
      perm_mask='0177'
      maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
      while IFS="^" read -r l_file l_mode l_user l_group; do
         l_out2=""
         [ $(( $l_mode & $perm_mask )) -gt 0 ] && l_out2="$l_out2\n  - Is
mode: \"$l_mode\" should be: \"$maxperm\" or more restrictive"
         [ "$l_user" != "root" ] && l_out2="$l_out2\n  - Is owned by
\"$l_user\" should be owned by \"root\""
         [ "$l_group" != "root" ] && l_out2="$l_out2\n  - Is group owned by
\"$l_user\" should be group owned by \"root\""
         if [ -n "$l_out2" ]; then
            l_output2="$l_output2\n - File: \"$l_file\":$l_out2"
         else
            l_output="$l_output\n - File: \"$l_file\":\n  - Correct: mode
($l_mode), owner ($l_user), and group owner ($l_group) configured"
         fi
      done <<< "$(printf '%s\n' "${a_sshdfiles[@]}")"
   fi
   unset a_sshdfiles
   # If l_output2 is empty, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  *** PASS ***\n- * Correctly set *
:\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
      [ -n "$l_output" ] && echo -e " - * Correctly set * :\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to set ownership and permissions on `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory:

```
#!/usr/bin/env bash

{
   chmod u-x,og-rwx /etc/ssh/sshd_config
   chown root:root /etc/ssh/sshd_config
   while IFS= read -r -d $'\0' l_file; do
      if [ -e "$l_file" ]; then
         chmod u-x,og-rwx "$l_file"
         chown root:root "$l_file"
      fi
   done < <(find /etc/ssh/sshd_config.d -type f -print0)
}
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098, T1098.004, T1543, T1543.002	TA0005	M1022

4.2.2 Ensure permissions on SSH private host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Audit:

Run the following script to verify SSH private host key files are owned by the root user and either:

- owned by the group root and mode 0600 or more restrictive

- OR -

- owned by the group designated to own openSSH private keys and mode 0640 or more restrictive

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   if command -v ssh-keygen &>/dev/null; then
      l_skgn="$(grep -Po -- '^(ssh_keys|_?ssh)\b' /etc/group)" # Group designated to own openSSH
keys
      l_skgid="$(awk -F: '($1 == "'"$l_skgn"'"){print $3}' /etc/group)" # Get gid of group
      [ -n "$l_skgid" ] && l_agroup="(root|$l_skgn)" || l_agroup="root"
      if [ -d /etc/ssh ]; then
         unset a_skarr && a_skarr=() # Clear and initialize array
         while IFS= read -r -d $'\0' l_file; do # Loop to populate array
            l_var="$(ssh-keygen -l -f 2>/dev/null "$l_file")"
            if [ -n "$l_var" ] && ! grep -Pq -- '\h+no\h+comment\b' <<< "$l_var"; then
               a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
            fi
         done < <(find -L /etc/ssh -xdev -type f -print0)
         if (( ${#a_skarr[@]} > 0 )); then
            while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
               l_out2=""
               [ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
               l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
               if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
                  l_out2="$l_out2\n  - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more
restrictive"
               fi
               if [ "$l_owner" != "root" ]; then
                  l_out2="$l_out2\n  - Owned by: \"$l_owner\" should be owned by \"root\""
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_out2="$l_out2\n  - Owned by group \"$l_group\" should be group owned by:
\"${l_agroup//|/ or }\""
               fi
               if [ -n "$l_out2" ]; then
                  l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
               else
                  l_output="$l_output\n - File: \"$l_file\"\n  - Correct: mode ($l_mode), owner
($l_owner), and group owner ($l_group) configured"
               fi
            done <<< "$(printf '%s\n' "${a_skarr[@]}")"
         else
            l_output="  - No private keys found in \"/etc/ssh\""
         fi
      else
         l_output="  - ssh directory not found on the system"
      fi
   else
      l_output2="  - ssh-keygen command not found\n  - manual check may be required"
   fi
   unset a_skarr
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  *** PASS ***\n- * Correctly set * :\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit failure * :\n$l_output2\n"
      [ -n "$l_output" ] && echo -e " - * Correctly set * :\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to set mode, ownership, and group on the private SSH host key files:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   l_skgn="$(grep -Po -- '^(ssh_keys|_?ssh)\b' /etc/group)" # Group designated to own openSSH
keys
   l_skgid="$(awk -F: '($1 == "'"$l_skgn"'"){print $3}' /etc/group)" # Get gid of group
   if [ -n "$l_skgid" ]; then
      l_agroup="(root|$l_skgn)" && l_sgroup="$l_skgn" && l_mfix="u-x,g-wx,o-rwx"
   else
      l_agroup="root" && l_sgroup="root" && l_mfix="u-x,go-rwx"
   fi
   if command -v ssh-keygen &>/dev/null; then
      unset a_skarr && a_skarr=() # Clear and initialize array
      if [ -d /etc/ssh ]; then
         while IFS= read -r -d $'\0' l_file; do # Loop to populate array
            l_var="$(ssh-keygen -l -f 2>/dev/null "$l_file")"
            if [ -n "$l_var" ] && ! grep -Pq -- '\h+no\h+comment\b' <<< "$l_var"; then
               a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
            fi
         done < <(find -L /etc/ssh -xdev -type f -print0)
         if (( ${#a_skarr[@]} > 0 )); then
            while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
               l_out2=""
               [ "$l_gid" = "$l_skgid" ] && l_pmask="0137" || l_pmask="0177"
               l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
               if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
                  l_out2="$l_out2\n  - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more
restrictive\n   - Revoking excess permissions"
                  chmod "$l_mfix" "$l_file"
               fi
               if [ "$l_owner" != "root" ]; then
                  l_out2="$l_out2\n  - Owned by: \"$l_owner\" should be owned by \"root\"\n   -
Changing ownership to \"root\""
                  chown root "$l_file"
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_out2="$l_out2\n  - Owned by group \"$l_group\" should be group owned by:
\"${l_agroup//|/ or }\"\n   - Changing group ownership to \"$l_sgroup\""
                  chgrp "$l_sgroup" "$l_file"
               fi
               [ -n "$l_out2" ] && l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
            done <<< "$(printf '%s\n' "${a_skarr[@]}")"
         else
            l_output="  - No private keys found in \"/etc/ssh\""
         fi
      else
         l_output="- ssh directory not found on the system"
      fi
      unset a_skarr
   else
      l_output2="  - ssh-keygen command not found\n  - manual remediation may be required"
   fi
   if [ -z "$l_output2" ]; then
      echo -e "\n- No access changes required\n"
   else
      echo -e "\n- Remediation results:\n$l_output2\n"
   fi
}
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552, T1552.004	TA0003, TA0006	M1022

4.2.3 Ensure permissions on SSH public host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:
Run the following script to verify SSH public host key files are mode 0644 or more restrictive, owned be the root user, and owned be the root group:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   l_skgn="$(grep -Po -- '^(ssh_keys|_?ssh)\b' /etc/group)" # Group designated to own openSSH
public keys
   l_skgid="$(awk -F: '($1 == "'"$l_skgn"'"){print $3}' /etc/group)" # Get gid of group
   [ -n "$l_skgid" ] && l_agroup="(root|$l_skgn)" || l_agroup="root"
   if command -v ssh-keygen &>/dev/null; then
      unset a_skarr && a_skarr=() # Clear and initialize array
      if [ -d "/etc/ssh" ]; then
         while IFS= read -r -d $'\0' l_file; do # Loop to populate array
            if grep -Pq -- '\h+no\h+comment\b' <<< "$(ssh-keygen -l -f 2>/dev/null "$l_file")";
then
               a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
            fi
         done < <(find -L /etc/ssh -xdev -type f -print0)
         if (( ${#a_skarr[@]} > 0 )); then
            while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
            echo "File: \"$l_file\" Mode: \"$l_mode\" Owner: \"$l_owner\" Group: \"$l_group\"
GID: \"$l_gid\""
               l_out2=""
               l_pmask="0133"
               l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
               if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
                  l_out2="$l_out2\n  - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more
restrictive"
               fi
               if [ "$l_owner" != "root" ]; then
                  l_out2="$l_out2\n  - Owned by: \"$l_owner\" should be owned by \"root\""
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_out2="$l_out2\n  - Owned by group \"$l_group\" should be group owned by:
\"${l_agroup//|/ or }\""
               fi
               if [ -n "$l_out2" ]; then
                  l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
               else
                  l_output="$l_output\n - File: \"$l_file\"\n  - Correct: mode ($l_mode), owner
($l_owner), and group owner ($l_group) configured"
               fi
            done <<< "$(printf '%s\n' "${a_skarr[@]}")"
         else
            l_output="  - No public keys found in \"/etc/ssh\""
         fi
      else
         l_output="- ssh directory not found on the system"
      fi
      unset a_skarr
   else
      l_output2="  - ssh-keygen command not found\n  - manual check may be required"
   fi
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  *** PASS ***\n- * Correctly set * :\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit failure * :\n$l_output2\n"
      [ -n "$l_output" ] && echo -e " - * Correctly set * :\n$l_output\n"
   fi
}
```

Remediation:

Run the following script to set mode, ownership, and group on the public SSH host key files:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   l_skgn="$(grep -Po -- '^(ssh_keys|_?ssh)\b' /etc/group)" # Group designated to own openSSH
keys
   l_skgid="$(awk -F: '($1 == "'"$l_skgn"'"){print $3}' /etc/group)" # Get gid of group
   l_mfix="u-x,go-wx"
   if command -v ssh-keygen &>/dev/null; then
      unset a_skarr && a_skarr=() # Clear and initialize array
      if [ -d /etc/ssh ]; then
         while IFS= read -r -d $'\0' l_file; do # Loop to populate array
            if grep -Pq -- '\h+no\h+comment\b' <<< "$(ssh-keygen -l -f 2>/dev/null "$l_file")";
then
               a_skarr+=("$(stat -Lc '%n^%#a^%U^%G^%g' "$l_file")")
            fi
         done < <(find -L /etc/ssh -xdev -type f -print0)
         if (( ${#a_skarr[@]} > 0 )); then
            while IFS="^" read -r l_file l_mode l_owner l_group l_gid; do
               l_out2=""
               l_pmask="0133"
               l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
               if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
                  l_out2="$l_out2\n  - Mode: \"$l_mode\" should be mode: \"$l_maxperm\" or more
restrictive\n   - Revoking excess permissions"
                  chmod "$l_mfix" "$l_file"
               fi
               if [ "$l_owner" != "root" ]; then
                  l_out2="$l_out2\n  - Owned by: \"$l_owner\" should be owned by \"root\"\n   -
Changing ownership to \"root\""
                  chown root "$l_file"
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_out2="$l_out2\n  - Owned by group \"$l_group\" should be group owned by:
\"${l_agroup//|/ or }\"\n   - Changing group ownership to \"$l_sgroup\""
                  chgrp "$l_sgroup" "$l_file"
               fi
               [ -n "$l_out2" ] && l_output2="$l_output2\n - File: \"$l_file\"$l_out2"
            done <<< "$(printf '%s\n' "${a_skarr[@]}")"
         else
            l_output="  - No public keys found in \"/etc/ssh\""
         fi
      else
         l_output="- ssh directory not found on the system"
      fi
      unset a_skarr
   else
      l_output2="  - ssh-keygen command not found\n  - manual remediation may be required"
   fi
   if [ -z "$l_output2" ]; then
      echo -e "\n- No access changes required\n"
   else
      echo -e "\n- Remediation results:\n$l_output2\n"
   fi
}
```

Default Value:

644 0/root 0/root

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557, T1557.000	TA0003, TA0006	M1022

4.2.4 Ensure sshd access is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- `AllowUsers`:
  - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- `AllowGroups`:
  - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- `DenyUsers`:
  - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- `DenyGroups`:
  - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -Pi '^\h*(allow|deny)(users|groups)\h+\H+'
```

Verify that the output matches at least one of the following lines:

```
allowusers <userlist>
-OR-
allowgroups <grouplist>
-OR-
denyusers <userlist>
-OR-
denygroups <grouplist>
```

- IF - `AllowUsers` or `AllowGroups` is returned, review the list(s) to ensure included users and/or groups follow local site policy
- IF - `Match` set statements are used in your environment, review `/etc/ssh/sshd_config`:

- Verify that the setting is not only in a match block
- Review all match blocks for incorrect configuration

Remediation:

Edit `/etc/ssh/sshd_config` and set one or more of the parameters above any `Match` set statements as follows:

```
AllowUsers <userlist>
-OR-
AllowGroups <grouplist>
-OR-
DenyUsers <userlist>
-OR-
DenyGroups <grouplist>
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.
Run the following command to reload the openSSH server daemon configuration:

```
# systemctl reload-or-try-restart sshd.service
```

Default Value:

None

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0008	M1018

4.2.5 Ensure sshd Banner is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Audit:

Run the following command to verify `Banner` is set:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -Pi '^banner\h+\/\H+'
```

Example:

```
banner /etc/issue.net
```

Run the following command to verify that `/etc/ssh/sshd_config` does not include setting `Banner` to `none`:

```
# grep -Pi '^\h*Banner\h+\"?none\b' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Match` entries as follows:

```
Banner /etc/issue.net
```

Note: First occurrence of a option takes precedence, Match set statements withstanding.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
	TA0001, TA0007	M1035

4.2.6 Ensure sshd Ciphers are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the ciphers that SSH can use during communication.

Note:

- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140-2 compliant are:
  - aes256-ctr
  - aes192-ctr
  - aes128-ctr

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

Audit:

Run the following command to verify none of the "weak" ciphers are being used:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -Pi
'^ciphers\h+\"?([^#\n\r]+,)?((3des|blowfish|cast128|aes(128|192|256))-
cbc|arcfour(128|256)?|rijndael-cbc@lysator\.liu\.se)\b'
```

Nothing should be returned
The following are considered "weak" ciphers, and should not be used:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Remediation:

Edit the /etc/ssh/sshd_config file and add or modify the `Ciphers` line to contain a comma separated list of the site approved (Strong) Ciphers:
Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Note: First occurrence of an option takes precedence.

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com, aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc

References:

1. https://nvd.nist.gov/vuln/detail/CVE-2016-2183
2. https://www.openssh.com/txt/cbc.adv
3. https://nvd.nist.gov/vuln/detail/CVE-2008-5161
4. https://www.openssh.com/txt/cbc.adv
5. SSHD_CONFIG(5)
6. NIST SP 800-53 Rev. 5: SC-8

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557	TA0006	M1041

4.2.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Note: To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before `8.2p1` there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in `8.2p1` and thus it can no longer be abused disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config`:

- `ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` Sets the number of client alive messages which may be sent without sshd(8) receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option en-abled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero ClientAliveCountMax disables connection termination.

Rationale:

In order to prevent resource exhaustion, appropriate values should be set for both `ClientAliveInterval` and `ClientAliveCountMax`. Specifically, looking at the source code, `ClientAliveCountMax` must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Audit:

Run the following commands and verify `ClientAliveInterval` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep clientaliveinterval
```

Example Output:

```
clientaliveinterval 15
```

Run the following command and verify `ClientAliveInterval` is not set to zero:

```
# grep -Psi '^\h*ClientAliveInterval\h+"?0\b' /etc/ssh/sshd_config

Nothing should be returned
```

Run the following command and verify `ClientAliveCountMax` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep clientalivecountmax
```

Example Output:

```
clientalivecountmax 3
```

Run the following command and verify `ClientAliveCountMax` is not set to zero:

```
# grep -Psi '^\h*ClientAliveCountMax\h+"?0\b' /etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, those locations should be checked for the correct configuration as well.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters above any `Match` entries according to site policy.
Example:

```
ClientAliveInterval 15
ClientAliveCountMax 3
```

Note: First occurrence of a option takes precedence, Match set statements withstanding.

Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

References:

1. https://man.openbsd.org/sshd_config
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

https://bugzilla.redhat.com/show_bug.cgi?id=1873547

https://github.com/openssh/openssh-portable/blob/V_8_9/serverloop.c#L137

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003	TA0001	M1026

4.2.8 Ensure sshd DisableForwarding is enabled (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

Description:

The `DisableForwarding` parameter disables all forwarding features, including X11, ssh-agent(1), TCP and StreamLocal. This option overrides all other forwarding-related options and may simplify restricted configurations.

- X11Forwarding provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.
- ssh-agent is a program to hold private keys used for public key authentication. Through use of environment variables the agent can be located and automatically used for authentication when logging in to other machines using ssh.
- SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

anyone with root privilege on the the intermediate server can make free use of ssh-agent to authenticate them to other servers

Leaving port forwarding enabled can expose the organization to security risks and backdoors. SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network.

Impact:

SSH tunnels are widely used in many corporate environments. In some environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

Audit:

Run the following command to verify `DisableForwarding` is set to `yes`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -i disableforwarding

disableforwarding yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `DisableForwarding` parameter to `yes`:

```
DisableForwarding yes
```

Note: First occurrence of a option takes precedence.

Default Value:

DisableForwarding no

References:

1. sshd_config(5)
2. NIST SP 800-53 Rev. 5: CM-7

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210, T1210.000	TA0008	M1042

4.2.9 Ensure sshd GSSAPIAuthentication is disabled (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

Description:

The `GSSAPIAuthentication` parameter specifies whether user authentication based on GSSAPI is allowed

Rationale:

Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, and should be disabled to reduce the attack surface of the system

Audit:

Run the following command to verify `GSSAPIAuthentication` is set to `no`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep gssapiauthentication

gssapiauthentication no
```

Run the following command and verify the output:

```
# grep -Psi '^\h*GSSAPIAuthentication\h+\"?yes\b' /etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, those locations should be checked for the correct configuration as well.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `GSSAPIAuthentication` parameter to `no` above any `Match` statement:

```
GSSAPIAuthentication no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Default Value:

GSSAPIAuthentication no

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

4.2.10 Ensure sshd HostbasedAuthentication is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit:

Run the following command to verify `HostbasedAuthentication` is set to `no`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep hostbasedauthentication

hostbasedauthentication no
```

Run the following command and verify the output:

```
# grep -Psi '^\h*HostbasedAuthentication\h+\"?yes\b' /etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, those locations should be checked for the correct configuration as well.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `HostbasedAuthentication` parameter to `no`:

```
HostbasedAuthentication no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Default Value:

HostbasedAuthentication no

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1042

4.2.11 Ensure sshd IgnoreRhosts is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

Audit:

Run the following command to verify `IgnoreRhosts` is set to `yes`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep ignorerhosts

ignorerhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `IgnoreRhosts` parameter to `yes`:

```
IgnoreRhosts yes
```

Note: First occurrence of a option takes precedence.

Default Value:

IgnoreRhosts yes

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0001	M1027

4.2.12 Ensure sshd KexAlgorithms is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140-2 approved are:
    - ecdh-sha2-nistp256
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp521
    - diffie-hellman-group-exchange-sha256
    - diffie-hellman-group16-sha512
    - diffie-hellman-group18-sha512
    - diffie-hellman-group14-sha256

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Audit:

Run the following command to verify none of the "weak" Key Exchange algorithms are being used:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -Pi 'kexalgorithms\h+([^#\n\r]+,)?(diffie-hellman-group1-
sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\b'

Nothing should be returned
```

The following are considered "weak" Key Exchange Algorithms, and should not be used:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

Remediation:

Edit `/etc/ssh/sshd_config` and add/modify the `KexAlgorithms` line to contain a comma separated list of the site approved, supported "strong" KexAlgorithms:
Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256
```

Note: First occurrence of an option takes precedence.

Default Value:

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

References:

1. NIST SP 800-53 Rev. 5: SC-8

Additional Information:

The supported algorithms are:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

4.2.13 Ensure sshd LoginGraceTime is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `LoginGraceTime` parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the `LoginGraceTime` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Audit:

Run the following command and verify that output `LoginGraceTime` is between `1` and `60` seconds:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep logingracetime

logingracetime 60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `LoginGraceTime` parameter is `60` or `1m`:

```
LoginGraceTime 60
```

Note: First occurrence of a option takes precedence.

Default Value:

LoginGraceTime 120

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-6

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003, T1110.004	TA0006	M1036

4.2.14 Ensure sshd LogLevel is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`LogLevel` gives the verbosity level that is used when logging messages from sshd. The possible values are: `QUIET`, `FATAL`, `ERROR`, `INFO`, `VERBOSE`, `DEBUG`, `DEBUG1`, `DEBUG2`, and `DEBUG3`. The default is INFO. `DEBUG` and `DEBUG1` are equivalent. `DEBUG2` and `DEBUG3` each specify higher levels of debugging output.

Note: Logging with a DEBUG level violates the privacy of users and is not recommended.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. The `DEBUG` options are specifically **not** recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

The `INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

The `VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep loglevel

loglevel VERBOSE
   - OR -
loglevel INFO
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `LogLevel` parameter as follows:

```
LogLevel VERBOSE
   - OR -
LogLevel INFO
```

Note: First occurrence of a option takes precedence.

Default Value:

LogLevel INFO

References:

1. https://www.ssh.com/ssh/sshd_config/
2. NIST SP 800-53 Rev. 5: AU-3, AU-12, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

4.2.15 Ensure sshd MACs are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Notes:

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140-2 approved are:
  - HMAC-SHA1
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

Audit:

Run the following command to verify none of the "weak" MACs are being used:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -Pi 'macs\h+([^#\n\r]+,)?(hmac-md5|hmac-md5-96|hmac-
ripemd160|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-
md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-
etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-
128-etm@openssh\.com)\b'

Nothing should be returned
```

The following are considered "weak" MACs, and should not be used:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1-96
umac-64@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the `MACs` line to contain a comma separated list of the site approved, supported "strong" MACs:
Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-
512,hmac-sha2-256
```

Note: The first occurrence of an option takes precedence.

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-etm@openssh.com

References:

1. More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH
2. SSHD_CONFIG(5)
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

The supported MACs are:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1040, T1040.000, T1557, T1557.000	TA0006	M1041

4.2.16 Ensure sshd MaxAuthTries is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit:

Run the following command and verify that `MaxAuthTries` is `4` or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep maxauthtries

maxauthtries 4
```

Note: If `Match` statements are used in your environment, these locations should be checked for the correct configuration as well.
Run the following command and verify that the output:

```
# grep -Pis '^\h*maxauthtries\h+\"?([5-9]|[1-9][0-9]+)\b'
/etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxAuthTries` parameter to `4` or less above any `Match` entries as follows:

```
MaxAuthTries 4
```

Note: First occurrence of a option takes precedence, Match set statements withstanding.

Default Value:

MaxAuthTries 6

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: AU-3

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1036

4.2.17 Ensure sshd MaxSessions is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that `MaxSessions` is `10` or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -i maxsessions

maxsessions 10
```

Run the following command and verify the output:

```
grep -Pis '^\h*MaxSessions\h+\"?(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+)\b'
/etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, these locations should be checked for the correct configuration as well.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxSessions` parameter to `10` or less above any `Match` entries as follows:

```
MaxSessions 10
```

Note: First occurrence of a option takes precedence, Match set statements withstanding.

Default Value:

MaxSessions 10

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

4.2.18 Ensure sshd MaxStartups is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command to verify `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -i maxstartups

maxstartups 10:30:60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxStartups` parameter to `10:30:60` or more restrictive:

```
MaxStartups 10:30:60
```

Note: First occurrence of a option takes precedence.

Default Value:

MaxStartups 10:30:100

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.002	TA0040	

4.2.19 Ensure sshd PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitEmptyPasswords` parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

Audit:

Run the following command to verify `PermitEmptyPasswords` is set to `no`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep permitemptypasswords

permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Psi '^\h*PermitEmptyPasswords\h+"?yes\b' /etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, these locations should be checked for the correct configuration as well.

Remediation:

Edit `/etc/ssh/sshd_config` and set the `PermitEmptyPasswords` parameter to `no` above any `Match` entries:

```
PermitEmptyPasswords no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Default Value:

PermitEmptyPasswords no

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

4.2.20 Ensure sshd PermitRootLogin is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using SSH. The default is `prohibit-password`.

Rationale:

Disallowing `root` logins over SSH requires system admins to authenticate using their own individual account, then escalating to `root`. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

Audit:

Run the following command to verify `PermitRootLogin` is set to `no`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep permitrootlogin

permitrootlogin no
```

Run the following command:

```
# grep -Psi '^\h*PermitRootLogin\h+\"?(yes|prohibit-password|forced-commands-
only)\b' /etc/ssh/sshd_config

Nothing should be returned
```

Note: If `Match` statements are used in your environment, these locations should be checked for the correct configuration as well.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `PermitRootLogin` parameter to `no` above any `Match` entries as follows:

```
PermitRootLogin no
```

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Default Value:

PermitRootLogin without-password

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5:AC-6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

4.2.21 Ensure sshd PermitUserEnvironment is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitUserEnvironment` option allows users to present environment options to the SSH daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

Audit:

Run the following command to verify `PermitUserEnviroment` is set to `no`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep permituserenvironment

permituserenvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter `PermitUserEnvironment` to `no`:

```
PermitUserEnvironment no
```

Note: First occurrence of a option takes precedence.

Default Value:

PermitUserEnvironment no

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021	TA0008	M1042

4.2.22 Ensure sshd UsePAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `UsePAM` directive enables the Pluggable Authentication Module (PAM) interface. If set to `yes` this will enable PAM authentication using `ChallengeResponseAuthentication` and `PasswordAuthentication` directives in addition to PAM account and session module processing for all authentication types.

Rationale:

When `usePAM` is set to `yes`, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Audit:

Run the following command to verify `UsePAM` is set to `yes`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(hostname -I | cut -d
' ' -f1)" | grep -i usepam

usepam yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `UsePAM` parameter to `yes`:

```
UsePAM yes
```

Note: First occurrence of a option takes precedence.

Default Value:

UsePAM yes

References:

1. SSHD_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0001	M1035

4.3 Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

sudo

https://www.sudo.ws/

The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

`sudo` supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, which is configured via the file `/etc/sudoers` and any entries in `/etc/sudoers.d`.

pkexec

https://www.freedesktop.org/software/polkit/docs/0.105/pkexec.1.html

4.3.1 Ensure sudo is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`sudo` allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

Rationale:

`sudo` supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, which is configured via the file `/etc/sudoers` and any entries in `/etc/sudoers.d`.

The security policy determines what privileges, if any, a user has to run `sudo`. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, `sudo` will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

Audit:

Verify that `sudo` is installed.
Run the following command:

```
# rpm -q sudo

sudo-<version>
```

Remediation:

Run the following command to install sudo

```
# yum install sudo
```

References:

1. SUDO(8)
2. NIST SP 800-53 Rev. 5: AC-6(2), AC-6(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548	TA0004	M1026

4.3.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`sudo` can be configured to run only from a pseudo terminal (`pseudo-pty`).

Rationale:

Attackers can run a malicious program using `sudo` which would fork a background process that remains even when the main program has finished executing.

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Audit:

Verify that `sudo` can only run other commands from a pseudo terminal.
Run the following command:

```
# grep -rPi '^\h*Defaults\h+([^#\n\r]+,)?use_pty(,\h*\h+\h*)*\h*(#.*)?$'
/etc/sudoers*

/etc/sudoers:Defaults use_pty
```

Remediation:

Edit the file `/etc/sudoers` with `visudo` or a file in `/etc/sudoers.d/` with `visudo -f` *<PATH_TO_FILE>* and add the following line:

```
Defaults use_pty
```

Note:

- sudo will read each file in `/etc/sudoers.d`, skipping file names that end in `~` or contain a `.` character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

References:

1. SUDO(8)
2. VISUDO(8)
3. NIST SP 800-53 Rev. 5: AC-6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.003, T1548, T1548.003	TA0001, TA0003	M1026, M1038

4.3.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `Defaults logfile` entry sets the path to the sudo log file. Setting a path turns on logging to a file; negating this option turns it off. By default, sudo logs via syslog.

Rationale:

Defining a dedicated log file for sudo simplifies auditing of sudo commands and creation of auditd rules for sudo.

Impact:

WARNING: Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

Creation of additional log files can cause disk space exhaustion if not correctly managed. You should configure `logrotate` to manage the sudo log in accordance with your local policy.

Audit:

Run the following command to verify that sudo has a custom log file configured

```
# grep -rPsi
"^\h*Defaults\h+([^#]+,\h*)?logfile\h*=\h*(\"|\')?\H+(\"|\')?(,\h*\H+\h*)*\h*
(#.*)?$" /etc/sudoers*
```

Example output:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with visudo or visudo -f <PATH TO FILE> and add the following line:

```
Defaults  logfile="<PATH TO CUSTOM LOG FILE>"
```

Example

```
Defaults logfile="/var/log/sudo.log"
```

Note:

- sudo will read each file in `/etc/sudoers.d`, skipping file names that end in `~` or contain a `.` character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

References:

1. SUDO(8)
2. VISUDO(8)
3. sudoers(5)
4. NIST SP 800-53 Rev. 5: AU-3, AU-12

Additional Information:

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1026

4.3.4 Ensure users must provide password for escalation (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must be configured so that users must provide a password for privilege escalation.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Impact:

This will prevent automated processes from being able to elevate privileges. To include Ansible and AWS builds

Audit:

Note: If passwords are not being used for authentication, this is not applicable.
Verify the operating system requires users to supply a password for privilege escalation.
Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*NOPASSWD" /etc/sudoers*
```

If any line is found refer to the remediation procedure below.

Remediation:

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.
Remove any line with occurrences of `NOPASSWD` tags in the file.

References:

1. NIST SP 800-53 Rev. 5: AC-6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

4.3.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The operating system must be configured so that users must re-authenticate for privilege escalation.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Audit:

Verify the operating system requires users to re-authenticate for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*\!authenticate" /etc/sudoers*
```

If any line is found with a `!authenticate` tag, refer to the remediation procedure below.

Remediation:

Configure the operating system to require users to reauthenticate for privilege escalation.
Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.
Remove any occurrences of `!authenticate` tags in the file(s).

References:

1. NIST SP 800-53 Rev. 5: AC-6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

4.3.6 Ensure sudo authentication timeout is configured correctly (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`sudo` caches used credentials for a default of 5 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

Audit:

Ensure that the caching timeout is no more than 15 minutes.
Example:

```
# grep -roP "timestamp_timeout=\K[0-9]*" /etc/sudoers*
```

If there is no `timestamp_timeout` configured in `/etc/sudoers*` then the default is 5 minutes. This default can be checked with:

```
# sudo -V | grep "Authentication timestamp timeout:"
```

NOTE: A value of `-1` means that the timeout is disabled. Depending on the configuration of the `timestamp_type`, this could mean for all terminals / processes of that user and not just that one single terminal session.

Remediation:

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on its own, or on the same line as `env_reset`. See the following two examples:

```
Defaults    env_reset, timestamp_timeout=15
Defaults    timestamp_timeout=15
Defaults    env_reset
```

References:

1. https://www.sudo.ws/man/1.9.0/sudoers.man.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

4.3.7 Ensure access to the su command is restricted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in a specific groups to execute `su`. This group should be empty to reinforce the use of `sudo` for privileged access.

Rationale:

Restricting the use of `su` , and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo` , whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following command:

```
# grep -Pi
'^\h*auth\h+[^#\n\r]+\h+pam_wheel\.so\h+([^#\n\r]+\h+)?(use_uid|group=\H+)\h+
([^#\n\r]+\h+)?(use_uid|group=\H+)\b' /etc/pam.d/su

auth required pam_wheel.so use_uid group=<group_name>
```

Example output:

```
auth            required        pam_wheel.so use_uid group=sugroup
```

Run the following command and verify that the group specified in `<group_name>` contains no users:

```
# grep <group_name> /etc/group

<group_name>:x:<GID>:
```

There should be no users listed after the Group ID field.

Remediation:

Create an empty group that will be specified for use of the `su` command. The group should be named according to site policy.
Example:

```
# groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:

```
auth required pam_wheel.so use_uid group=sugroup
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078	TA0005	M1026

4.4 Configure Pluggable Authentication Modules

Pluggable Authentication Modules (PAM) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

4.4.1 Configure PAM software packages

Updated versions of PAM and authselect include additional functionality

4.4.1.1 Ensure latest version of pam is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Updated versions of PAM include additional functionality

Rationale:

To ensure the system has full functionality and access to the options covered by this Benchmark, pam-1.3.1-25 or latter is required

Audit:

Run the following command to verify the version of `PAM` on the system:

```
# rpm -q pam
```

The output should be similar to:

```
pam-1.1.8-23
```

Remediation:

- IF - the version of `PAM` on the system is less that version `pam-1.1.8-23.`:
Run the following command to update to the latest version of `PAM`:

```
# yum upgrade pam
```

4.4.1.2 Ensure libpwquality is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The libpwquality package provides common functions for password quality checking

Rationale:

Strong passwords reduce the risk of systems being hacked through brute force methods.

Audit:

Run the following command to verify `libpwquility` is installed:

```
# rpm -q libpwquality

libpwquality-<version>
```

Remediation:

Run the following command to install `libpwquality`:

```
# yum install libpwquality
```

References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004		

4.4.2 Configure pluggable module arguments

Pluggable Authentication Modules (PAM) uses arguments to pass information to a pluggable module during authentication for a particular module type. These arguments allow the PAM configuration files for particular programs to use a common PAM module but in different ways.

Invalid arguments are ignored and do not otherwise affect the success or failure of the PAM module. When an invalid argument is passed, an error is usually written to `/var/log/messages` file. However, since the reporting method is controlled by the PAM module, the module must be written correctly to log the error to this file.

4.4.2.1 Configure pam_faillock module

`pam_faillock.so` provides a way to configure the default settings for locking the user after multiple failed authentication attempts.

Options:

- `<dir=/path/to/tally-directory>` - The directory where the user files with the failure records are kept. The default is /var/run/faillock. Note: These files will disappear after reboot on systems configured with directory /var/run/faillock mounted on virtual memory.
- `audit` - Will log the user name into the system log if the user is not found.
- `silent` - Don't print informative messages to the user. Please note that when this option is not used there will be difference in the authentication behavior for users which exist on the system and non-existing users.
- `no_log_info` - Don't log informative messages via syslog(3).
- `local_users_only` - Only track failed user authentications attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users. The faillock(8) command will also no longer track user failed authentication attempts. Enabling this option will prevent a double-lockout scenario where a user is locked out locally and in the centralized mechanism.
- `nodelay` - Don't enforce a delay after authentication failures.
- `deny=<n>` - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds . The default is 3.
- `fail_interval=n` - The length of the interval during which the consecutive authentication failures must happen for the user account lock out is n seconds. The default is 900 (15 minutes).
- `unlock_time=n` - The access will be re-enabled after n seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the faillock(8) command. The default is 600 (10 minutes). Note that the default directory that pam_faillock uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the dir option. Also note that it is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- `even_deny_root` - Root account can become locked as well as regular accounts.
- `root_unlock_time=n` - This option implies even_deny_root option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the unlock_time option.
- `admin_group=name` - If a group name is specified with this option, members of the group will be handled by this module the same as the root account (the options even_deny_root and root_unlock_time will apply to them. By default the option is not set.

4.4.2.1.1 Ensure pam_faillock module is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_faillock.so` module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications (this is defined by the `deny` parameter in the faillock configuration). It stores the failure records into per-user files in the tally directory.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Run the following commands to verify that `pam_faillock` is enabled:

```
# grep -P -- '\bpam_faillock.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth        required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/password-auth:auth        [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root

/etc/pam.d/password-auth:account     required        pam_faillock.so

/etc/pam.d/system-auth:auth          required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/system-auth:auth          [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root

/etc/pam.d/system-auth:account       required        pam_faillock.so
```

Remediation:

Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:
Add the following lines to the `auth` section:

```
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root
```

The `auth` sections should look similar to the following example:
WARNING: The ordering on the lines in the auth section is important. The `preauth` line needs to below the line `auth required pam_env.so` and above all password validation lines. The `authfail` line needs to be after all password validation lines such as `pam_sss.so`. **Incorrect order can cause you to be locked out of the system.**
Example:

```
auth        required      pam_env.so
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root # <- Under "auth required pam_env.so"
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root # <- Last auth line before "auth requisite
pam_succeed_if.so"
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
```

Add the following line to the `account` section:

```
account     required      pam_faillock.so
```

Example:

```
account     required     pam_faillock.so
account     required     pam_unix.so
account     sufficient   pam_localuser.so
account     sufficient   pam_pam_succeed_if.so uid < 1000 quiet
account     required     pam_permit.so
```

References:

1. faillock(8) - Linux man page
2. pam_faillock(8) - Linux man page
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

4.4.2.1.2 Ensure password failed attempts lockout is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `deny=<n>` option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds .

Rationale:

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Run the following command to verify that Number of failed logon attempts before the account is locked is no greater than `5` and meets local site policy:

```
# grep -Pi --
'^\h*auth\h+([^#\n\r]+)\h+pam_faillock\.so\h+(preauth|authfail)\h+([^#\n\r]+\
h+)?deny=[1-5]\b' /etc/pam.d/{system,password}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth        required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/password-auth:auth        [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root

/etc/pam.d/system-auth:auth          required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/system-auth:auth          [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root
```

Verify the lines include the `deny=` option, the the value is between `1` and `5`, and follows local site policy.

Remediation:

Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:
Add the following lines to the `auth` section:

```
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root
```

The `auth` sections should look similar to the following example:
Example:

```
auth        required      pam_env.so
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root # <- Under "auth required pam_env.so"
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root # <- Last auth line before "auth requisite
pam_succeed_if.so"
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
```

WARNING: The ordering on the lines in the auth section is important. The `preauth` line needs to below the line `auth required pam_env.so` and above all password validation lines. The `authfail` line needs to be after all password validation lines such as `pam_sss.so`. **Incorrect order can cause you to be locked out of the system.**

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

4.4.2.1.3 Ensure password unlock time is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`unlock_time=<n>` - The access will be re-enabled after seconds after the lock out. The value `0` has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the faillock(8) command.

Note:

- The default directory that pam_faillock uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the dir option.
- It is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- The maximum configurable value for `unlock_time` is `604800`

Rationale:

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Impact:

Use of `unlock_time=0` may allow an attacker to cause denial of service to legitimate users. This will also require a systems administrator with elevated privileges to unlock the account.

Audit:

Run the following command to verify that the time in seconds before the account is unlocked is either `0` (never) or `900` (15 minutes) or more and meets local site policy:

```
# grep -Pi --
'^\h*auth\h+([^#\n\r]+)\h+pam_faillock\.so\h+(preauth|authfail)\h+([^#\n\r]+\
h+)?unlock_time=(0|9[0-9][0-9]|[1-9][0-9]{3,})\b'
/etc/pam.d/{system,password}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth        required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/password-auth:auth        [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root

/etc/pam.d/system-auth:auth          required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/system-auth:auth          [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root
```

Verify the lines include the `unlock_time=` option, the the value is `0` or greater than `900`, and follows local site policy.

Remediation:

Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:
Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:
Add the following lines to the `auth` section:

```
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root
```

The `auth` sections should look similar to the following example:
Example:

```
auth        required      pam_env.so
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root # <- Under "auth required pam_env.so"
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root # <- Last auth line before "auth requisite
pam_succeed_if.so"
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
```

WARNING: The ordering on the lines in the auth section is important. The `preauth` line needs to below the line `auth required pam_env.so` and above all password validation lines. The `authfail` line needs to be after all password validation lines such as `pam_sss.so`. **Incorrect order can cause you to be locked out of the system.**

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

4.4.2.1.4 Ensure password failed attempts lockout includes root account (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`even_deny_root` - Root account can become locked as well as regular accounts

`root_unlock_time=n` - This option implies even_deny_root option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the unlock_time option.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Impact:

Use of `unlock_time=0` or `root_unlock_time=0` may allow an attacker to cause denial of service to legitimate users.

Audit:

Run the following command to verify that `even_deny_root` and/or `root_unlock_time` is enabled:

```
# grep -Pi --
'(?i)^\h*auth\h+([^#\n\r]+)\h+pam_faillock\.so\h+(auth|preauth)\h+([^#\n\r]+\
h+)?(even_deny_root|root_unlock_time=([6-9][0-9]{1,}))\b'
/etc/pam.d/{system,password}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth        required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/password-auth:auth        [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root

/etc/pam.d/system-auth:auth          required        pam_faillock.so preauth
silent audit deny=5 unlock_time=900 even_deny_root
/etc/pam.d/system-auth:auth          [default=die]   pam_faillock.so authfail
audit deny=5 unlock_time=900 even_deny_root
```

Verify the lines include the `even_deny_root` and/or `root_unlock_time=` option, the same option(s) exist on all lines, and follows local site policy.
- IF - `root_unlock_time` is set, verify it is set to `60` (One minute) or more.

Remediation:

Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:
Add the following lines to the `auth` section:

```
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root
```

The `auth` sections should look similar to the following example:
Example:

```
auth        required      pam_env.so
auth        required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 even_deny_root # <- Under "auth required pam_env.so"
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 even_deny_root # <- Last auth line before "auth requisite
pam_succeed_if.so"
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
```

WARNING: The ordering on the lines in the auth section is important. The `preauth` line needs to below the line `auth required pam_env.so` and above all password validation lines. The `authfail` line needs to be after all password validation lines such as `pam_sss.so`. **Incorrect order can cause you to be locked out of the system.**

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

4.4.2.2 Configure pam_pwquality module

The `pam_pwquality.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

These checks are configurable by either:

- use of the module arguments
- modifying the `/etc/security/pwquality.conf` configuration file

Note: The module arguments override the settings in the `/etc/security/pwquality.conf` configuration file.

4.4.2.2.1 Ensure pam_pwquality module is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_pwquality.so` module performs password quality checking. This module can be plugged into the password stack of a given service to provide strength-checking for passwords. The code was originally based on pam_cracklib module and the module is backwards compatible with its options.

The action of this module is to prompt the user for a password and check its strength against a system dictionary and a set of rules for identifying poor choices.

The first action is to prompt for a single password, check its strength and then, if it is considered strong, prompt for the password a second time (to verify that it was typed correctly on the first occasion). All being well, the password is passed on to subsequent modules to be installed as the new authentication token.

Rationale:

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

Audit:

Run the following commands to verify that `pam_pwquality` is enabled:

```
# grep -P -- '\bpam_pwquality\.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password   requisite   pam_pwquality.so
local_users_only
/etc/pam.d/system-auth:password   requisite   pam_pwquality.so
local_users_only
```

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Add the following line to the `password` section:

```
password    requisite    pam_pwquality.so try_first_pass local_users_only
```

Example password section:

```
password    requisite     pam_pwquality.so try_first_pass local_users_only
retry=3 #<- added pam_pwquality.so line
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
password    required      pam_deny.so
```

Note: the `use_authtok` option should exist on all password lines except the first entry and the `pam_deny.so` line

References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.2 Ensure password number of changed characters is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pwquality difok` option sets the number of characters in a password that must not be present in the old password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Run the following command to verify that the `difok` option is set to `2` or more and follows local site policy:

```
# grep -Psi -- '^\h*difok\h*=\h*([2-9]|[1-9][0-9]+)\b'
/etc/security/pwquality.conf

difok = 2
```

Verify returned value is `2` or more and meet local site policy
Run the following command to verify that `difok` is not set, is `2` or more, and conforms to local site policy:

```
grep -Psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?difok\h*=\h*([0-1])\b' /etc/pam.d/system-auth /etc/pam.d/password-
auth

Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity
- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit or add the following line in `/etc/security/pwquality.conf` to a value of `2` or more and meets local site policy:

```
difok = 2
```

Example:

```
# sed -ri 's/^\s*difok\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "difok = 2" >> /etc/security/pwquality.conf
```

Run the following script to remove setting `difok` on the `pam_pwquality.so` module in the PAM files:

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
difok\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

difok = 1

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.3 Ensure password length is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`minlen` - Minimum acceptable size for the new password (plus one if credits are not disabled which is the default). Cannot be set to lower value than 6.

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Run the following command to verify that password length is `14` or more characters, and conforms to local site policy:

```
# grep -Psi -- '^\h*minlen\h*=\h*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b'
/etc/security/pwquality.conf

minlen = 14
```

Run the following command to verify that `minlen` is not set, or is `14` or more characters, and conforms to local site policy:

```
grep -Psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?minlen\h*=\h*([0-9]|1[0-3])\b' /etc/pam.d/{password,system}-auth

Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity
- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit the file `/etc/security/pwquality.conf` and add or modify the following line to set password length of `14` or more characters. Ensure that password length conforms to local site policy:

```
minlen = 14
```

Run the following script to remove setting `minlen` on the `pam_pwquality.so` module in the PAM files:

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
minlen\s*=\s*[0-9]+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

minlen = 8

References:

1. pam_pwquality(8)
2. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.4 Ensure password complexity is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Password complexity can be set through:

- `minclass` - The minimum number of classes of characters required in a new password. (digits, uppercase, lowercase, others). e.g. `minclass = 4` requires digits, uppercase, lower case, and special characters.
- `dcredit` - The maximum credit for having digits in the new password. If less than `0` it is the minimum number of digits in the new password. e.g. `dcredit = -1` requires at least one digit
- `ucredit` - The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. e.g. `ucredit = -1` requires at least one uppercase character
- `ocredit` - The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. e.g. `ocredit = -1` requires at least one special character
- `lcredit` - The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. e.g. `lcredit = -1` requires at least one lowercase character

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Run the following command to verify that complexity conforms to local site policy:

```
# grep -Psi -- '^\h*(minclass|[dulo]credit)\b' /etc/security/pwquality.conf
```

Example output:

```
minclass = 4
  -- AND/OR --
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Run the following command to verify that:

- `minclass` is not set to less than `4`
- `dcredit`, `ucredit`, `lcredit`, and `ocredit` are not set to `0` or greater

```
grep -Psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?(minclass=[0-3]|[dulo]credit=[^-]\d*)\b'
/etc/pam.d/{password,system}-auth

Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity
- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit `/etc/security/pwquality.conf` and add or modify the following line to set:

```
minclass = 4
```

--AND/OR--

```
dcredit = -_N>
ucredit = <N>
ocredit = <N>
lcredit = <N>
```

Example:

```
# printf '\n%s' "minclass = 4" >> /etc/security/pwquality.conf
```

--AND/OR--

```
# printf '%s\n' "dcredit = -1" "ucredit = -1" "ocredit = -1" "lcredit = -1"
>> /etc/security/pwquality.conf
```

Run the following script to remove setting `minclass`, `dcredit`, `ucredit`, `lcredit`, and `ocredit` on the `pam_pwquality.so` module in the PAM files

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
minclass\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
dcredit\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
ucredit\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
lcredit\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
ocredit\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

minclass = 0

dcredit = 0

ucredit = 0

ocredit = 0

lcredit = 0

References:

1. pam_pwquality(8)
2. PWQUALITY.CONF(5)
3. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.5 Ensure password same consecutive characters is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pwquality maxrepeat` option sets the maximum number of allowed same consecutive characters in a new password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Run the following command to verify that the `maxrepeat` option is set to `3` or less, not `0`, and follows local site policy:

```
# grep -Psi -- '^\h*maxrepeat\h*=\h*[1-3]\b' /etc/security/pwquality.conf

maxrepeat = 3
```

Verify returned value(s) are `3` or less, not `0`, and meet local site policy
Run the following command to verify that `maxrepeat` is not set, is `3` or less, not `0`, and conforms to local site policy:

```
grep -Psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?maxrepeat\h*=\h*(0|[4-9]|[1-9][0-9]+)\b'
/etc/pam.d/{password,system}-auth
Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity
- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit `/etc/security/pwquality.conf` and add or modify the following line to set `maxrepeat` to `3` or less and not `0`. Ensure setting conforms to local site policy:

```
maxrepeat = 3
```

Run the following script to remove setting `maxrepeat` on the `pam_pwquality.so` module in the PAM files:

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
maxrepeat\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

maxrepeat = 0

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.6 Ensure password maximum sequential characters is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pwquality maxsequence` option sets the maximum length of monotonic character sequences in the new password. Examples of such sequence are `12345` or `fedcb`. The check is disabled if the value is `0`.

Note: Most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Run the following command to verify that the `maxsequence` option is set to `3` or less, not `0`, and follows local site policy:

```
# grep -Psi -- '^\h*maxsequence\h*=\h*[1-3]\b' /etc/security/pwquality.conf

maxsequence = 3
```

Verify returned value(s) are `3` or less, not `0`, and meet local site policy
Run the following command to verify that `maxsequence` is not set, is `3` or less, not `0`, and conforms to local site policy:

```
grep -Psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?maxsequence\h*=\h*(0|[4-9]|[1-9][0-9]+)\b'
/etc/pam.d/{password,system}-auth

Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity
- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit `/etc/security/pwquality.conf` and add or modify the following line to set `maxsequence` to `3` or less and not `0`. Ensure setting conforms to local site policy:

```
maxsequence = 3
```

Run the following script to remove setting `maxsequence` on the `pam_pwquality.so` module in the PAM files:

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
maxsequence\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

maxsequence = 0

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.2.7 Ensure password dictionary check is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pwquality dictcheck` option sets whether to check for the words from the `cracklib` dictionary.

Rationale:

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

Audit:

Run the following command to verify that the `dictcheck` option is not set to `0` (disabled) in `/etc/security/pwquality.conf`:

```
# grep -Psi -- '^\h*dictcheck\h*=\h*0\b' /etc/security/pwquality.conf

Nothing should be returned
```

Run the following command to verify that the `dictcheck` option is not set to `0` (disabled) as a module argument in a PAM file:

```
# grep -psi --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([^#\n\
r]+\h+)?dictcheck\h*=\h*0\b' /etc/pam.d/{password,system}-auth

Nothing should be returned
```

Note:

- Module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwquality.conf`

Remediation:

Edit `/etc/security/pwquality.conf` and comment out or remove any instance of `dictcheck = 0`:
Example:

```
# sed -ri 's/^\s*dictcheck\s*=/# &/' /etc/security/pwquality.conf
```

Run the following script to remove setting `dictcheck` on the `pam_pwquality.so` module in the PAM files:

```
#!/usr/bin/env bash

{
   for l_pam_file in system-auth password-auth; do
     sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*)(\s+
dictcheck\s*=\s*\S+)(.*$)/\1\4/' /etc/pam.d/"$l_pam_file"
   done
}
```

Default Value:

dictcheck = 1

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.3 Configure pam_pwhistory module

`pam_pwhistory` - PAM module to remember last passwords

`pam_history.so` module - This module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with `NIS` or `LDAP`, since the old passwords are stored on the local machine and are not available on another machine for password history checking.

Options:

- `debug` - Turns on debugging via syslog(3).
- `use_authtok` - When password changing enforce the module to use the new password provided by a previously stacked password module (this is used in the example of the stacking of the `pam_passwdqc module` documented below).
- `enforce_for_root` - If this option is set, the check is enforced for root, too.
- `remember=<N>` - The last <*N*> passwords for each user are saved. The default is `10`. Value of `0` makes the module to keep the existing contents of the opasswd file unchanged.
- `retry=<N>` - Prompt user at most <*N*> times before returning with error. The default is `1`.
- `authtok_type=<STRING>` - See pam_get_authtok(3) for more details.

The options for configuring the module behavior are described in the pwhistory.conf(5) manual page.

4.4.2.3.1 Ensure pam_pwhistory module is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_history.so` module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

Audit:

Run the following commands to verify that `pam_pwhistory` is enabled:

```
# grep -P -- '\bpam_pwhistory\.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password   required   pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
/etc/pam.d/system-auth:password   required   pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
```

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Add the following line to the `password` section:

```
password   required   pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
```

Example password section:

```
password    requisite     pam_pwquality.so try_first_pass local_users_only
retry=3
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
password    required      pam_deny.so
```

Note: the `use_authtok` option should exist on all password lines except the first entry and the `pam_deny.so` line

References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.3.2 Ensure password history remember is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

- remember=<N> - `<N>` is the number of old passwords to remember

Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

Note: These change only apply to accounts configured on the local system.

Audit:

Run the following command and verify that the remember option is set to `24` or more and meets local site policy in `/etc/security/pwhistory.conf`:

```
# grep -Pi --
'^\h*password\h+(required|requisite)\h+pam_pwhistory\.so\h+([^#\n\r]+\h+)?rem
ember=(2[4-9]|[3-9][0-9]|[1-9][0-9]{2,})\b' /etc/pam.d/{system,password}-auth

remember = 24
```

Output should be similar to:

```
/etc/pam.d/system-auth:password    required      pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
/etc/pam.d/password-auth:password    required      pam_pwhistory.so
remember=24 enforce_for_root try_first_pass use_authtok
```

Verify the lines include the `remember=` option with a value of `24` or more and follows local site policy

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Add the following line to the `password` section:

```
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
```

Example password section:

```
password    requisite     pam_pwquality.so try_first_pass local_users_only
retry=3
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
password    required      pam_deny.so
```

Note: the `use_authtok` option should exist on all password lines except the first entry and the `pam_deny.so` line

References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004		

4.4.2.3.3 Ensure password history is enforced for the root user (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

If the `pwhistory` `enforce_for_root` option is enabled, the module will enforce password history for the root user as well

Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password

Note: These change only apply to accounts configured on the local system.

Audit:

Run the following command to verify that the `enforce_for_root` option is enabled:

```
# grep -Pi --
'^\h*password\h+(required|requisite)\h+pam_pwhistory\.so\h+([^#\n\r]+\h+)?enf
orce_for_root\b' /etc/pam.d/{system,password}-auth
```

Output should be similar to:

```
/etc/pam.d/system-auth:password    required      pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
/etc/pam.d/password-auth:password    required      pam_pwhistory.so
remember=24 enforce_for_root try_first_pass use_authtok
```

Verify the lines include the `enforce_for_root` option

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Add the following line to the `password` section:

```
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
```

Example password section:

```
password    requisite     pam_pwquality.so try_first_pass local_users_only
retry=3 #<- added pam_pwquality.so line
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
password    required      pam_deny.so
```

Note: the `use_authtok` option should exist on all password lines except the first entry and the `pam_deny.so` line

Default Value:

disabled

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004	TA0006	M1027

4.4.2.3.4 Ensure pam_pwhistory includes use_authtok (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`use_authtok` - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

Rationale:

`use_authtok` allows multiple pam modules to confirm a new password before it is accepted.

Audit:

Run the following command to verify that `use_authtok` is set on the pam_pwhistory.so module lines in the password stack:

```
# grep -P --
'^\h*password\h+([^#\n\r]+)\h+pam_pwhistory\.so\h+([^#\n\r]+\h+)?use_authtok\
b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    required      pam_pwhistory.so
remember=24 enforce_for_root try_first_pass use_authtok
/etc/pam.d/system-auth:password    required      pam_pwhistory.so remember=24
enforce_for_root try_first_pass use_authtok
```

Verify that the lines include `use_authtok` option

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Add the following line to the `password` section:

```
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
```

Example password section:

```
password    requisite     pam_pwquality.so try_first_pass local_users_only
retry=3 #<- added pam_pwquality.so line
password    required      pam_pwhistory.so remember=24 enforce_for_root
try_first_pass use_authtok
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
password    required      pam_deny.so
```

Note: the `use_authtok` option should exist on all password lines except the first entry and the `pam_deny.so` line

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.4.2.4 Configure pam_unix module

The `pam_unix.so` module is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the `/etc/passwd` and the `/etc/shadow` file as well if shadow is enabled.

4.4.2.4.1 Ensure pam_unix does not include nullok (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nullok` argument overrides the default action of `pam_unix.so` to not permit the user access to a service if their official password is blank.

Rationale:

Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

Audit:

Run the following command to verify that the `nullok` argument is not set on the `pam_unix.so` module:

```
# grep -P --
'^\h*(auth|account|password|session)\h+(requisite|required|sufficient)\h+pam_
unix\.so\b' /etc/pam.d/{password,system}-auth | grep -Pv -- '\bnullok\b'
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth   sufficient   pam_unix.so try_first_pass
/etc/pam.d/password-auth:account   required   pam_unix.so
/etc/pam.d/password-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok
/etc/pam.d/password-auth:session   required   pam_unix.so

/etc/pam.d/system-auth:auth   sufficient   pam_unix.so try_first_pass
/etc/pam.d/system-auth:account   required   pam_unix.so
/etc/pam.d/system-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok
/etc/pam.d/system-auth:session   required   pam_unix.so
```

Verify that none of the `pam_unix` lines include the `nullok` option

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Edit the following lines and remove the `nullok` option:

```
auth        sufficient   pam_unix.so try_first_pass
account     required     pam_unix.so
password    sufficient   pam_unix.so sha512 shadow try_first_pass use_authtok
session     required     pam_unix.so
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.4.2.4.2 Ensure pam_unix does not include remember (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `remember=n` argument saves the last n passwords for each user in `/etc/security/opasswd` in order to force password change history and keep the user from alternating between the same password too frequently. The MD5 password hash algorithm is used for storing the old passwords. Instead of this option the `pam_pwhistory` module should be used. The `pam_pwhistory` module saves the last n passwords for each user in `/etc/security/opasswd` using the password hash algorithm set on the `pam_unix` module. This allows for the `sha512` hash algorithm to be used.

Rationale:

The `remember=n` argument should be removed to ensure a strong password hashing algorithm is being used. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user's old passwords stored in `/etc/security/opasswd`.

Audit:

Run the following command to verify that the `remember` argument is not set on the `pam_unix.so` module:

```
# grep -Pi '^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\b'
/etc/pam.d/{password,system}-auth | grep -Pv '\bremember=\d\b'
```

Output should be similar to:

```
/etc/pam.d/password-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok

/etc/pam.d/system-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok
```

Verify that none of the `pam_unix` lines include the `remember=` option

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Edit the following lines and remove the `remember=` option:

```
auth        sufficient    pam_unix.so try_first_pass
account     required      pam_unix.so
password    sufficient    pam_unix.so sha512 shadow try_first_pass use_authtok
session     required      pam_unix.so
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.4.2.4.3 Ensure pam_unix includes a strong password hashing algorithm (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

Rationale:

The `SHA-512` algorithm provides a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

Note: These changes only apply to the local system.

Audit:

Run the following command to verify that a strong password hashing algorithm is set on the pam_unix.so module:

```
# grep -P --
'^\h*password\h+([^#\n\r]+)\h+pam_unix\.so\h+([^#\n\r]+\h+)?sha512\b'
/etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password   sufficient   pam_unix.so sha512 shadow
use_authtok

/etc/pam.d/system-auth:password   sufficient   pam_unix.so sha512 shadow
use_authtok
```

Verify that the lines include `sha512` and do no include `md5`, `bigcrypt`, `sha256`, or `blowfish`

Remediation:

Note: This only effects local users and passwords created after updating the files to use `sha512`. If it is determined that the password algorithm being used is not `sha512`, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login.
Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Edit the following lines and:

- Add the `sha512` argument
- Remove all `md5`, `bigcrypt`, `sha256`, and `blowfish` arguments

```
auth        sufficient    pam_unix.so try_first_pass
account     required      pam_unix.so
password    sufficient    pam_unix.so sha512 shadow try_first_pass use_authtok
session     required      pam_unix.so
```

References:

1. NIST SP 800-53 Rev. 5: IA-5

Additional Information:

Additional module options may be set, recommendation only covers those listed here.

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '( $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $1 !=
"nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.4.2.4.4 Ensure pam_unix includes use_authtok (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`use_authtok` - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

Rationale:

`use_authtok` allows multiple pam modules to confirm a new password before it is accepted.

Audit:

Run the following command to verify that `use_authtok` is set on the pam_unix.so module lines in the password stack:

```
# grep -P --
'^\h*password\h+([^#\n\r]+)\h+pam_unix\.so\h+([^#\n\r]+\h+)?use_authtok\b'
/etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok

/etc/pam.d/system-auth:password   sufficient   pam_unix.so sha512 shadow
try_first_pass use_authtok
```

Verify that the lines include `use_authtok`

Remediation:

Edit the files /etc/pam.d/system-auth and /etc/pam.d/password-auth:
Edit the following line and add the `use_authtok` argument:

```
password   sufficient   pam_unix.so sha512 shadow try_first_pass use_authtok
```

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

4.5.1 Configure shadow password suite parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

4.5.1.1 Ensure strong password hashing algorithm is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

Rationale:

The `SHA-512` and `yescrypt` algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

Note: These changes only apply to the local system.

Audit:

Note: `yescrypt` is not currently supported in Fedora 28 based distributions. It has been included as an acceptable option if it becomes available in a future update to the Operating System.
Verify password hashing algorithm is sha512 or yescrypt:
Run the following command to verify the hashing algorithm is `sha512` or `yescrypt` in `/etc/libuser.conf`:

```
# grep -Pi -- '^\h*crypt_style\h*=\h*(sha512|yescrypt)\b' /etc/libuser.conf

crypt_style = sha512
```

Run the following command to verify the hashing algorithm is `sha512` or `yescrypt` in `/etc/login.defs`:

```
# grep -Pi -- '^\h*ENCRYPT_METHOD\h+(SHA512|yescrypt)\b' /etc/login.defs

ENCRYPT_METHOD SHA512
```

Remediation:

Note: If `yescrypt` becomes available in a future release, this would also be acceptable. It is highly recommended that the chosen hashing algorithm is consistent across `/etc/libuser.conf`, `/etc/login.defs`, `/etc/pam.d/password-auth`, and `/etc/pam.d/system-auth`.
Set password hashing algorithm to sha512.
Edit `/etc/libuser.conf` and edit or add the following line:

```
crypt_style = sha512
```

Edit `/etc/login.defs` and edit or add the following line:

```
ENCRYPT_METHOD SHA512
```

Note: This only effects local users and passwords created after updating the files to use `sha512` or `yescrypt`. If it is determined that the password algorithm being used is not `sha512` or `yescrypt`, once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.

References:

1. NIST SP 800-53 Rev. 5: IA-5

Additional Information:

Additional module options may be set, recommendation only covers those listed here.

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '( $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $1 !=
"nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1110, T1110.002	TA0006	M1041

4.5.1.2 Ensure password expiration is 365 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Impact:

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep PASS_MAX_DAYS /etc/login.defs

PASS_MAX_DAYS 365
```

Run the following command and Review list of users and PASS_MAX_DAYS to verify that all users' PASS_MAX_DAYS conforms to site policy (no more than 365 days):

```
# grep -E '^[^:]+:[^!*]' /etc/shadow | cut -d: -f1,5

<user>:<PASS_MAX_DAYS>
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs` :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

A value of -1 will disable password expiration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004		

4.5.1.3 Ensure password expiration warning days is 7 or more (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following command and verify `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep PASS_WARN_AGE /etc/login.defs

PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:
Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# awk -F: '/^[^:\n\r]+:[^!\*xX\n\r]/ {print $1 ":" $6}' /etc/shadow

<user>:<PASS_WARN_AGE>
```

Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs` :

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078	TA0006	M1027

4.5.1.4 Ensure inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify `INACTIVE` conforms to site policy (no more than 30 days):

```
# useradd -D | grep INACTIVE

INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires
Verify all users with a password have Password inactive no more than 30 days after password expires: Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# awk -F: '/^[^#:]+:[^!\*:]*:[^:]*:[^:]*:[^:]*:[^:]*:(\s*|-1|3[1-9]|[4-9][0-
9]|[1-9][0-9][0-9]+):[^:]*:[^:]*\s*$/ {print $1":"$7}' /etc/shadow

No <user>:<INACTIVE> should be returned
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.002, T1078.003	TA0001	M1027

4.5.1.5 Ensure all users last password change date is in the past (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

All users should have a password change date in the past.

Rationale:

If a user's recorded password change date is in the future, then they could bypass any set password expiration.

Audit:

Run the following command and verify nothing is returned

```
{
   while IFS= read -r l_user; do
      l_change=$(date -d "$(chage --list $l_user | grep '^Last password
change' | cut -d: -f2 | grep -v 'never$')" +%s)
      if [[ "$l_change" -gt "$(date +%s)" ]]; then
         echo "User: \"$l_user\" last password change was \"$(chage --list
$l_user | grep '^Last password change' | cut -d: -f2)\""
      fi
   done < <(awk -F: '/^[^:\n\r]+:[^!*xX\n\r]/{print $1}' /etc/shadow)
}
```

Remediation:

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004		

4.5.2 Configure root and system accounts and environment

4.5.2.1 Ensure default group for the root account is GID 0 (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `usermod` command can be used to specify which group the `root` account belongs to. This affects permissions of files that are created by the `root` account.

Rationale:

Using GID 0 for the `root` account helps prevent `root` -owned files from accidentally becoming accessible to non-privileged users.

Audit:

Run the following command to verify the `root` user's primary group ID is `0`:

```
# awk -F: '$1=="root"{print $1":"$4}' /etc/passwd

root:0
```

Remediation:

Run the following command to set the `root` user's default group ID to `0`:

```
# usermod -g 0 root
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0005	M1026

4.5.2.2 Ensure root user umask is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rwxrwxrwx`), and for any newly created file it is 0666 (`rw-rw-rw-`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either `Octal` or `Symbolic` values:

- `Octal` (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx,g=rx,o=` is the `Symbolic` equivalent of the `Octal` `umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

root user Shell Configuration Files:

- `/root/.bash_profile` - Is executed to configure the root users' shell before the initial command prompt. **Is only read by login shells.**
- `/root/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`.

Order of precedence:

1. `/root/.bash_profile`
2. `/root/.bashrc`
3. The system default umask

Rationale:

Setting a secure value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Audit:

Run the following to verify the root user `umask` is set to enforce a newly created directories' permissions to be `750 (drwxr-x---)`, and a newly created file's permissions be `640 (rw-r-----)`, or more restrictive:

```
grep -Psi -- '^\h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-
6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-
6]\b)|(u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?\b)(,o=[rwx]{1,3})?)|((g=[wrx
]{1,3},)?o=[wrx]{1,3}\b)))' /root/.bash_profile /root/.bashrc

Nothing should be returned
```

Remediation:

Edit `/root/.bash_profile` and `/root/.bashrc` and remove, comment out, or update any line with `umask` to be `0027` or more restrictive.

Default Value:

System default `umask`

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1083	TA0007	

4.5.2.3 Ensure system accounts are secured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the `nologin` shell. This prevents the account from potentially being used to run any commands.

Audit:

System accounts

Check critical system accounts for `nologin`
Run the following command:

```
# awk -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' || $3 == 65534) &&
$7!~/^(\/usr)?\/sbin\/nologin$/) { print $1 }' /etc/passwd
```

Verify no results are returned.

Disabled accounts

Ensure all accounts that configured the shell as `nologin` also have their passwords disabled.
Run the following command:

```
# awk -F: '/nologin/ {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

Verify no results are returned.

Remediation:

System accounts

Set the shell for any accounts returned by the audit to `nologin`:

```
# usermod -s $(command -v nologin) <user>
```

Disabled accounts

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

Large scale changes

The following command will set all system accounts to `nologin`:

```
# awk -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' || $3 == 65534)) { print $1 }'
/etc/passwd | while read user; do usermod -s $(command -v nologin) $user
>/dev/null; done
```

The following command will automatically lock all accounts that have their shell set to `nologin`:

```
# awk -F: '/nologin/ {print $1}' /etc/passwd | while read user; do usermod -L
$user; done
```

References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

Additional Information:

The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1026

4.5.2.4 Ensure root password is set (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system.

Rationale:

Access to `root` should be secured at all times.

Impact:

If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

Audit:

Run the following command:

```
# passwd -S root | grep -Poi 'Password\h+set\b' || echo "Password not set"

Password set
```

Remediation:

Set the `root` password with:

```
# passwd root
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078	TA0005	M1026

4.5.3 Configure user default environment

4.5.3.1 Ensure nologin is not listed in /etc/shells (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`/etc/shells` is a text file which contains the full pathnames of valid login shells. This file is consulted by `chsh` and available to be queried by other programs.

Be aware that there are programs which consult this file to find out if a user is a normal user; for example, FTP daemons traditionally disallow access to users with shells not included in this file.

Rationale:

A user can use `chsh` to change their configured shell.

If a user has a shell configured that isn't in in `/etc/shells`, then the system assumes that they're somehow restricted. In the case of `chsh` it means that the user cannot change that value.

Other programs might query that list and apply similar restrictions.

By putting `nologin` in `/etc/shells`, any user that has `nologin` as its shell is considered a full, unrestricted user. This is not the expected behavior for `nologin`.

Audit:

Run the following command to verify that `nologin` is not listed in the `/etc/shells` file:

```
# grep '/nologin\b' /etc/shells
```

Nothing should be returned

Remediation:

Edit `/etc/shells` and remove any lines that include `nologin`

References:

1. shells(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

4.5.3.2 Ensure default user shell timeout is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- TMOUT=*n* - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- export TMOUT - exports the TMOUT variable

System Wide Shell Configuration Files:

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive *login* shells, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `/etc/bashrc` also invokes /etc/profile.d/*.sh if *non-login* shell, but redirects output to `/dev/null` if *non-interactive.* **Is only executed for *interactive* shells or if `BASH_ENV` is set to `/etc/bashrc`.**

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

Audit:

Run the following script to verify that `TMOUT` is configured to: include a timeout of no more than `900` seconds, to be `readonly`, to be `exported`, and is not being changed to a longer timeout.

```
#!/usr/bin/env bash

{
   output1="" output2=""
   [ -f /etc/bashrc ] && BRC="/etc/bashrc"
   for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
      grep -Pq '^\s*([^#]+\s+)?TMOUT=(900|[1-8][0-9][0-9]|[1-9][0-9]|[1-
9])\b' "$f" && grep -Pq
'^\s*([^#]+;\s*)?readonly\s+TMOUT(\s+|\s*;|\s*$|=(900|[1-8][0-9][0-9]|[1-
9][0-9]|[1-9]))\b' "$f" && grep -Pq
'^\s*([^#]+;\s*)?export\s+TMOUT(\s+|\s*;|\s*$|=(900|[1-8][0-9][0-9]|[1-9][0-
9]|[1-9]))\b' "$f" &&
   output1="$f"
   done
   grep -Pq '^\s*([^#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+|[1-9]\d{3,})\b'
/etc/profile /etc/profile.d/*.sh "$BRC" && output2=$(grep -Ps
'^\s*([^#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+|[1-9]\d{3,})\b'
/etc/profile /etc/profile.d/*.sh $BRC)
   if [ -n "$output1" ] && [ -z "$output2" ]; then
      echo -e "\nPASSED\n\nTMOUT is configured in: \"$output1\"\n"
   else
      [ -z "$output1" ] && echo -e "\nFAILED\n\nTMOUT is not configured\n"
      [ -n "$output2" ] && echo -e "\nFAILED\n\nTMOUT is incorrectly
configured in: \"$output2\"\n"
   fi
}
```

Remediation:

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy. `TMOUT` should not exceed 900 or be equal to `0`.
Configure `TMOUT` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

`TMOUT` configuration examples:

- As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078	TA0005	M1026

4.5.3.3 Ensure default user umask is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rwxrwxrwx`), and for any newly created file it is 0666 (`rw-rw-rw-`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either `Octal` or `Symbolic` values:

- `Octal` (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx,g=rx,o=` is the `Symbolic` equivalent of the `Octal umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

The default `umask` can be set to use the `pam_umask` module or in a `System Wide Shell Configuration File`. The user creating the directories or files has the discretion of changing the permissions via the chmod command, or choosing a different default `umask` by adding the `umask` command into a `User Shell Configuration File`, (`.bash_profile` or `.bashrc`), in their home directory.

Setting the default umask:

- pam_umask module:
  - will set the umask according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to yes in `/etc/login.defs` (default):
    - will enable setting of the `umask` group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the `uid` is the same as `gid`, and `username` is the same as the `<primary group name>`

        - userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user
- `System Wide Shell Configuration File`:
    - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive *login* shells, or shells executed with the --login parameter.**
    - `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
    - `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes /etc/profile.d/*.sh if *non-login* shell, but redirects output to `/dev/null` if *non-interactive.* **Is only executed for *interactive* shells or if `BASH_ENV` is set to `/etc/bashrc`.**

User Shell Configuration Files:

- `~/.bash_profile` - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- `~/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`.

Order of precedence:

1. A file in `/etc/profile.d/` ending in `.sh` - This will override any other system-wide `umask` setting
2. In the file `/etc/profile`
3. On the `pam_umask.so` module in `/etc/pam.d/postlogin`
4. In the file `/etc/login.defs`
5. In the file `/etc/default/login`

Rationale:

Setting a secure default value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Audit:

Run the following to verify the default user `umask` is set to enforce a newly created directories' permissions to be `750 (drwxr-x---)`, and a newly created file's permissions be `640 (rw-r-----)`, or more restrictive:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   file_umask_chk()
   {
      if grep -Psiq -- '^\h*umask\h+(0?[0-7][2-
7]7|u(=[rwx]{0,3}),g=([rx]{0,2}),o=)(\h*#.*)?$' "$l_file"; then
         l_output="$l_output\n - umask is set correctly in \"$l_file\""
      elif grep -Psiq -- '^\h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-
7][0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-
6]\b)|(u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?\b)(,o=[rwx]{1,3})?)|((g=[wrx
]{1,3},)?o=[wrx]{1,3}\b)))' "$l_file"; then
         l_output2="$l_output2\n - umask is incorrectly set in \"$l_file\""
      fi
   }
   while IFS= read -r -d $'\0' l_file; do
      file_umask_chk
   done < <(find /etc/profile.d/ -type f -name '*.sh' -print0)
   l_file="/etc/profile" && file_umask_chk
   l_file="/etc/bashrc" && file_umask_chk
   l_file="/etc/bash.bashrc" && file_umask_chk
   l_file="/etc/pam.d/postlogin"
   if grep -Psiq --
'^\h*session\h+[^#\n\r]+\h+pam_umask\.so\h+([^#\n\r]+\h+)?umask=(0?[0-7][2-
7]7)\b' "$l_file"; then
      l_output1="$l_output1\n - umask is set correctly in \"$l_file\""
   elif grep -Psiq
'^\h*session\h+[^#\n\r]+\h+pam_umask\.so\h+([^#\n\r]+\h+)?umask=(([0-7][0-
7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b)|([0-7][01][0-7]\b))' "$l_file"; then
      l_output2="$l_output2\n - umask is incorrectly set in \"$l_file\""
   fi
   l_file="/etc/login.defs" && file_umask_chk
   l_file="/etc/default/login" && file_umask_chk
   [[ -z "$l_output" && -z "$l_output2" ]] && l_output2="$l_output2\n - umask
is not set"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2"
      [ -n "$l_output" ] && echo -e "\n- * Correctly configured *
:\n$l_output\n"
   fi
}
```

Remediation:

Run the following script and perform the instructions in the output:

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_out=""
   file_umask_chk()
   {
      if grep -Psiq -- '^\h*umask\h+(0?[0-7][2-
7]7|u(=[rwx]{0,3}),g=([rx]{0,2}),o=)(\h*#.*)?$' "$l_file"; then
         l_out="$l_out\n - umask is set correctly in \"$l_file\""
      elif grep -Psiq -- '^\h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-
7][0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-
6]\b)|(u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?\b)(,o=[rwx]{1,3})?)|((g=[wrx
]{1,3},)?o=[wrx]{1,3}\b)))' "$l_file"; then
         l_output2="$l_output2\n   - \"$l_file\""
      fi
   }
   while IFS= read -r -d $'\0' l_file; do
      file_umask_chk
   done < <(find /etc/profile.d/ -type f -name '*.sh' -print0)
   [ -n "$l_out" ] && l_output="$l_out"
   l_file="/etc/profile" && file_umask_chk
   l_file="/etc/bashrc" && file_umask_chk
   l_file="/etc/bash.bashrc" && file_umask_chk
   l_file="/etc/pam.d/postlogin"
   if grep -Psiq
'^\h*session\h+[^#\n\r]+\h+pam_umask\.so\h+([^#\n\r]+\h+)?umask=(([0-7][0-
7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b)|([0-7][01][0-7]\b))' "$l_file"; then
      l_output2="$l_output2\n   - \"$l_file\""
   fi
   l_file="/etc/login.defs" && file_umask_chk
   l_file="/etc/default/login" && file_umask_chk
   if [ -z "$l_output2" ]; then
      echo -e " - No files contain a UMASK that is not restrictive enough\n
No UMASK updates required to existing files"
   else
      echo -e "\n - UMASK is not restrictive enough in the following
file(s):$l_output2\n\n- Remediation Procedure:\n - Update these files and
comment out the UMASK line\n   or update umask to be \"0027\" or more
restrictive"
   fi
   if [ -n "$l_output" ]; then
      echo -e "$l_output"
   else
      echo -e " - Configure UMASK in a file in the \"/etc/profile.d/\"
directory ending in \".sh\"\n\n   Example Command (Hash to represent being
run at a root prompt):\n\n# printf '%s\\\n' \"umask 027\" >
/etc/profile.d/50-systemwide_umask.sh\n"
   fi
}
```

Note:

- This method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked
- If the `pam_umask.so` module is going to be used to set `umask`, ensure that it's not being overridden by another setting. Refer to the PAM_UMASK(8) man page for more information

Default Value:

UMASK 022

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Additional Information:

- Other methods of setting a default user umask exist
- If other methods are in use in your environment they should be audited
- The default user umask can be overridden with a user specific umask
- The user creating the directories or files has the discretion of changing the permissions:
    - Using the chmod command
    - Setting a different default umask by adding the umask command into a User Shell Configuration File, (.bashrc), in their home directory
    - Manually changing the umask for the duration of a login session by running the umask command

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1083	TA0007	

5 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. Reference <http://chrony.tuxfamily.org/> manual page for more information on configuring chrony.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

5.1 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

What is covered

This section will cover the minimum best practices for the usage of **either** `rsyslog` **or** `journald`. The recommendations are written such that each is wholly independent of each other and **only one is implemented**.

- If your organization makes use of an enterprise wide logging system completely outside of `rsyslog` or `journald`, then the following recommendations do not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both `rsyslog` and `journald`, take care how the recommendations may or may not apply to you.

What is not covered

- Enterprise logging systems not utilizing `rsyslog` or `journald`. As logging is very situational and dependent on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both `rsyslog` and `journald` supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period of logging on the local system), but the log server is out of scope for these recommendations.

5.1.1 Configure rsyslog

The `rsyslog` software package may be used instead of the default `journald` logging mechanism.

Note: This section only applies if `rsyslog` is the chosen method for client side logging. Do not apply this section if `journald` is used.

5.1.1.1 Ensure rsyslog is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` software is recommended in environments where `journald` does not meet operation requirements.

Rationale:

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit:

Verify `rsyslog` is installed.
Run the following command:

```
# rpm -q rsyslog
```

Verify the output matches:

```
rsyslog-<version>
```

Remediation:

Run the following command to install `rsyslog`:

```
# yum install rsyslog
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1005, T1005.000, T1070, T1070.002	TA0005	

5.1.1.2 Ensure rsyslog service is enabled (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Once the `rsyslog` package is installed, ensure that the service is enabled.

Rationale:

If the `rsyslog` service is not enabled to start on boot, the system will not capture logging events.

Audit:

- IF - rsyslog is being used for logging on the system:
Run the following command to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
```

Verify the output matches:

```
enabled
```

Remediation:

Run the following command to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1211, T1562, T1562.001	TA0005	

5.1.1.3 Ensure journald is configured to send logs to rsyslog (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from `systemd-journald` may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of `systemd-journald` logs, however, use of the `rsyslog` service provides a consistent means of log collection and export.

Rationale:

-IF- `rsyslog` is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

Note: This recommendation only applies if `rsyslog` is the chosen method for client side logging. Do not apply this recommendation if `systemd-journald` is used.

Audit:

-IF- `rsyslog` is the preferred method for capturing logs
Run the following command to verify that logs are forwarded to `rsyslog` by setting `ForwardToSyslog` to `yes` in the systemd-journald configuration:

```
grep -Pi -- '^\h*ForwardToSyslog' /etc/systemd/journald.conf

ForwardToSyslog=yes
```

Run the following command to verify `systemd-journald.service` and `rsyslog.service` are loaded and active:

```
# systemctl list-units --type service | grep -P -- '(journald|rsyslog)'
```

Output should be similar to:

```
rsyslog.service                                    loaded active running
System Logging Service
systemd-journald.service                           loaded active running
Journal Service
```

Remediation:

Create or edit the file `/etc/systemd/journald.conf` and add or edit the following line:

```
ForwardToSyslog=yes
```

Reload the `systemd-journald` service:

```
# systemctl systemctl reload-or-try-restart systemd-journald.service
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, AU-2, AU-4, AU-12, MP-2, SI-5
2. SYSTEMD-JOURNALD.SERVICE(8)
3. JOURNALD.CONF(5)

Additional Information:

As noted in the `systemd-journald` man pages, `systemd-journald` logs may be exported to `rsyslog` either through the process mentioned here, or through a facility like `systemd-journald.service`. There are trade-offs involved in each implementation, where `ForwardToSyslog` will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as `systemd-journald.service`, on the other hand, will record bootup events, but may delay sending the information to `rsyslog`, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006, T1565	TA0040	M1029

5.1.1.4 Ensure rsyslog default file permissions are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Impact:

The systems global `umask` could override, but only making the file permissions stricter, what is configured in RSyslog with the `FileCreateMode` directive. RSyslog also has its own `$umask` directive that can alter the intended file creation mode. In addition, consideration should be given to how `FileCreateMode` is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/rsyslog.conf`, `/etc/rsyslog.d/*conf` files and that `FileCreateMode` is set before any file is created.

Audit:

Run the following command:

```
# grep -Ps '^\h*\$FileCreateMode\h+0[0,2,4,6][0,2,4]0\b' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

Verify the output is includes 0640 or more restrictive:

```
$FileCreateMode 0640
```

Remediation:

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.1.1.5 Ensure logging is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information as expected:

```
# ls -l /var/log/
```

Remediation:

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment.
Note: The below configuration is shown for example purposes only. Due care should be given to how the organization wish to store log data.

```
*.emerg                                 :omusrmsg:*
auth,authpriv.*                         /var/log/secure
mail.*                                  -/var/log/mail
mail.info                               -/var/log/mail.info
mail.warning                            -/var/log/mail.warn
mail.err                                /var/log/mail.err
cron.*                                  /var/log/cron
*.=warning;*.=err                       -/var/log/warn
*.crit                                  /var/log/warn
*.*;mail.none;news.none                 -/var/log/messages
local0,local1.*                         -/var/log/localmessages
local2,local3.*                         -/var/log/localmessages
local4,local5.*                         -/var/log/localmessages
local6,local7.*                         -/var/log/localmessages
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0005	

5.1.1.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

RSyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

Old format

```
# grep "^*.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `@@<FQDN or IP of remote loghost>`, for example

```
*.* @@loghost.example.com
```

New format

```
# grep -E '^\s*([^#]+\s+)?action\(([^#]+\s+)?\btarget=\"?[^#"]+\"?\b'
/etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `target=<FQDN or IP of remote loghost>`, for example:

```
*.* action(type="omfwd" target="loghost.example.com" port="514"
protocol="tcp"
```

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"
           action.resumeRetryCount="100"
           queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the rsyslog.conf(5) man page for more information.

Additional Information:

In addition, see the RSyslog documentation for implementation details of TLS.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.1.7 Ensure rsyslog is not configured to receive logs from a remote client (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

RSyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that the system is not configured to accept incoming logs.
New format

```
# grep -Ps -- '^\h*module\(load="imtcp"\)' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
# grep -Ps -- '^\h*input\(type="imtcp" port="514"\)' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

No output expected.
-**OR**-
Old format

```
# grep -s '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
# grep -s '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

No output expected.

Remediation:

Should there be any active log server configuration found in the auditing section, modify those files and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.
New format

```
module(load="imtcp")
input(type="imtcp" port="514")
```

-**OR**-
Old format

```
$ModLoad imtcp
$InputTCPServerRun
```

Restart the service:

```
# systemctl restart rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1029

5.1.2 Configure journald

Included in the systemd suite is a journaling service called `systemd-journald.service` for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the /dev/log socket
- STDOUT/STDERR of programs via StandardOutput=journal + StandardError=journal in service files (both of which are default settings)
- Kernel log messages via the /dev/kmsg device node
- Audit records via the kernel's audit subsystem
- Structured log messages via journald's native protocol

Any changes made to the `systemd-journald` configuration will require a re-start of `systemd-journald`

5.1.2.1 Ensure journald is configured to send logs to a remote log host

5.1.2.1.1 Ensure systemd-journal-remote is installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

-IF- journald will be used for logging on the system:
Verify `system-journal-gateway` is installed.
Run the following command:

```
# rpm -q system-journal-gateway
```

Verify the output matches:

```
systemd-journal-remote-<version>
```

Remediation:

Run the following command to install `system-journal-gateway`:

```
# yum install system-journal-gateway
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.2.1.2 Ensure systemd-journal-remote is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Verify `systemd-journal-remote` is configured.
Run the following command:

```
# grep -P "^ *URL=|^ *ServerKeyFile=|^ *ServerCertificateFile=|^
*TrustedCertificateFile=" /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server. Example:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Remediation:

Edit the `/etc/systemd/journal-upload.conf` file and ensure the following lines are set per your environment:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.2.1.3 Ensure systemd-journal-remote is enabled (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

Audit:

Verify `systemd-journal-remote` is enabled.
Run the following command:

```
# systemctl is-enabled systemd-journal-upload.service

enabled
```

Remediation:

Run the following command to enable `systemd-journal-remote`:

```
# systemctl --now enable systemd-journal-upload.service
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, CM-7, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.2.1.4 Ensure journald is not configured to receive logs from a remote client (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

NOTE:

- The same package, `systemd-journal-remote`, is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; `systemd-journal-remote.socket` and `systemd-journal-remote.service`.

Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.

Audit:

Run the following command to verify `systemd-journal-remote.socket` is not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket
```

Verify the output matches:

```
masked
```

Remediation:

Run the following command to disable `systemd-journal-remote.socket`:

```
# systemctl --now mask systemd-journal-remote.socket
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.2.2 Ensure journald service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Ensure that the `systemd-journald` service is enabled to allow capturing of logging events.

Rationale:

If the `systemd-journald` service is not enabled to start on boot, the system will not capture logging events.

Audit:

Run the following command to verify `systemd-journald` is enabled:

```
# systemctl is-enabled systemd-journald.service
```

Verify the output matches:

```
static
```

Remediation:

By default the `systemd-journald` service does not have an `[Install]` section and thus cannot be enabled / disabled. It is meant to be referenced as `Requires` or `Wants` by other unit files. As such, if the status of `systemd-journald` is not `static`, investigate why.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0040	M1029

5.1.2.3 Ensure journald is configured to compress large log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Audit:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep ^\s*Compress /etc/systemd/journald.conf
```

Verify the output matches:

```
Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

Restart the service:

```
# systemctl restart systemd-journald.service
```

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters.

It is possible to change the default threshold of 512 bytes per object before compression is used.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1053

5.1.2.4 Ensure journald is configured to write logfiles to persistent disk (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Audit:

Review `/etc/systemd/journald.conf` and verify that logs are persisted to disk:

```
# grep ^\s*Storage /etc/systemd/journald.conf
```

Verify the output matches:

```
Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

Restart the service:

```
# systemctl restart systemd-journald.service
```

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006	TA0005	M1022

5.1.2.5 Ensure journald is not configured to send logs to rsyslog (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from `journald` should be kept in the confines of the service and not forwarded on to other services.

Rationale:

IF journald is the method for capturing logs, all logs of the system should be handled by journald and not forwarded to other logging mechanisms.

Note: This recommendation only applies if journald is the chosen method for client side logging. Do not apply this recommendation if rsyslog is used.

Audit:

IF journald is the method for capturing logs
Review `/etc/systemd/journald.conf` and verify that logs are not forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify that there is no output.

Remediation:

Edit the `/etc/systemd/journald.conf` file and ensure that `ForwardToSyslog=yes` is removed.
Restart the service:

```
# systemctl systemctl reload-or-try-restart systemd-journald.service
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1562, T1562.006, T1565	TA0040	M1029

5.1.2.6 Ensure journald log rotation is configured per site policy (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

Remediation:

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.
The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

Additional Information:

See `man 5 journald.conf` for detailed information regarding the parameters in use.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0040	M1022

5.1.3 Ensure logrotate is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Review `/etc/logrotate.conf` and `/etc/logrotate.d/*` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/*` to ensure logs are rotated according to site policy.

References:

1. NIST SP 800-53 Rev. 5: AU-8

Additional Information:

If no `maxage` setting is set for `logrotate` a situation can occur where `logrotate` is interrupted and fails to delete rotated log files. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such log file is removed but standard rotation settings are not overridden.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002	TA0040	M1022

5.1.4 Ensure all logfiles have appropriate access configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files stored in `/var/log/` contain logged information from many services on the system and potentially from other logged hosts as well.

Rationale:

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

Audit:

Run the following script to verify that files in `/var/log/` have appropriate permissions and ownership:

```
#!/usr/bin/env bash

{
   l_op2="" l_output2=""
   l_uidmin="$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"
   file_test_chk()
   {
      l_op2=""
      if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then
         l_op2="$l_op2\n  - Mode: \"$l_mode\" should be \"$maxperm\" or more
restrictive"
      fi
      if [[ ! "$l_user" =~ $l_auser ]]; then
         l_op2="$l_op2\n  - Owned by: \"$l_user\" and should be owned by
\"${l_auser//|/ or }\""
      fi
      if [[ ! "$l_group" =~ $l_agroup ]]; then
         l_op2="$l_op2\n  - Group owned by: \"$l_group\" and should be group
owned by \"${l_agroup//|/ or }\""
      fi
      [ -n "$l_op2" ] && l_output2="$l_output2\n - File: \"$l_fname\"
is:$l_op2\n"
   }
   unset a_file && a_file=() # clear and initialize array
   # Loop to create array with stat of files that could possibly fail one of
the audits
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_file+=("$(stat -Lc '%n^%#a^%U^%u^%G^%g'
"$l_file")")
   done < <(find -L /var/log -type f \( -perm /0137 -o ! -user root -o ! -
group root \) -print0)
   while IFS="^" read -r l_fname l_mode l_user l_uid l_group l_gid; do
      l_bname="$(basename "$l_fname")"
      case "$l_bname" in
         lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-
* | README)
            perm_mask='0113'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="root"
            l_agroup="(root|utmp)"
            file_test_chk
            ;;
         secure | auth.log | syslog | messages)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="(root|syslog)"
            l_agroup="(root|adm)"
            file_test_chk
            ;;
         SSSD | sssd)
            perm_mask='0117'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="(root|SSSD)"
            l_agroup="(root|SSSD)"
            file_test_chk
            ;;
         gdm | gdm3)
```

```
            perm_mask='0117'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="root"
            l_agroup="(root|gdm|gdm3)"
            file_test_chk
            ;;
         *.journal | *.journal~)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="root"
            l_agroup="(root|systemd-journal)"
            file_test_chk
            ;;
         *)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="(root|syslog)"
            l_agroup="(root|adm)"
            if [ "$l_uid" -lt "$l_uidmin" ] && [ -z "$(awk -v grp="$l_group"
-F: '$1==grp {print $4}' /etc/group)" ]; then
               if [[ ! "$l_user" =~ $l_auser ]]; then
                  l_auser="(root|syslog|$l_user)"
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_tst=""
                  while l_out3="" read -r l_duid; do
                     [ "$l_duid" -ge "$l_uidmin" ] && l_tst=failed
                  done <<< "$(awk -F: '$4=='"$l_gid"' {print $3}'
/etc/passwd)"
                  [ "$l_tst" != "failed" ] && l_agroup="(root|adm|$l_group)"
               fi
            fi
            file_test_chk
            ;;
      esac
   done <<< "$(printf '%s\n' "${a_file[@]}")"
   unset a_file # Clear array
   # If all files passed, then we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Results:\n ** Pass **\n- All files in \"/var/log/\"
have appropriate permissions and ownership\n"
   else
      # print the reason why we are failing
      echo -e "\n- Audit Results:\n ** Fail **\n$l_output2"
   fi
}
```

Remediation:

Run the following script to update permissions and ownership on files in `/var/log`. Although the script is not destructive, ensure that the output is captured in the event that the remediation causes issues.

```
#!/usr/bin/env bash

{
   l_op2="" l_output2=""
   l_uidmin="$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"
   file_test_fix()
   {
      l_op2=""
      l_fuser="root"
      l_fgroup="root"
      if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then
         l_op2="$l_op2\n  - Mode: \"$l_mode\" should be \"$maxperm\" or more restrictive\n   -
Removing excess permissions"
         chmod "$l_rperms" "$l_fname"
      fi
      if [[ ! "$l_user" =~ $l_auser ]]; then
         l_op2="$l_op2\n  - Owned by: \"$l_user\" and should be owned by \"${l_auser//|/ or }\"\n
- Changing ownership to: \"$l_fuser\""
         chown "$l_fuser" "$l_fname"
      fi
      if [[ ! "$l_group" =~ $l_agroup ]]; then
         l_op2="$l_op2\n  - Group owned by: \"$l_group\" and should be group owned by
\"${l_agroup//|/ or }\"\n   - Changing group ownership to: \"$l_fgroup\""
         chgrp "$l_fgroup" "$l_fname"
      fi
      [ -n "$l_op2" ] && l_output2="$l_output2\n - File: \"$l_fname\" is:$l_op2\n"
   }
   unset a_file && a_file=() # clear and initialize array
   # Loop to create array with stat of files that could possibly fail one of the audits
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_file+=("$(stat -Lc '%n^%#a^%U^%u^%G^%g' "$l_file")")
   done < <(find -L /var/log -type f \( -perm /0137 -o ! -user root -o ! -group root \) -print0)
   while IFS="^" read -r l_fname l_mode l_user l_uid l_group l_gid; do
      l_bname="$(basename "$l_fname")"
      case "$l_bname" in
         lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
            perm_mask='0113'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_rperms="ug-x,o-wx"
            l_auser="root"
            l_agroup="(root|utmp)"
            file_test_fix
            ;;
         secure | auth.log | syslog | messages)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_rperms="u-x,g-wx,o-rwx"
            l_auser="(root|syslog)"
            l_agroup="(root|adm)"
            file_test_fix
            ;;
         SSSD | sssd)
            perm_mask='0117'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_rperms="ug-x,o-rwx"
            l_auser="(root|SSSD)"
            l_agroup="(root|SSSD)"
            file_test_fix
            ;;
         gdm | gdm3)
            perm_mask='0117'
            l_rperms="ug-x,o-rwx"
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_auser="root"
            l_agroup="(root|gdm|gdm3)"
            file_test_fix
            ;;
         *.journal | *.journal~)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_rperms="u-x,g-wx,o-rwx"
```

```
            l_auser="root"
            l_agroup="(root|systemd-journal)"
            file_test_fix
            ;;
         *)
            perm_mask='0137'
            maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
            l_rperms="u-x,g-wx,o-rwx"
            l_auser="(root|syslog)"
            l_agroup="(root|adm)"
            if [ "$l_uid" -lt "$l_uidmin" ] && [ -z "$(awk -v grp="$l_group" -F: '$1==grp {print
$4}' /etc/group)" ]; then
               if [[ ! "$l_user" =~ $l_auser ]]; then
                  l_auser="(root|syslog|$l_user)"
               fi
               if [[ ! "$l_group" =~ $l_agroup ]]; then
                  l_tst=""
                  while l_out3="" read -r l_duid; do
                     [ "$l_duid" -ge "$l_uidmin" ] && l_tst=failed
                  done <<< "$(awk -F: '$4=='"$l_gid"' {print $3}' /etc/passwd)"
                  [ "$l_tst" != "failed" ] && l_agroup="(root|adm|$l_group)"
               fi
            fi
            file_test_fix
            ;;
      esac
   done <<< "$(printf '%s\n' "${a_file[@]}")"
   unset a_file # Clear array
   # If all files passed, then we report no changes
   if [ -z "$l_output2" ]; then
      echo -e "- All files in \"/var/log/\" have appropriate permissions and ownership\n  - No
changes required\n"
   else
      # print report of changes
      echo -e "\n$l_output2"
   fi
}
```

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.
If there are services that log to other locations, ensure that those log files have the appropriate access configured.

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	M1028

5.2 Configure System Accounting (auditd)

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log`, which can be configured in `/etc/audit/auditd.conf`.

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules`. These rules have to be merged and loaded before they are active.

Notes:

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used in compliance auditing. The usage of key names is highly recommended as it facilitates organization and searching; as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/`. Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of `50` which is center weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN`. All sample output uses `1000`, but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^\s*UID_MIN/{print $2}' /etc/login.defs`

Normalization

The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values `-1` / `unset` / `4294967295` are equivalent and normalized to `-1`.
- When comparing field types and both sides of the comparison is valid fields types, such as `euid!=uid`, then the auditing system may normalize such that the output is `uid!=euid`.
- Some parts of the rule may be rearranged whilst others are dependent on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F
key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
```

Capacity planning

The recommendations in this section implement auditing policies that not only produce large quantities of logged data, but may also negatively impact system performance. Capacity planning is critical in order not to adversely impact production environments.

- Disk space. If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- Disk IO. It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

5.2.1 Ensure auditing is enabled

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

5.2.1.1 Ensure audit is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`auditd` is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command and verify `audit` and `audit-libs` packages are installed:

```
#  rpm -q audit audit-libs

audit-<version>
audit-libs-<version>
```

Remediation:

Run the following command to install `audit` and `audit-libs`:

```
# yum install audit audit-libs
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-3(1), AU-12, SI-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	M1022

5.2.1.2 Ensure auditing for processes that start prior to auditd is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure `grub2` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd` , so that potential malicious activity cannot go undetected.

Audit:

Note: `/etc/default/grub` should be checked because the `grub2-mkconfig -o` command will overwrite `grub.cfg` with parameters listed in `/etc/default/grub`.
Run the following command to verify that the `audit=1` parameter has been set:

```
# grubby --info=ALL | grep -Po '\baudit=1\b'

audit=1
```

Note: `audit=1` may be returned multiple times
Run the following command to verify that the `audit=1` parameter has been set in `/etc/default/grub`:

```
# grep -Psoi -- '^\h*GRUB_CMDLINE_LINUX=\"([^#\n\r]+\h+)?audit=1\b'
/etc/default/grub
```

Example output:

```
GRUB_CMDLINE_LINUX="quiet audit=1"
```

Note: Other parameters may also be listed

Remediation:

Run the following command to update the `grub2` configuration with `audit=1`:

```
# grubby --update-kernel ALL --args 'audit=1'
```

Edit `/etc/default/grub` and add `audit=1` to the `GRUB_CMDLINE_LINUX=` line between the opening and closing double quotes:
Example:

```
GRUB_CMDLINE_LINUX="quiet audit=1"
```

Note: Other parameters may also be listed

Additional Information:

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

`grubby` is a command line tool used to configure bootloader menu entries across multiple architectures. It is used for updating and displaying information about the configuration files for various architecture specific bootloaders.

It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

The grubby executable has full support for the grub2 bootloader on x86_64 systems using legacy BIOS or modern UEFI firmware and ppc64 and ppc64le hardware using OPAL or SLOF as firmware.

Legacy s390 and the current s390x architectures and their zipl bootloader are fully supported.

Support for yaboot has been deprecated as all ppc architecture hardware since the Power8 uses grub2 or petitboot which both use the grub2 configuration file format.

Legacy bootloaders LILO, SILO, and ELILO are deprecated and no longer receiving active support in favor of previously mentioned bootloaders.

The default bootloader target is primarily determined by the architecture for which grubby has been built. Each architecture has a preferred bootloader, and each bootloader has its own configuration file. If no bootloader is selected on the command line, grubby will use these default settings to search for an existing configuration. If no bootloader configuration file is found, grubby will use the default value for that architecture.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

5.2.1.3 Ensure audit_backlog_limit is sufficient (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `audit_backlog_limit` parameter determines how auditd records can be held in the auditd backlog. The default setting of 64 may be insufficient to store all audit events during boot.

Rationale:

During boot if `audit=1`, then the backlog will hold 64 records. If more than 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected.

Audit:

Note: `/etc/default/grub` should be checked because the `grub2-mkconfig -o` command will overwrite `grub.cfg` with parameters listed in `/etc/default/grub`.
Run the following command and verify the `audit_backlog_limit=` parameter is set to an appropriate size for your organization

```
# grubby --info=ALL | grep -Po "\baudit_backlog_limit=\d+\b"

audit_backlog_limit=<BACKLOG SIZE>
```

Validate that the line(s) returned contain a value for `audit_backlog_limit=` that is sufficient for your organization.
Recommended that this value be `8192` or larger.
Run the following command to verify that the `audit_backlog_limit=<BACKLOG SIZE>` parameter has been set in `/etc/default/grub`:

```
# grep -Psoi --
'^\h*GRUB_CMDLINE_LINUX=\"([^#\n\r]+\h+)?\baudit_backlog_limit=\d+\b'
/etc/default/grub
```

Example output:

```
GRUB_CMDLINE_LINUX="quiet audit_backlog_limit=8192"
```

Note: Other parameters may also be listed

Remediation:

Run the following command to add `audit_backlog_limit=<BACKLOG SIZE>` to GRUB_CMDLINE_LINUX:

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=<BACKLOG SIZE>'
```

Example:

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=8192'
```

Edit `/etc/default/grub` and add `audit_backlog_limit=<BACKLOG SIZE>` to the `GRUB_CMDLINE_LINUX=` line between the opening and closing double quotes:
Example:

```
GRUB_CMDLINE_LINUX="quiet audit_backlog_limit=8192"
```

Note: Other parameters may also be listed

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

Additional Information:

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

`grubby` is a command line tool used to configure bootloader menu entries across multiple architectures. It is used for updating and displaying information about the configuration files for various architecture specific bootloaders.

It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

The grubby executable has full support for the grub2 bootloader on x86_64 systems using legacy BIOS or modern UEFI firmware and ppc64 and ppc64le hardware using OPAL or SLOF as firmware.

Legacy s390 and the current s390x architectures and their zipl bootloader are fully supported.

Support for yaboot has been deprecated as all ppc architecture hardware since the Power8 uses grub2 or petitboot which both use the grub2 configuration file format.

Legacy bootloaders LILO, SILO, and ELILO are deprecated and no longer receiving active support in favor of previously mentioned bootloaders.

The default bootloader target is primarily determined by the architecture for which grubby has been built. Each architecture has a preferred bootloader, and each bootloader has its own configuration file. If no bootloader is selected on the command line, grubby will use these default settings to search for an existing configuration. If no bootloader configuration file is found, grubby will use the default value for that architecture.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

5.2.1.4 Ensure auditd service is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd

enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `auditd`:

```
# systemctl --now enable auditd
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

Additional Information:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

5.2.2 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

5.2.2.1 Ensure audit log storage size is configured (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:

Run the following command and ensure output is in compliance with site policy:

```
# grep -w "^\s*max_log_file\s*=" /etc/audit/auditd.conf

max_log_file = <MB>
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

References:

1. NIST SP 800-53 Rev. 5: AU-8

Additional Information:

The `max_log_file` parameter is measured in megabytes.

Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in `auditd` configurations. Manual audit of custom configurations should be evaluated for effectiveness and completeness.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0040	M1053

5.2.2.2 Ensure audit logs are not automatically deleted (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Audit:

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf

max_log_file_action = keep_logs
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

References:

1. NIST SP 800-53 Rev. 5: AU-8

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.2.3 Ensure system is disabled when audit logs are full (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `auditd` daemon can be configured to halt the system or put the system in single user mode, if no free space is available or an error is detected on the partition that holds the audit log files.

The `disk_full_action` parameter tells the system what action to take when no free space is available on the partition that holds the audit log files. Valid values are `ignore`, `syslog`, `rotate`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon will issue a syslog message but no other action is taken
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- `suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shut down the system

The `disk_error_action` parameter tells the system what action to take when an error is detected on the partition that holds the audit log files. Valid values are `ignore`, `syslog`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon will not take any action
- `syslog`, the audit daemon will issue no more than 5 consecutive warnings to syslog
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script
- `suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shut down the system

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Impact:

-IF-

- The `disk_full_action` parameter is set to `halt` the `auditd` daemon will shutdown the system when the disk partition containing the audit logs becomes full.
- The `disk_full_action` parameter is set to `single` the `auditd` daemon will put the computer system in single user mode when the disk partition containing the audit logs becomes full.

-IF-

- The `disk_error_action` parameter is set to `halt` the `auditd` daemon will shutdown the system when an error is detected on the partition that holds the audit log files.
- The `disk_error_action` parameter is set to `single` the `auditd` daemon will put the computer system in single user mode when an error is detected on the partition that holds the audit log files.
- The `disk_error_action` parameter is set to `syslog` the `auditd` daemon will issue no more than 5 consecutive warnings to syslog when an error is detected on the partition that holds the audit log files.

Audit:

Run the following command and verify the `disk_full_action` is set to either `halt` or `single`:

```
# grep -P -- '^\h*disk_full_action\h*=\h*(halt|single)\b'
/etc/audit/auditd.conf

disk_full_action = <halt|single>
```

Run the following command and verify the `disk_error_action` is set to `syslog`, `single`, or `halt`:

```
# grep -P -- '^\h*disk_error_action\h*=\h*(syslog|single|halt)\b'
/etc/audit/auditd.conf

disk_error_action = <syslog|single|halt>
```

Remediation:

Set one of the following parameters in `/etc/audit/auditd.conf` depending on your local security policies.

```
disk_full_action = <halt|single>
disk_error_action = <syslog|single|halt>
```

Example:

```
disk_full_action = halt
disk_error_action = halt
```

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5
2. AUDITD.CONF(5)
3. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening#configuring-auditd-for-a-secure-environment_auditing-the-system

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.2.4 Ensure system warns when audit logs are low on space (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `auditd` daemon can be configured to halt the system, put the system in single user mode or send a warning message, if the partition that holds the audit log files is low on space.

The `space_left_action` parameter tells the system what action to take when the system has detected that it is starting to get low on disk space. Valid values are `ignore`, `syslog`, `rotate`, `email`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `email`, the audit daemon will send a warning to the email account specified in `action_mail_acct` as well as sending the message to syslog
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- `suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shut down the system

The `admin_space_left_action` parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are `ignore`, `syslog`, `rotate`, `email`, `exec`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `syslog`, the audit daemon will issue a warning to syslog
- `rotate`, the audit daemon will rotate logs, losing the oldest to free up space
- `email`, the audit daemon will send a warning to the email account specified in `action_mail_acct` as well as sending the message to syslog
- `exec`, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- `suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shut down the system

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Impact:

If the `admin_space_left_action` is set to `single` the audit daemon will put the computer system in single user mode.

Audit:

Run the following command and verify the `space_left_action` is set to `email`, `exec`, `single`, or `halt`:

```
grep -P -- '^\h*space_left_action\h*=\h*(email|exec|single|halt)\b'
/etc/audit/auditd.conf
```

Verify the output is `email`, `exec`, `single`, or `halt`
Example output

```
space_left_action = email
```

Run the following command and verify the `admin_space_left_action` is set to `single` **- OR -** `halt`:

```
grep -P -- '^\h*admin_space_left_action\h*=\h*(single|halt)\b'
/etc/audit/auditd.conf
```

Verify the output is `single` or `halt`
Example output:

```
admin_space_left_action = single
```

Note: A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

Remediation:

Set the `space_left_action` parameter in `/etc/audit/auditd.conf` to `email`, `exec`, `single`, or `halt`:
Example:

```
space_left_action = email
```

Set the `admin_space_left_action` parameter in `/etc/audit/auditd.conf` to `single` or `halt`:
Example:

```
admin_space_left_action = single
```

Note: A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5
2. AUDITD.CONF(5)
3. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening#configuring-auditd-for-a-secure-environment_auditing-the-system

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.3 Configure auditd rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the auditctl utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/audit.d/` directory.

5.2.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers`, or files in `/etc/sudoers.d`, will be written to when the file(s) or related attributes have changed. The audit records will be tagged with the identifier "scope".

Rationale:

Changes in the `/etc/sudoers` and `/etc/sudoers.d` files can indicate that an unauthorized change has been made to the scope of system administrator activity.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&/\/etc\/sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&/\/etc\/sudoers/ \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor scope changes for system administrators.
Example:

```
# printf "
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
" >> /etc/audit/rules.d/50-scope.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

5.2.3.2 Ensure actions as another user are always logged (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`sudo` provides users with temporary elevated privileges to perform operations, either as the superuser or another user.

Rationale:

Creating an audit log of users with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo`'s logfile to verify if unauthorized commands have been executed.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&(/ -C *euid!=uid/||/ -C *uid!=euid/) \
&&/ -S *execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&(/ -C *euid!=uid/||/ -C *uid!=euid/) \
&&/ -S *execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F
key=user_emulation
-a always,exit -F arch=b32 -S execve -C uid!=euid -F auid!=-1 -F
key=user_emulation
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor elevated privileges.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
" >> /etc/audit/rules.d/50-user_emulation.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

5.2.3.3 Ensure events that modify the sudo log file are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log` . Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale:

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# {
 SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*logfile=//;s/,? .*//' -e 's/"//g' -e 's|/|\\/|g')
 [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && awk "/^ *-w/ \
 &&/"${SUDO_LOG_FILE_ESCAPED}"/ \
 &&/ +-p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output of matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

Running configuration

Run the following command to check loaded rules:

```
# {
 SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*logfile=//;s/,? .*//' -e 's/"//g' -e 's|/|\\/|g')
 [ -n "${SUDO_LOG_FILE_ESCAPED}" ] && auditctl -l | awk "/^ *-w/ \
 &&/"${SUDO_LOG_FILE_ESCAPED}"/ \
 &&/ +-p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the sudo log file.
Example:

```
# {
SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?
.*//' -e 's/"//g')
[ -n "${SUDO_LOG_FILE}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules || printf "ERROR: Variable
'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	

5.2.3.4 Ensure events that modify date and time information are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the;

- `adjtimex` - tune kernel clock
- `settimeofday` - set time using `timeval` and `timezone` structures
- `stime` - using seconds since 1/1/1970
- `clock_settime` - allows for the setting of several internal clocks and timers

system calls have been executed. Further, ensure to write an audit record to the configured audit log file upon exit, tagging the records with a unique identifier such as "time-change".

Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&/ -S/ \
 &&(/adjtimex/ \
   ||/settimeofday/ \
   ||/clock_settime/ ) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

 awk '/^ *-w/ \
 &&/\/etc\/localtime/ \
 &&/ +-p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify output of matches:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-
change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-
change
-w /etc/localtime -p wa -k time-change
```

Running configuration

Run the following command to check loaded rules:

```
# {
 auditctl -l | awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&/ -S/ \
 &&(/adjtimex/ \
   ||/settimeofday/ \
   ||/clock_settime/ ) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'

 auditctl -l | awk '/^ *-w/ \
 &&/\/etc\/localtime/ \
 &&/ +-p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-w /etc/localtime -p wa -k time-change
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.
In addition, also audit for the `stime` system call rule. For example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k
time-change
```

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify date and time information.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-
change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-
change
-w /etc/localtime -p wa -k time-change
" >> /etc/audit/rules.d/50-time-change.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`. In addition, add `stime` to the system call audit. Example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k
time-change
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.3.5 Ensure events that modify the system's network environment are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record changes to network environment files or system calls. The below parameters monitors the following system calls, and write an audit event on system call exit:

- `sethostname` - set the systems host name
- `setdomainname` - set the systems domain name

The files being monitored are:

- `/etc/issue` and `/etc/issue.net` - messages displayed pre-login
- `/etc/hosts` - file containing host names and associated IP addresses
- `/etc/sysconfig/network` - additional information that is valid to all network interfaces
- `/etc/sysconfig/network-scripts/` - directory containing network interface scripts and configurations files

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domain name of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records should have a relevant tag associated with them.

Audit:

64 Bit systems

On disk configuration

Run the following commands to check the on disk rules:

```
# {
 awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&/ -S/ \
 &&(/sethostname/ \
   ||/setdomainname/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

 awk '/^ *-w/ \
 &&(/\/etc\/issue/ \
   ||/\/etc\/issue.net/ \
   ||/\/etc\/hosts/ \
   ||/\/etc\/sysconfig\/network/) \
 &&/ +p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale
```

Running configuration

Run the following command to check loaded rules:

```
# {
 auditctl -l | awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&/ -S/ \
 &&(/sethostname/ \
   ||/setdomainname/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'

 auditctl -l | awk '/^ *-w/ \
 &&(/\/etc\/issue/ \
   ||/\/etc\/issue.net/ \
   ||/\/etc\/hosts/ \
   ||/\/etc\/sysconfig\/network/) \
 &&/ +-p *wa/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts -p wa -k system-locale
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's network environment.

64 Bit systems

Example:

```
# printf "
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale
" >> /etc/audit/rules.d/50-system_locale.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0003	M1047

5.2.3.6 Ensure use of privileged commands are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor privileged programs, those that have the `setuid` and/or `setgid` bit set on execution, to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Impact:

Both the audit and remediation section of this recommendation will traverse all mounted file systems that is not mounted with either `noexec` or `nosuid` mount options. If there are large file systems without these mount options, **such traversal will be significantly detrimental to the performance of the system.**

Before running either the audit or remediation section, inspect the output of the following command to determine exactly which file systems will be traversed:

```
# findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid"
```

To exclude a particular file system due to adverse performance impacts, update the audit and remediation sections by adding a sufficiently unique string to the `grep` statement. The above command can be used to test the modified exclusions.

Audit:

On disk configuration

Run the following command to check on disk rules:

```
# for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }'
/proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print
$1}'); do
    for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
        grep -qr "${PRIVILEGED}" /etc/audit/rules.d && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in on disk configuration.\n"
    done
done
```

Verify that all output is `OK`.

Running configuration

Run the following command to check loaded rules:

```
# {
   RUNNING=$(auditctl -l)
   [ -n "${RUNNING}" ] && for PARTITION in $(findmnt -n -l -k -it $(awk
'/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv
"noexec|nosuid" | awk '{print $1}'); do
      for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
         printf -- "${RUNNING}" | grep -q "${PRIVILEGED}" && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in running configuration.\n"
      done
   done \
   || printf "ERROR: Variable 'RUNNING' is unset.\n"
}
```

Verify that all output is `OK`.

Special mount points

If there are any special mount points that are not visible by default from `findmnt` as per the above audit, said file systems would have to be manually audited.

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor the use of privileged commands.
Example:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  AUDIT_RULE_FILE="/etc/audit/rules.d/50-privileged.rules"
  NEW_DATA=()
  for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }'
/proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print
$1}'); do
    readarray -t DATA < <(find "${PARTITION}" -xdev -perm /6000 -type f | awk
-v UID_MIN=${UID_MIN} '{print "-a always,exit -F path=" $1 " -F perm=x -F
auid>="UID_MIN" -F auid!=unset -k privileged" }')
      for ENTRY in "${DATA[@]}"; do
        NEW_DATA+=("${ENTRY}")
      done
  done
  readarray &> /dev/null -t OLD_DATA < "${AUDIT_RULE_FILE}"
  COMBINED_DATA=( "${OLD_DATA[@]}" "${NEW_DATA[@]}" )
  printf '%s\n' "${COMBINED_DATA[@]}" | sort -u > "${AUDIT_RULE_FILE}"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Special mount points

If there are any special mount points that are not visible by default from just scanning `/`, change the `PARTITION` variable to the appropriate partition and re-run the remediation.

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0002	M1026

5.2.3.7 Ensure unsuccessful file access attempts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor for unsuccessful attempts to access files. The following parameters are associated with system calls that control files:

- creation - `creat`
- opening - `open` , `openat`
- truncation - `truncate` , `ftruncate`

An audit log record will only be written if all of the following criteria is met for the user when trying to access a file:

- a non-privileged user (auid>=UID_MIN)
- is not a Daemon event (auid=4294967295/unset/-1)
- if the system call returned EACCES (permission denied) or EPERM (some other permanent error associated with the specific system call)

Rationale:

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&(/ -F *exit=-EACCES/||/ -F *exit=-EPERM/) \
 &&/ -S/ \
 &&/creat/ \
 &&/open/ \
 &&/truncate/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-
EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-
EPERM -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-
EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-
EPERM -F auid>=1000 -F auid!=unset -k access
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&(/ -F *exit=-EACCES/||/ -F *exit=-EPERM/) \
 &&/ -S/ \
 &&/creat/ \
 &&/open/ \
 &&/truncate/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-
EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit=-
EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor unsuccessful file access attempts.

64 Bit systems

Example:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-
EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-
EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-
EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-
EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
" >> /etc/audit/rules.d/50-access.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0007	

5.2.3.8 Ensure events that modify user/group information are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record events affecting the modification of user or group information, including that of passwords and old passwords if in use.

- `/etc/group` - system groups
- `/etc/passwd` - system users
- `/etc/gshadow` - encrypted password for each group
- `/etc/shadow` - system user passwords
- `/etc/security/opasswd` - storage of old passwords if the relevant PAM module is in use

The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/etc\/group/ \
  ||/\/etc\/passwd/ \
  ||/\/etc\/gshadow/ \
  ||/\/etc\/shadow/ \
  ||/\/etc\/security\/opasswd/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/etc\/group/ \
  ||/\/etc\/passwd/ \
  ||/\/etc\/gshadow/ \
  ||/\/etc\/shadow/ \
  ||/\/etc\/security\/opasswd/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify user/group information.
Example:

```
# printf "
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
" >> /etc/audit/rules.d/50-identity.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

5.2.3.9 Ensure discretionary access control permission modification events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The following commands and system calls effect the permissions, ownership and various attributes of files.

- `chmod`
- `fchmod`
- `fchmodat`
- `chown`
- `fchown`
- `fchownat`
- `lchown`
- `setxattr`
- `lsetxattr`
- `fsetxattr`
- `removexattr`
- `lremovexattr`
- `fremovexattr`

In all cases, an audit record will only be written for non-system user ids and will ignore Daemon events. All audit records will be tagged with the identifier "perm_mod."

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

Note: Output showing all audited syscalls, e.g. (-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod) is also acceptable. These have been separated by function on the displayed output for clarity.

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -S/ \
 &&/ -F *auid>=${UID_MIN}/ \
 &&(/chmod/||/fchmod/||/fchmodat/ \
   ||/chown/||/fchown/||/fchownat/||/lchown/ \
   ||/setxattr/||/lsetxattr/||/fsetxattr/ \
   ||/removexattr/||/lremovexattr/||/fremovexattr/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -S/ \
 &&/ -F *auid>=${UID_MIN}/ \
 &&(/chmod/||/fchmod/||/fchmodat/ \
   ||/chown/||/fchown/||/fchownat/||/lchown/ \
   ||/setxattr/||/lsetxattr/||/fsetxattr/ \
   ||/removexattr/||/lremovexattr/||/fremovexattr/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor discretionary access control permission modification events.

64 Bit systems

Example:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
" >> /etc/audit/rules.d/50-perm_mod.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.10 Ensure successful file system mounts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user

Rationale:

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -S/ \
 &&/mount/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -S/ \
 &&/mount/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful file system mounts.

64 Bit systems

Example:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
" >> /etc/audit/rules.d/50-mounts.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

References:

1. NIST SP 800-53 Rev. 5: CM-6

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0010	M1034

5.2.3.11 Ensure session initiation information is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor session initiation events. The parameters in this section track changes to the files associated with session events.

- `/var/run/utmp` - tracks all currently logged in users.
- `/var/log/wtmp` - file tracks logins, logouts, shutdown, and reboot events.
- `/var/log/btmp` - keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`.

All audit records will be tagged with the identifier "session."

Rationale:

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
  ||/\/var\/log\/wtmp/ \
  ||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
  ||/\/var\/log\/wtmp/ \
  ||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor session initiation information.
Example:

```
# printf "
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
" >> /etc/audit/rules.d/50-session.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0001	

5.2.3.12 Ensure login and logout events are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- `/var/log/lastlog` - maintain records of the last time a user successfully logged in.
- `/var/run/faillock` - directory maintains records of login failures via the `pam_faillock` module.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/log\/lastlog/ \
  ||/\/var\/run\/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/log\/lastlog/ \
  ||/\/var\/run\/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor login and logout events.
Example:

```
# printf "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" >> /etc/audit/rules.d/50-login.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.9 Log and Alert on Unsuccessful Administrative Account Login Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0001	

5.2.3.13 Ensure file deletion events by users are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for:

- `unlink` - remove a file
- `unlinkat` - remove a file attribute
- `rename` - rename a file
- `renameat` rename a file attribute system calls and tags them with the identifier "delete".

Rationale:

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -S/ \
 &&(/unlink/||/rename/||/unlinkat/||/renameat/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -S/ \
 &&(/unlink/||/rename/||/unlinkat/||/renameat/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor file deletion events by users.

64 Bit systems

Example:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
" >> /etc/audit/rules.d/50-delete.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	

5.2.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor SELinux, an implementation of mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the `/etc/selinux/` and `/usr/share/selinux/` directories.

Note: If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.

Rationale:

Changes to files in the `/etc/selinux/` and `/usr/share/selinux/` directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit:

On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/etc\/selinux/ \
  ||/\/usr\/share\/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/etc\/selinux/ \
  ||/\/usr\/share\/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's Mandatory Access Controls.
Example:

```
# printf "
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
" >> /etc/audit/rules.d/50-MAC-policy.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `chcon` command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

64 Bit systems

On disk configuration

Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/chcon/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/chcon/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chcon` command.

64 Bit systems

Example:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `setfacl` command

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

64 Bit systems

On disk configuration
Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/setfacl/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/setfacl/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `setfacl` command.

64 Bit systems

Example:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `chacl` command

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

64 Bit systems

On disk configuration
Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/chacl/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/chacl/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chacl` command.

64 Bit systems

Example:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The operating system must generate audit records for successful/unsuccessful uses of the `usermod` command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

64 Bit systems

On disk configuration
Run the following command to check the on disk rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/sbin\/usermod/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k usermod
```

Running configuration

Run the following command to check loaded rules:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/sbin\/usermod/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=usermod
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `usermod` command.

64 Bit systems

Example:

```
# {
 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k usermod
" >> /etc/audit/rules.d/50-usermod.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0005	M1022

5.2.3.19 Ensure kernel module loading unloading and modification is collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor the loading and unloading of kernel modules. All the loading / listing / dependency checking of modules is done by `kmod` via symbolic links.

The following system calls control loading and unloading of modules:

- `init_module` - load a module
- `finit_module` - load a module (used when the overhead of using cryptographically signed modules to determine the authenticity of a module can be avoided)
- `delete_module` - delete a module
- `create_module` - create a loadable module entry
- `query_module` - query the kernel for various bits pertaining to modules

Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of `modules`.

Rationale:

Monitoring the use of all the various ways to manipulate kernel modules could provide system administrators with evidence that an unauthorized change was made to a kernel module, possibly compromising the security of the system.

Audit:

64 Bit systems

On disk configuration

Run the following commands to check the on disk rules:

```
# {
awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
 &&/ -S/ \
 &&(/init_module/ \
   ||/finit_module/ \
   ||/delete_module/ \
   ||/create_module/ \
   ||/query_module/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/kmod/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" /etc/audit/rules.d/*.rules \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=1000 -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k kernel_modules
```

Running configuration

Run the following command to check loaded rules:

```
# {
 auditctl -l | awk '/^ *-a *always,exit/ \
 &&/ -F *arch=b(32|64)/ \
 &&(/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
 &&/ -S/ \
 &&(/init_module/ \
   ||/finit_module/ \
   ||/delete_module/ \
   ||/create_module/ \
   ||/query_module/) \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'

 UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
 [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
 &&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
 &&/ -F *auid>=${UID_MIN}/ \
 &&/ -F *perm=x/ \
 &&/ -F *path=\/usr\/bin\/kmod/ \
 &&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)" \
 || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S
create_module,init_module,delete_module,query_module,finit_module -F
auid>=1000 -F auid!=-1 -F key=kernel_modules
-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=kernel_modules
```

Symlink audit

Audit if the symlinks that `kmod` accepts is indeed pointing at it:

```
# S_LINKS=$(ls -l /usr/sbin/lsmod /usr/sbin/rmmod /usr/sbin/insmod
/usr/sbin/modinfo /usr/sbin/modprobe /usr/sbin/depmod | grep -v " ->
../bin/kmod" || true) \
&& if [[ "${S_LINKS}" != "" ]]; then printf "Issue with symlinks:
${S_LINKS}\n"; else printf "OK\n"; fi
```

Verify the output states `OK`. If there is a symlink pointing to a different location it should be investigated.

Remediation:

Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor kernel module modification.

64 Bit systems

Example:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=${UID_MIN} -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k kernel_modules
" >> /etc/audit/rules.d/50-kernel_modules.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.006	TA0004	M1047

5.2.3.20 Ensure the audit configuration is immutable (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Set system audit so that audit rules cannot be modified with `auditctl` . Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

Note: This setting will require the system to be rebooted to update the active `auditd` configuration settings.

Rationale:

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Audit:

Run the following command and verify output matches:

```
# grep -Ph -- '^\h*-e\h+2\b' /etc/audit/rules.d/*.rules | tail -1

-e 2
```

Remediation:

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the line `-e 2` at the end of the file:
Example:

```
# printf '%s\n' "-e 2" > /etc/audit/rules.d/99-finalize.rules
```

Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

References:

1. NIST SP 800-53 Rev. 5: AC-3, AU-3, AU-3(1), MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562, T1562.001	TA0005	

5.2.3.21 Ensure the running and on disk configuration is the same (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Audit system have both on disk and running configuration. It is possible for these configuration settings to differ.

Note: Due to the limitations of `augenrules` and `auditctl`, it is not absolutely guaranteed that loading the rule sets via `augenrules --load` will result in all rules being loaded or even that the user will be informed if there was a problem loading the rules.

Rationale:

Configuration differences between what is currently running and what is on disk could cause unexpected problems or may give a false impression of compliance requirements.

Audit:

Merged rule sets

Ensure that all rules in `/etc/audit/rules.d` have been merged into `/etc/audit/audit.rules`:

```
# augenrules --check

/usr/sbin/augenrules: No change
```

Should there be any drift, run `augenrules --load` to merge and load all rules.

Remediation:

If the rules are not aligned across all three () areas, run the following command to merge and load all rules:

```
# augenrules --load
```

Check if reboot is required.

```
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then echo "Reboot required
to load rules"; fi
```

Additional Information:

Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.2.4 Configure auditd file access

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

5.2.4.1 Ensure the audit log directory is 0750 or more restrictive (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The audit log directory contains audit log files.

Rationale:

Audit information includes all information including: audit records, audit settings and audit reports. This information is needed to successfully audit system activity. This information must be protected from unauthorized modification or deletion. If this information were to be compromised, forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

Audit:

Run the following command to verify that the audit log directory has a mode of 0750 or less permissive:

```
# stat -Lc "%n %a" "$(dirname $( awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}'
/etc/audit/auditd.conf))" | grep -Pv -- '^\h*\H+\h+([0,5,7][0,5]0)'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log directory to have a mode of "0750" or less permissive:

```
# chmod g-w,o-rwx "$(dirname $( awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}'
/etc/audit/auditd.conf))"
```

Default Value:

750

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.2 Ensure audit log files are mode 0640 or less permissive (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify audit log files have mode `0640` or less permissive:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "="
'/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f \( ! -
perm 600 -a ! -perm 0400 -a ! -perm 0200 -a ! -perm 0000 -a ! -perm 0640 -a !
-perm 0440 -a ! -perm 0040 \) -exec stat -Lc "%n %#a" {} +
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode than `0640` from audit log files:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "="
'/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f \( ! -
perm 600 -a ! -perm 0400 -a ! -perm 0200 -a ! -perm 0000 -a ! -perm 0640 -a !
-perm 0440 -a ! -perm 0040 \) -exec chmod u-x,g-wx,o-rwx {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.3 Ensure only authorized users own audit log files (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify audit log files are owned by the `root` user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "="
'/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f ! -user
root -exec stat -Lc "%n %U" {} +
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by the `root` user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F "="
'/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f ! -user
root -exec chown root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.4 Ensure only authorized groups are assigned ownership of audit log files (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit log files contain information about the system and system activity.

Rationale:

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

Audit:

Run the following command to verify `log_group` parameter is set to either `adm` or `root` in `/etc/audit/auditd.conf`:

```
# grep -Piw -- '^\h*log_group\h*=\h*(adm|root)\b' /etc/audit/auditd.conf
```

Verify the output is:

```
log_group = adm
-OR-
log_group = root
```

Using the path of the directory containing the audit logs, determine if the audit log files are owned by the "root" or "adm" group by using the following command:

```
# stat -c "%n %G" "$(dirname $(awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}'
/etc/audit/auditd.conf | xargs))"/* | grep -Pv '^\h*\H+\h+(adm|root)\b'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by `root` group:

```
# find $(dirname $(awk -F"=" '/^\s*log_file\s*=\s*/ {print $2}'
/etc/audit/auditd.conf | xargs)) -type f \( ! -group adm -a ! -group root \)
-exec chgrp root {} +
```

Run the following command to configure the audit log files to be owned by the `root` group:

```
# chgrp root /var/log/audit/
```

Run the following command to set the `log_group` parameter in the audit configuration file to `log_group = root`:

```
# sed -ri 's/^\s*#?\s*log_group\s*=\s*\S+(\s*#.*)?.*$/log_group = root\1/'
/etc/audit/auditd.conf
```

Run the following command to restart the audit daemon to reload the configuration file:

```
# systemctl restart auditd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.5 Ensure audit configuration files are 640 or more restrictive (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) -exec stat
-Lc "%n %a" {} + | grep -Pv -- '^\h*\H+\h*([0,2,4,6][0,4]0)\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) -exec
chmod u-x,g-wx,o-rwx {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.6 Ensure audit configuration files are owned by root (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user
root
```

Nothing should be returned

Remediation:

Run the following command to change ownership to `root` user:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user
root -exec chown root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.7 Ensure audit configuration files belong to group root (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit configuration files control auditd and what events are audited.

Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -group
root
```

Nothing should be returned

Remediation:

Run the following command to change group to `root`:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -group
root -exec chgrp root {} +
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.8 Ensure audit tools are 755 or more restrictive (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode `755` or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %a" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules | grep -Pv -- '^\h*\H+\h+([0-
7][0,1,4,5][0,1,4,5])\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.9 Ensure audit tools are owned by root (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode `755` or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules | grep -Pv -- '^\h*\H+\h+root\h*$'
```

Nothing should be returned

Remediation:

Run the following command to change the owner of the audit tools to the `root` user:

```
# chown root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.10 Ensure audit tools belong to group root (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

Audit:

Run the following command to verify the audit tools have mode `755` or more restrictive, are owned by the root user and group root:

```
# stat -c "%n %a %U %G" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/augenrules | grep -Pv -- '^\h*\H+\h+([0-
7][0,1,4,5][0,1,4,5])\h+root\h+root\h*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

Run the following command to change owner and group of the audit tools to `root` user and group:

```
# chown root:root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1070, T1070.002, T1083, T1083.000	TA0007	

5.3 Configure Integrity Checking

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

5.3.1 Ensure AIDE is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Advanced Intrusion Detection Environment (AIDE) is a intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories.

`aide` takes a snapshot of files and directories including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

Rationale:

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Audit:

Run the following command and verify `aide` is installed:

```
# rpm -q aide

aide-<version>
```

Remediation:

Run the following command to install `aide`:

```
# yum install aide
```

Configure `aide` as appropriate for your environment. Consult the `aide` documentation for options.
Initialize `aide`:
Run the following commands:

```
# aide --init
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

References:

1. AIDE stable manual: http://aide.sourceforge.net/stable/manual.html
2. NIST SP 800-53 Rev. 5: AU-2

Additional Information:

The prelinking feature can interfere with `aide` because it alters binaries to speed up their start up times. Run `prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from `aide`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1565, T1565.001	TA0001	M1022

5.3.2 Ensure filesystem integrity is regularly checked (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Audit:

Run the following commands to verify a cron job scheduled to run the aide check.

```
# grep -Ers '^([^#]+\s+)?(\/usr\/s?bin\/|^\s*)aide(\.wrapper)?\s(--?\S+\s)*(--(check|update)|\$AIDEARGS)\b' /etc/cron.* /etc/crontab /var/spool/cron/
```

Ensure a cron job in compliance with site policy is returned.
- OR -
Run the following commands to verify that `aidecheck.service` and `aidecheck.timer` are enabled and `aidcheck.timer` is running

```
# systemctl is-enabled aidecheck.service

# systemctl is-enabled aidecheck.timer
# systemctl status aidecheck.timer
```

Remediation:

- IF - `cron` will be used to schedule and run aide check
Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/sbin/aide --check
```

- OR -
- IF - `aidecheck.service` and `aidecheck.timer` will be used to schedule and run aide check:
Create or edit the file `/etc/systemd/system/aidecheck.service` and add the following lines:

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/sbin/aide --check

[Install]
WantedBy=multi-user.target
```

Create or edit the file `/etc/systemd/system/aidecheck.timer` and add the following lines:

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*
# chmod 0644 /etc/systemd/system/aidecheck.*

# systemctl daemon-reload

# systemctl enable aidecheck.service
# systemctl --now enable aidecheck.timer
```

References:

1. https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service
2. https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer
3. NIST SP 800-53 Rev. 5: AU-2

Additional Information:

The checking in this recommendation occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1036, T1036.005	TA0040	M1022

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Ensure permissions on /etc/passwd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/passwd` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/passwd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd`:

```
# chmod u-x,go-wx /etc/passwd
# chown root:root /etc/passwd
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.2 Ensure permissions on /etc/passwd- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd-` file contains backup user account information.

Rationale:

It is critical to ensure that the `/etc/passwd-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/passwd-` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/passwd-

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd-`:

```
# chmod u-x,go-wx /etc/passwd-
# chown root:root /etc/passwd-
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: { 0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.3 Ensure permissions on /etc/group are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to verify `/etc/group` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group`:

```
# chmod u-x,go-wx /etc/group
# chown root:root /etc/group
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.4 Ensure permissions on /etc/group- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

Rationale:

It is critical to ensure that the `/etc/group-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/group-` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/group-

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group-`:

```
# chmod u-x,go-wx /etc/group-
# chown root:root /etc/group-
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.5 Ensure permissions on /etc/shadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:

Run the following command to verify `/etc/shadow` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/shadow

Access: (0/----------)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/shadow`:

```
# chown root:root /etc/shadow
# chmod 0000 /etc/shadow
```

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/shadow-` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/shadow-

Access: (0/----------)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/shadow-`:

```
# chown root:root /etc/shadow-
# chmod 0000 /etc/shadow-
```

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.7 Ensure permissions on /etc/gshadow are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

Audit:

Run the following command to verify `/etc/gshadow` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/gshadow

Access: (0/----------)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/gshadow`:

```
# chown root:root /etc/gshadow
# chmod 0000 /etc/gshadow
```

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.8 Ensure permissions on /etc/gshadow- are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/gshadow-` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/gshadow-

Access: (0/----------)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/gshadow-`:

```
# chown root:root /etc/gshadow-
# chmod 0000 /etc/gshadow-
```

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.9 Ensure permissions on /etc/shells are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`/etc/shells` is a text file which contains the full pathnames of valid login shells. This file is consulted by `chsh` and available to be queried by other programs.

Rationale:

It is critical to ensure that the `/etc/shells` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/shells` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/shells

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/shells`:

```
# chmod u-x,go-wx /etc/shells
# chown root:root /etc/shells
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.10 Ensure permissions on /etc/security/opasswd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`/etc/security/opasswd` and it's backup `/etc/security/opasswd.old` hold user's previous passwords if `pam_unix` or `pam_pwhistory` is in use on the system

Rationale:

It is critical to ensure that `/etc/security/opasswd` is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following commands to verify `/etc/security/opasswd` and `/etc/security/opasswd.old` are mode 600 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root` if they exist:

```
#  [ -e "/etc/security/opasswd" ] && stat -Lc '%n Access: (%#a/%A)  Uid: (
%u/ %U) Gid: ( %g/ %G)' /etc/security/opasswd

/etc/security/opasswd Access: (0600/-rw-------)  Uid: ( 0/ root) Gid: ( 0/
root)
 -OR-
Nothing is returned
#  [ -e "/etc/security/opasswd.old" ] && stat -Lc '%n Access: (%#a/%A)  Uid:
( %u/ %U) Gid: ( %g/ %G)' /etc/security/opasswd.old

/etc/security/opasswd.old Access: (0600/-rw-------)  Uid: ( 0/ root) Gid: (
0/ root)
 -OR-
Nothing is returned
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/security/opasswd` and `/etc/security/opasswd.old` is they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd
# [ -e "/etc/security/opasswd" ] && chown root:root /etc/security/opasswd
# [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx
/etc/security/opasswd.old
# [ -e "/etc/security/opasswd.old" ] && chown root:root
/etc/security/opasswd.old
```

Default Value:

/etc/security/opasswd Access: (0600/-rw-------) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008, T1222, T1222.002	TA0005	M1022

6.1.11 Ensure world writable files and directories are secured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

World writable files are the least secure. Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. See the `chmod(2)` man page for more information.

Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

This feature prevents the ability to delete or rename files in world writable directories (such as `/tmp`) that are owned by another user.

Audit:

Run the following script to verify:

- No world writable files exist
- No world writable directories without the sticky bit exist

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   l_smask='01000'
   a_path=(); a_arr=(); a_file=(); a_dir=() # Initialize arrays
   a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a ! -path
"*/kubelet/pods/*" -a ! -path "/sys/kernel/security/apparmor/*" -a ! -path "/snap/*" -a ! -path
"/sys/fs/cgroup/memory/*" -a ! -path "/sys/fs/selinux/*")
   while read -r l_bfs; do
      a_path+=( -a ! -path ""$l_bfs"/*")
   done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/ {print $2}')
   # Populate array with files that will possibly fail one of the audits
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%#a' "$l_file")")
   done < <(find / \( "${a_path[@]}" \) \( -type f -o -type d \) -perm -0002 -print0 2>/dev/null)
   while IFS="^" read -r l_fname l_mode; do # Test files in the array
      [ -f "$l_fname" ] && a_file+=("$l_fname") # Add WR files
      if [ -d "$l_fname" ]; then # Add directories w/o sticky bit
         [ ! $(( $l_mode & $l_smask )) -gt 0 ] && a_dir+=("$l_fname")
      fi
   done < <(printf '%s\n' "${a_arr[@]}")
   if ! (( ${#a_file[@]} > 0 )); then
      l_output="$l_output\n  - No world writable files exist on the local filesystem."
   else
      l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_file[@]}")\" World writable files
on the system.\n   - The following is a list of World writable files:\n$(printf '%s\n'
"${a_file[@]}")\n   - end of list\n"
   fi
   if ! (( ${#a_dir[@]} > 0 )); then
      l_output="$l_output\n  - Sticky bit is set on world writable directories on the local
filesystem."
   else
      l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_dir[@]}")\" World writable
directories without the sticky bit on the system.\n   - The following is a list of World writable
directories without the sticky bit:\n$(printf '%s\n' "${a_dir[@]}")\n   - end of list\n"
   fi
   unset a_path; unset a_arr; unset a_file; unset a_dir # Remove arrays
   # If l_output2 is empty, we pass
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured * :\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit failure * :\n$l_output2"
      [ -n "$l_output" ] && echo -e "- * Correctly configured * :\n$l_output\n"
   fi
}
```

Note: On systems with a large number of files and/or directories, this audit may be a long running process

Remediation:

- World Writable Files:
  - It is recommended that write access is removed from `other` with the command (`chmod o-w <filename>`), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.
- World Writable Directories:
  - Set the sticky bit on all world writable directories with the command (`chmod a+t <directory_name>`)

Run the following script to:

- Remove other write permission from any world writable files
- Add the sticky bit to all world writable directories

```
#!/usr/bin/env bash

{
   l_smask='01000'
   a_path=(); a_arr=() # Initialize array
   a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a ! -path
"*/kubelet/pods/*" -a ! -path "/sys/kernel/security/apparmor/*" -a ! -path "/snap/*" -a ! -path
"/sys/fs/cgroup/memory/*" -a ! -path "/sys/fs/selinux/*")
   while read -r l_bfs; do
      a_path+=( -a ! -path ""$l_bfs"/*")
   done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/ {print $2}')
   # Populate array with files
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%#a' "$l_file")")
   done < <(find / \( "${a_path[@]}" \) \( -type f -o -type d \) -perm -0002 -print0 2>/dev/null)
   while IFS="^" read -r l_fname l_mode; do # Test files in the array
      if [ -f "$l_fname" ]; then # Remove excess permissions from WW files
         echo -e " - File: \"$l_fname\" is mode: \"$l_mode\"\n  - removing write permission on
\"$l_fname\" from \"other\""
         chmod o-w "$l_fname"
      fi
      if [ -d "$l_fname" ]; then
         if [ ! $(( $l_mode & $l_smask )) -gt 0 ]; then # Add sticky bit
            echo -e " - Directory: \"$l_fname\" is mode: \"$l_mode\" and doesn't have the sticky
bit set\n  - Adding the sticky bit"
            chmod a+t "$l_fname"
         fi
      fi
   done < <(printf '%s\n' "${a_arr[@]}")
   unset a_path; unset a_arr # Remove array
}
```

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002, T1548	TA0004, TA0005	M1022, M1028

6.1.12 Ensure no unowned or ungrouped files or directories exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

Rationale:

A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

Audit:

Run the following script to verify no unowned or ungrouped files or directories exist:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_path=(); a_arr=(); a_nouser=(); a_nogroup=() # Initialize arrays
   a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"*/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"/sys/fs/cgroup/memory/*")
   while read -r l_bfs; do
      a_path+=( -a ! -path ""$l_bfs"/*")
   done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^\s*(nfs|proc|smb)/
{print $2}')
   while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%U^%G' "$l_file")") && echo
"Adding: $l_file"
   done < <(find / \( "${a_path[@]}" \) \( -type f -o -type d \) \( -nouser -
o -nogroup \) -print0 2> /dev/null)
   while IFS="^" read -r l_fname l_user l_group; do # Test files in the array
      [ "$l_user" = "UNKNOWN" ] && a_nouser+=("$l_fname")
      [ "$l_group" = "UNKNOWN" ] && a_nogroup+=("$l_fname")
   done <<< "$(printf '%s\n' "${a_arr[@]}")"
   if ! (( ${#a_nouser[@]} > 0 )); then
      l_output="$l_output\n  - No unowned files or directories exist on the
local filesystem."
   else
      l_output2="$l_output2\n  - There are \"$(printf '%s'
"${#a_nouser[@]}")\" unowned files or directories on the system.\n   - The
following is a list of unowned files and/or directories:\n$(printf '%s\n'
"${a_nouser[@]}")\n   - end of list"
   fi
   if ! (( ${#a_nogroup[@]} > 0 )); then
      l_output="$l_output\n  - No ungrouped files or directories exist on the
local filesystem."
   else
      l_output2="$l_output2\n  - There are \"$(printf '%s'
"${#a_nogroup[@]}")\" ungrouped files or directories on the system.\n   - The
following is a list of ungrouped files and/or directories:\n$(printf '%s\n'
"${a_nogroup[@]}")\n   - end of list"
   fi
   unset a_path; unset a_arr ; unset a_nouser; unset a_nogroup # Remove
arrays
   if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
      echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2"
      [ -n "$l_output" ] && echo -e "\n- * Correctly configured *
:\n$l_output\n"
   fi
}
```

Note: On systems with a large number of files and/or directories, this audit may be a long running process

Remediation:

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0007	M1022

6.1.13 Ensure SUID and SGID files are reviewed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID and SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different checksum than what from the package. This is an indication that the binary may have been replaced.

Audit:

Run the following script to generate a list of SUID and SGID files:

```
#!/usr/bin/env bash

{
   l_output="" l_output2=""
   a_arr=(); a_suid=(); a_sgid=() # initialize arrays
   # Populate array with files that will possibly fail one of the audits
   while read -r l_mpname; do
      while IFS= read -r -d $'\0' l_file; do
         [ -e "$l_file" ] && a_arr+=("$(stat -Lc '%n^%#a' "$l_file")")
      done < <(find "$l_mpname" -xdev -not -path "/run/user/*"  -type f \( -
perm -2000 -o -perm -4000 \) -print0)
   done <<< "$(findmnt -Derno target)"
   # Test files in the array
   while IFS="^" read -r l_fname l_mode; do
      if [ -f "$l_fname" ]; then
         l_suid_mask="04000"; l_sgid_mask="02000"
         [ $(( $l_mode & $l_suid_mask )) -gt 0 ] && a_suid+=("$l_fname")
         [ $(( $l_mode & $l_sgid_mask )) -gt 0 ] && a_sgid+=("$l_fname")
      fi
   done <<< "$(printf '%s\n' "${a_arr[@]}")"
   if ! (( ${#a_suid[@]} > 0 )); then
      l_output="$l_output\n - There are no SUID files exist on the system"
   else
      l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_suid[@]}")\"
SUID executable files:\n$(printf '%s\n' "${a_suid[@]}")\n - end of list -\n"
   fi
   if ! (( ${#a_sgid[@]} > 0 )); then
      l_output="$l_output\n - There are no SGID files exist on the system"
   else
      l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_sgid[@]}")\"
SGID executable files:\n$(printf '%s\n' "${a_sgid[@]}")\n - end of list -\n"
   fi
   [ -n "$l_output2" ] && l_output2="$l_output2\n- Review the preceding
list(s) of SUID and/or SGID files to\n- ensure that no rogue programs have
been introduced onto the system.\n"
   unset a_arr; unset a_suid; unset a_sgid # Remove arrays
   # If l_output2 is empty, Nothing to report
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n$l_output\n"
   else
      echo -e "\n- Audit Result:\n$l_output2\n"
      [ -n "$l_output" ] && echo -e "$l_output\n"
   fi
}
```

Note: on systems with a large number of files, this may be a long running process

Remediation:

Ensure that no rogue SUID or SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5, AC-3, MP-2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.001	TA0004	M1028

6.1.14 Audit system file permissions (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `RPM Package Manager` has a number of useful options. One of these, the `-V` for RPM option, can be used to verify that system packages are correctly installed. The `-V` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

```
Code   Meaning
S      File size differs.
M      File mode differs (includes permissions and file type).
5      digest (formerly MD5 sum) differs.
D      Device file major/minor number mismatch.
L      readLink(2) path mismatch.
U      User ownership differs.
G      Group ownership differs.
T      The file time (mtime) differs.
P      Capabilities differ.
```

The `rpm -qf` command can be used to determine which package a particular file belongs to. For example, the following commands determines which package the `/bin/bash` file belongs to:

```
# rpm -qf /bin/bash
bash-4.4.19-2.fc28.x86_64
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V bash-4.4.19-2.fc28.x86_64
.M.......    /bin/bash
# rpm --verify bash
??5?????? c /etc/bash.bashrc
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`
.M...... c /etc/passwd
S.5....T c /etc/printcap
```

The `rpm -qi` command can be used to display package information, including name, version, and description. Following example displays information for `bash` package:

```
# rpm -qi bash
Name        : bash
Version     : 4.4.19
Release     : 2.fc28
Architecture: x86_64
Install Date: Tue 15 Aug 2023 10:27:28 AM EDT
Group       : Unspecified
Size        : 6910653
License     : GPLv3+
Signature   : RSA/SHA256, Thu 15 Mar 2018 10:10:10 AM EDT, Key ID
e08e7e629db62fb1
Source RPM  : bash-4.4.19-2.fc28.src.rpm
Build Date  : Thu 15 Mar 2018 10:01:10 AM EDT
Build Host  : buildhw-07.phx2.fedoraproject.org
Relocations : (not relocatable)
Packager    : Fedora Project
Vendor      : Fedora Project
URL         : https://www.gnu.org/software/bash
Bug URL     : https://bugz.fedoraproject.org/bash
Summary     : The GNU Bourne Again shell
Description :
The GNU Bourne Again shell (Bash) is a shell or command language
interpreter that is compatible with the Bourne shell (sh). Bash
incorporates useful features from the Korn shell (ksh) and the C shell
(csh). Most sh scripts can be run by bash without modification.
```

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Audit:

Run the following command to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto --noconfig --noghost >
<filename>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

References:

1. https://docs.fedoraproject.org/en-US/quick-docs/package-management/
2. RPM(8)
3. NIST SP 800-53 Rev. 5: AC-3, CM-1, CM-2, CM-6, CM-7, IA-5, MP-2

Additional Information:

Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.

Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file's permissions even if the new state is more secure than the default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222	TA0005	M1022

6.2 Local User and Group Settings

This section provides guidance on securing aspects of the local users and groups.

Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment, similar checks should be performed against domain users and groups.

6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Local accounts can use shadowed passwords. With shadowed passwords, the passwords are saved in shadow password file, `/etc/shadow`, encrypted by a salted one-way hash. Accounts with a shadowed password have an `x` in the second field in `/etc/passwd`.

Rationale:

The `/etc/passwd` file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the `/etc/passwd` file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the `/etc/passwd` file. This can be mitigated by using shadowed passwords, thus moving the passwords in the `/etc/passwd` file to `/etc/shadow`. The `/etc/shadow` file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

Note:

- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
- A user account with an empty second field in `/etc/passwd` allows the account to be logged into by providing only the username.

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}'
/etc/passwd
```

Remediation:

Run the following command to set accounts to use shadowed passwords and migrate passwords in `/etc/passwd` to `/etc/shadow`:

```
# pwconv
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

References:

1. NIST SP 800-53 Rev. 5: IA-5
2. PWCONV(8)

Additional Information:

The `pwconv` command creates shadow from `passwd` and an optionally existing `shadow`.

- The `pwunconv` command creates `passwd` from `passwd` and `shadow` and then removes `shadow`.
- The `grpconv` command creates `gshadow` from `group` and an optionally existing `gshadow`.
- The `grpunconv` command creates `group` from `group` and `gshadow` and then removes `gshadow`.

These four programs all operate on the normal and shadow password and group files: `/etc/passwd`, `/etc/group`, `/etc/shadow`, and `/etc/gshadow`.

Each program acquires the necessary locks before conversion. `pwconv` and `grpconv` are similar. First, entries in the shadowed file which don't exist in the main file are removed. Then, shadowed entries which don't have `x' as the password in the main file are updated. Any missing shadowed entries are added. Finally, passwords in the main file are replaced with` x'. These programs can be used for initial conversion as well to update the shadowed file if the main file is edited by hand.

`pwconv` will use the values of PASS_MIN_DAYS, PASS_MAX_DAYS, and PASS_WARN_AGE from /etc/login.defs when adding new entries to /etc/shadow.

`pwunconv` and `grpunconv` are similar. Passwords in the main file are updated from the shadowed file. Entries which exist in the main file but not in the shadowed file are left alone. Finally, the shadowed file is removed. Some password aging information is lost by `pwunconv`. It will convert what it can.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1003, T1003.008	TA0003	M1027

6.2.2 Ensure /etc/shadow password fields are not empty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow
```

Remediation:

If any accounts in the `/etc/shadow` file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

References:

1. NIST SP 800-53 Rev. 5: IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0003	M1027

6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group` .

Rationale:

Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
   for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
     grep -Pq -- "^.*?:[^:]*:$i:" /etc/group
     if [ $? -ne 0 ]; then
       echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
     fi
   done
}
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0003	M1027

6.2.4 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
  while read -r l_count l_uid; do
    if [ "$l_count" -gt 1 ]; then
      echo -e "Duplicate UID: \"$l_uid\" Users: \"$(awk -F: '($3 == n) {
print $1 }' n=$l_uid /etc/passwd | xargs)\""
    fi
  done < <(cut -f3 -d":" /etc/passwd | sort -n | uniq -c)
}
```

Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

6.2.5 Ensure no duplicate GIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
   while read -r l_count l_gid; do
      if [ "$l_count" -gt 1 ]; then
      echo -e "Duplicate GID: \"$l_gid\" Groups: \"$(awk -F: '($3 == n) {
print $1 }' n=$l_gid /etc/group | xargs)\""
    fi
  done < <(cut -f3 -d":" /etc/group | sort -n | uniq -c)
}
```

Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

6.2.6 Ensure no duplicate user names exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the username.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd` . For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
   while read -r l_count l_user; do
      if [ "$l_count" -gt 1 ]; then
         echo -e "Duplicate User: \"$l_user\" Users: \"$(awk -F: '($1 == n) {
print $1 }' n=$l_user /etc/passwd | xargs)\""
      fi
   done < <(cut -f1 -d":" /etc/passwd | sort -n | uniq -c)
}
```

Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0004	M1027

6.2.7 Ensure no duplicate group names exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group` . Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
   while read -r l_count l_group; do
      if [ "$l_count" -gt 1 ]; then
         echo -e "Duplicate Group: \"$l_group\" Groups: \"$(awk -F: '($1 ==
n) { print $1 }' n=$l_group /etc/group | xargs)\""
      fi
   done < <(cut -f1 -d":" /etc/group | sort -n | uniq -c)
}
```

Remediation:

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0004	M1027

6.2.8 Ensure root path integrity (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

Run the following script to verify root's path does not include:

- Locations that are not directories
- An empty directory (`::`)
- A trailing (`:`)
- Current working directory (`.`)
- Non `root` owned directories
- Directories that less restrictive than mode `0755`

```
#!/usr/bin/env bash

{
   l_output2=""
   l_pmask="0022"
   l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
   l_root_path="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"
   unset a_path_loc && IFS=":" read -ra a_path_loc <<< "$l_root_path"
   grep -q "::" <<< "$l_root_path" && l_output2="$l_output2\n - root's path
contains a empty directory (::)"
   grep -Pq ":\h*$" <<< "$l_root_path" && l_output2="$l_output2\n - root's
path contains a trailing (:)"
   grep -Pq '(\h+|:)\.(:|\h*$)' <<< "$l_root_path" && l_output2="$l_output2\n
- root's path contains current working directory (.)"
   while read -r l_path; do
      if [ -d "$l_path" ]; then
         while read -r l_fmode l_fown; do
            [ "$l_fown" != "root" ] && l_output2="$l_output2\n - Directory:
\"$l_path\" is owned by: \"$l_fown\" should be owned by \"root\""
            [ $(( $l_fmode & $l_pmask )) -gt 0 ] && l_output2="$l_output2\n -
Directory: \"$l_path\" is mode: \"$l_fmode\" and should be mode:
\"$l_maxperm\" or more restrictive"
         done <<< "$(stat -Lc '%#a %U' "$l_path")"
      else
         l_output2="$l_output2\n - \"$l_path\" is not a directory"
      fi
   done <<< "$(printf "%s\n" "${a_path_loc[@]}")"
   if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  *** PASS ***\n - Root's path is correctly
configured\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
   fi
}
```

Remediation:

Correct or justify any:

- Locations that are not directories
- Empty directories (`::`)
- Trailing (`:`)
- Current working directory (`.`)
- Non `root` owned directories
- Directories that less restrictive than mode `0755`

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1204, T1204.002	TA0006	M1022

6.2.9 Ensure root is the only UID 0 account (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

Audit:

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd

root
```

Remediation:

Remove any users other than `root` with UID `0` or assign them a new UID if appropriate.

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0001	M1026

6.2.10 Ensure local interactive user home directories are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Run the following script to:

- Ensure local interactive user home directories exist
- Ensure local interactive users own their home directories
- Ensure local interactive user home directories are mode 750 or more restrictive

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_heout2="" l_hoout2="" l_haout2=""
   l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed -rn
'/^\//{s,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
   unset a_uarr && a_uarr=() # Clear and initialize array
   while read -r l_epu l_eph; do # Populate array with users and user home location
      a_uarr+=("$l_epu $l_eph")
   done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd)"
   l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding
   [ "$l_asize " -gt "10000" ] && echo -e "\n  ** INFO **\n  - \"$l_asize\" Local interactive
users found on the system\n  - This may be a long running check\n"
   while read -r l_user l_home; do
      if [ -d "$l_home" ]; then
         l_mask='0027'
         l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
         while read -r l_own l_mode; do
            [ "$l_user" != "$l_own" ] && l_hoout2="$l_hoout2\n  - User: \"$l_user\" Home
\"$l_home\" is owned by: \"$l_own\""
            if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
               l_haout2="$l_haout2\n  - User: \"$l_user\" Home \"$l_home\" is mode: \"$l_mode\"
should be mode: \"$l_max\" or more restrictive"
            fi
         done <<< "$(stat -Lc '%U %#a' "$l_home")"
      else
         l_heout2="$l_heout2\n  - User: \"$l_user\" Home \"$l_home\" Doesn't exist"
      fi
   done <<< "$(printf '%s\n' "${a_uarr[@]}")"
   [ -z "$l_heout2" ] && l_output="$l_output\n   - home directories exist" ||
l_output2="$l_output2$l_heout2"
   [ -z "$l_hoout2" ] && l_output="$l_output\n   - own their home directory" ||
l_output2="$l_output2$l_hoout2"
   [ -z "$l_haout2" ] && l_output="$l_output\n   - home directories are mode: \"$l_max\" or more
restrictive" || l_output2="$l_output2$l_haout2"
   [ -n "$l_output" ] && l_output="  - All local interactive users:$l_output"
   if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
      echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured * :\n$l_output"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit failure * :\n$l_output2"
      [ -n "$l_output" ] && echo -e "\n- * Correctly configured * :\n$l_output"
   fi
}
```

Remediation:

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:

- Lock the user account
- Remove the user from the system
- Create a directory for the user. If undefined, edit `/etc/passwd` and add the absolute path to the directory to the last field of the user.

Run the following script to:

- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner

```
#!/usr/bin/env bash

{
   l_output2=""
   l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed -rn
'/^\//{s,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
   unset a_uarr && a_uarr=() # Clear and initialize array
   while read -r l_epu l_eph; do # Populate array with users and user home location
      a_uarr+=("$l_epu $l_eph")
   done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }'
/etc/passwd)"
   l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding
   [ "$l_asize " -gt "10000" ] && echo -e "\n  ** INFO **\n  - \"$l_asize\" Local interactive
users found on the system\n  - This may be a long running process\n"
   while read -r l_user l_home; do
      if [ -d "$l_home" ]; then
         l_mask='0027'
         l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
         while read -r l_own l_mode; do
            if [ "$l_user" != "$l_own" ]; then
               l_output2="$l_output2\n  - User: \"$l_user\" Home \"$l_home\" is owned by:
\"$l_own\"\n  -  changing ownership to: \"$l_user\"\n"
               chown "$l_user" "$l_home"
            fi
            if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
               l_output2="$l_output2\n  - User: \"$l_user\" Home \"$l_home\" is mode: \"$l_mode\"
should be mode: \"$l_max\" or more restrictive\n  -  removing excess permissions\n"
               chmod g-w,o-rwx "$l_home"
            fi
         done <<< "$(stat -Lc '%U %#a' "$l_home")"
      else
         l_output2="$l_output2\n  - User: \"$l_user\" Home \"$l_home\" Doesn't exist\n  -  Please
create a home in accordance with local site policy"
      fi
   done <<< "$(printf '%s\n' "${a_uarr[@]}")"
   if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
      echo -e " - No modification needed to local interactive users home directories"
   else
      echo -e "\n$l_output2"
   fi
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.002	TA0005	M1022

6.2.11 Ensure local interactive user dot files access is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

- `.forward` file specifies an email address to forward the user's mail to.
- `.rhost` file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- `.netrc` file contains data for logging into a remote host or passing authentication to an API.
- `.bash_history` file keeps track of the user's last 500 commands.

Rationale:

User configuration files with excessive or incorrect access may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script to verify local interactive user dot files:

- Don't include `.forward`, `.rhost`, or `.netrc` files
- Are mode 0644 or more restrictive
- Are owned by the local interactive user
- Are group owned by the user's primary group
- `.bash_history` is mode 0600 or more restrictive

Note: If a `.netrc` file is required, and follows local site policy, it should be mode `0600` or more restrictive.

```
#!/usr/bin/env bash

{
   l_output="" l_output2="" l_output3=""
   l_bf="" l_df="" l_nf="" l_hf=""
   l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^\//{s,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
   unset a_uarr && a_uarr=() # Clear and initialize array
   while read -r l_epu l_eph; do # Populate array with users and user home
location
      [[ -n "$l_epu" && -n "$l_eph" ]] && a_uarr+=("$l_epu $l_eph")
   done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
   l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
   l_maxsize="1000" # Maximun number of local interactive users before
warning (Default 1,000)
   [ "$l_asize " -gt "$l_maxsize" ] && echo -e "\n  ** INFO **\n  -
\"$l_asize\" Local interactive users found on the system\n  - This may be a
long running check\n"
   file_access_chk()
   {
      l_facout2=""
      l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
      if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
         l_facout2="$l_facout2\n  - File: \"$l_hdfile\" is mode: \"$l_mode\"
and should be mode: \"$l_max\" or more restrictive"
      fi
      if [[ ! "$l_owner" =~ ($l_user) ]]; then
         l_facout2="$l_facout2\n  - File: \"$l_hdfile\" owned by:
\"$l_owner\" and should be owned by \"${l_user//|/ or }\""
      fi
      if [[ ! "$l_gowner" =~ ($l_group) ]]; then
         l_facout2="$l_facout2\n  - File: \"$l_hdfile\" group owned by:
\"$l_gowner\" and should be group owned by \"${l_group//|/ or }\""
      fi
   }
   while read -r l_user l_home; do
      l_fe="" l_nout2="" l_nout3="" l_dfout2="" l_hdout2="" l_bhout2=""
      if [ -d "$l_home" ]; then
         l_group="$(id -gn "$l_user" | xargs)"
         l_group="${l_group// /|}"
         while IFS= read -r -d $'\0' l_hdfile; do
            while read -r l_mode l_owner l_gowner; do
               case "$(basename "$l_hdfile")" in
                  .forward | .rhost )
                     l_fe="Y" && l_bf="Y"
                     l_dfout2="$l_dfout2\n  - File: \"$l_hdfile\" exists" ;;
                  .netrc )
                     l_mask='0177'
                     file_access_chk
                     if [ -n "$l_facout2" ]; then
                        l_fe="Y" && l_nf="Y"
                        l_nout2="$l_facout2"
                     else
                        l_nout3="   - File: \"$l_hdfile\" exists"
                     fi ;;
```

```
                  .bash_history )
                     l_mask='0177'
                     file_access_chk
                     if [ -n "$l_facout2" ]; then
                        l_fe="Y" && l_hf="Y"
                        l_bhout2="$l_facout2"
                     fi ;;
                  * )
                     l_mask='0133'
                     file_access_chk
                     if [ -n "$l_facout2" ]; then
                        l_fe="Y" && l_df="Y"
                        l_hdout2="$l_facout2"
                     fi ;;
                  esac
            done <<< "$(stat -Lc '%#a %U %G' "$l_hdfile")"
         done < <(find "$l_home" -xdev -type f -name '.*' -print0)
      fi
      if [ "$l_fe" = "Y" ]; then
         l_output2="$l_output2\n - User: \"$l_user\" Home Directory:
\"$l_home\""
         [ -n "$l_dfout2" ] && l_output2="$l_output2$l_dfout2"
         [ -n "$l_nout2" ] && l_output2="$l_output2$l_nout2"
         [ -n "$l_bhout2" ] && l_output2="$l_output2$l_bhout2"
         [ -n "$l_hdout2" ] && l_output2="$l_output2$l_hdout2"
      fi
      [ -n "$l_nout3" ] && l_output3="$l_output3\n  - User: \"$l_user\" Home
Directory: \"$l_home\"\n$l_nout3"
   done <<< "$(printf '%s\n' "${a_uarr[@]}")"
   unset a_uarr # Remove array
   [ -n "$l_output3" ] && l_output3=" - ** Warning **\n - \".netrc\" files
should be removed unless deemed necessary\n   and in accordance with local
site policy:$l_output3"
   [ -z "$l_bf" ] && l_output="$l_output\n   - \".forward\" or \".rhost\"
files"
   [ -z "$l_nf" ] && l_output="$l_output\n   - \".netrc\" files with
incorrect access configured"
   [ -z "$l_hf" ] && l_output="$l_output\n   - \".bash_history\" files with
incorrect access configured"
   [ -z "$l_df" ] && l_output="$l_output\n   - \"dot\" files with incorrect
access configured"
   [ -n "$l_output" ] && l_output="  - No local interactive users home
directories contain:$l_output"
   if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
      echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:\n$l_output\n"
      echo -e "$l_output3\n"
   else
      echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
      echo -e "$l_output3\n"
      [ -n "$l_output" ] && echo -e "- * Correctly configured *
:\n$l_output\n"
   fi
}
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.
The following script will:

- remove excessive permissions on `dot` files within interactive users' home directories
- change ownership of `dot` files within interactive users' home directories to the user
- change group ownership of `dot` files within interactive users' home directories to the user's primary group
- list `.forward` and `.rhost` files to be investigated and manually deleted

```
#!/usr/bin/env bash

{
   l_valid_shells="^($( awk -F\/ '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^\//{s,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
   unset a_uarr && a_uarr=() # Clear and initialize array
   while read -r l_epu l_eph; do # Populate array with users and user home
location
      [[ -n "$l_epu" && -n "$l_eph" ]] && a_uarr+=("$l_epu $l_eph")
   done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
   l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
   l_maxsize="1000" # Maximum number of local interactive users before
warning (Default 1,000)
   [ "$l_asize " -gt "$l_maxsize" ] && echo -e "\n  ** INFO **\n  -
\"$l_asize\" Local interactive users found on the system\n  - This may be a
long running check\n"
   file_access_fix()
   {
      l_facout2=""
      l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
      if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
         echo -e "  - File: \"$l_hdfile\" is mode: \"$l_mode\" and should be
mode: \"$l_max\" or more restrictive\n   - Changing to mode \"$l_max\""
         chmod "$l_chp" "$l_hdfile"
      fi
      if [[ ! "$l_owner" =~ ($l_user) ]]; then
         echo -e "  - File: \"$l_hdfile\" owned by: \"$l_owner\" and should
be owned by \"${l_user//|/ or }\"\n   - Changing ownership to \"$l_user\""
         chown "$l_user" "$l_hdfile"
      fi
      if [[ ! "$l_gowner" =~ ($l_group) ]]; then
         echo -e "  - File: \"$l_hdfile\" group owned by: \"$l_gowner\" and
should be group owned by \"${l_group//|/ or }\"\n   - Changing group
ownership to \"$l_group\""
         chgrp "$l_group" "$l_hdfile"
      fi
   }
   while read -r l_user l_home; do
      if [ -d "$l_home" ]; then
         echo -e "\n - Checking user: \"$l_user\" home directory:
\"$l_home\""
         l_group="$(id -gn "$l_user" | xargs)"
         l_group="${l_group// /|}"
         while IFS= read -r -d $'\0' l_hdfile; do
            while read -r l_mode l_owner l_gowner; do
               case "$(basename "$l_hdfile")" in
                  .forward | .rhost )
                     echo -e "  - File: \"$l_hdfile\" exists\n   - Please
investigate and manually delete \"$l_hdfile\""
                  ;;
                  .netrc )
                     l_mask='0177'
                     l_chp="u-x,go-rwx"
                     file_access_fix ;;
                  .bash_history )
```

```
                    l_mask='0177'
                    l_chp="u-x,go-rwx"
                    file_access_fix ;;
                 * )
                    l_mask='0133'
                    l_chp="u-x,go-wx"
                    file_access_fix ;;
                 esac
           done <<< "$(stat -Lc '%#a %U %G' "$l_hdfile")"
        done < <(find "$l_home" -xdev -type f -name '.*' -print0)
     fi
  done <<< "$(printf '%s\n' "${a_uarr[@]}")"
  unset a_uarr # Remove array
}
```

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1222, T1222.001, T1222.002, T1552, T1552.003, T1552.004	TA0005	M1022

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Initial Setup**		
1.1	**Filesystem**		
1.1.1	**Configure Filesystem Kernel Modules**		
1.1.1.1	Ensure cramfs kernel module is not available (Automated)	☐	☐
1.1.1.2	Ensure freevxfs kernel module is not available (Automated)	☐	☐
1.1.1.3	Ensure hfs kernel module is not available (Automated)	☐	☐
1.1.1.4	Ensure hfsplus kernel module is not available (Automated)	☐	☐
1.1.1.5	Ensure jffs2 kernel module is not available (Automated)	☐	☐
1.1.1.6	Ensure squashfs kernel module is not available (Automated)	☐	☐
1.1.1.7	Ensure udf kernel module is not available (Automated)	☐	☐
1.1.1.8	Ensure usb-storage kernel module is not available (Automated)	☐	☐
1.1.2	**Configure Filesystem Partitions**		
1.1.2.1	**Configure /tmp**		
1.1.2.1.1	Ensure /tmp is a separate partition (Automated)	☐	☐
1.1.2.1.2	Ensure nodev option set on /tmp partition (Automated)	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition (Automated)	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.2.2	**Configure /dev/shm**		
1.1.2.2.1	Ensure /dev/shm is a separate partition (Automated)	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition (Automated)	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition (Automated)	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition (Automated)	☐	☐
1.1.2.3	**Configure /home**		
1.1.2.3.1	Ensure separate partition exists for /home (Automated)	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition (Automated)	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition (Automated)	☐	☐
1.1.2.4	**Configure /var**		
1.1.2.4.1	Ensure separate partition exists for /var (Automated)	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition (Automated)	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition (Automated)	☐	☐
1.1.2.5	**Configure /var/tmp**		
1.1.2.5.1	Ensure separate partition exists for /var/tmp (Automated)	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition (Automated)	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition (Automated)	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.2.6	**Configure /var/log**		
1.1.2.6.1	Ensure separate partition exists for /var/log (Automated)	☐	☐
1.1.2.6.2	Ensure nodev option set on /var/log partition (Automated)	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition (Automated)	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition (Automated)	☐	☐
1.1.2.7	**Configure /var/log/audit**		
1.1.2.7.1	Ensure separate partition exists for /var/log/audit (Automated)	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition (Automated)	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition (Automated)	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition (Automated)	☐	☐
1.2	**Configure Software and Patch Management**		
1.2.1	Ensure GPG keys are configured (Manual)	☐	☐
1.2.2	Ensure gpgcheck is globally activated (Automated)	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated (Manual)	☐	☐
1.2.4	Ensure package manager repositories are configured (Manual)	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed (Manual)	☐	☐
1.3	**Configure Secure Boot Settings**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3.1	Ensure bootloader password is set (Automated)	☐	☐
1.3.2	Ensure permissions on bootloader config are configured (Automated)	☐	☐
1.3.3	Ensure authentication required for single user mode (Automated)	☐	☐
1.4	**Configure Additional Process Hardening**		
1.4.1	Ensure address space layout randomization (ASLR) is enabled (Automated)	☐	☐
1.4.2	Ensure ptrace_scope is restricted (Automated)	☐	☐
1.4.3	Ensure core dump backtraces are disabled (Automated)	☐	☐
1.4.4	Ensure core dump storage is disabled (Automated)	☐	☐
1.5	**Mandatory Access Control**		
1.5.1	**Configure SELinux**		
1.5.1.1	Ensure SELinux is installed (Automated)	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	☐	☐
1.5.1.3	Ensure SELinux policy is configured (Automated)	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled (Automated)	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing (Automated)	☐	☐
1.5.1.6	Ensure no unconfined services exist (Automated)	☐	☐
1.5.1.7	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed (Automated)	☐	☐
1.6	**Configure Command Line Warning Banners**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.6.1	Ensure message of the day is configured properly (Automated)	☐	☐
1.6.2	Ensure local login warning banner is configured properly (Automated)	☐	☐
1.6.3	Ensure remote login warning banner is configured properly (Automated)	☐	☐
1.6.4	Ensure access to /etc/motd is configured (Automated)	☐	☐
1.6.5	Ensure access to /etc/issue is configured (Automated)	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured (Automated)	☐	☐
1.7	**Configure GNOME Display Manager**		
1.7.1	Ensure GNOME Display Manager is removed (Automated)	☐	☐
1.7.2	Ensure GDM login banner is configured (Automated)	☐	☐
1.7.3	Ensure GDM disable-user-list option is enabled (Automated)	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle (Automated)	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden (Automated)	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled (Automated)	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)	☐	☐
1.7.8	Ensure GDM autorun-never is enabled (Automated)	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.7.10	Ensure XDMCP is not enabled (Automated)	☐	☐
2	**Services**		
2.1	**Configure Time Synchronization**		
2.1.1	Ensure time synchronization is in use (Automated)	☐	☐
2.1.2	Ensure chrony is configured (Automated)	☐	☐
2.1.3	Ensure chrony is not run as the root user (Automated)	☐	☐
2.2	**Configure Special Purpose Services**		
2.2.1	Ensure autofs services are not in use (Automated)	☐	☐
2.2.2	Ensure avahi daemon services are not in use (Automated)	☐	☐
2.2.3	Ensure dhcp server services are not in use (Automated)	☐	☐
2.2.4	Ensure dns server services are not in use (Automated)	☐	☐
2.2.5	Ensure dnsmasq services are not in use (Automated)	☐	☐
2.2.6	Ensure samba file server services are not in use (Automated)	☐	☐
2.2.7	Ensure ftp server services are not in use (Automated)	☐	☐
2.2.8	Ensure message access server services are not in use (Automated)	☐	☐
2.2.9	Ensure network file system services are not in use (Automated)	☐	☐
2.2.10	Ensure nis server services are not in use (Automated)	☐	☐
2.2.11	Ensure print server services are not in use (Automated)	☐	☐
2.2.12	Ensure rpcbind services are not in use (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.13	Ensure rsync services are not in use (Automated)	☐	☐
2.2.14	Ensure snmp services are not in use (Automated)	☐	☐
2.2.15	Ensure telnet server services are not in use (Automated)	☐	☐
2.2.16	Ensure tftp server services are not in use (Automated)	☐	☐
2.2.17	Ensure web proxy server services are not in use (Automated)	☐	☐
2.2.18	Ensure web server services are not in use (Automated)	☐	☐
2.2.19	Ensure xinetd services are not in use (Automated)	☐	☐
2.2.20	Ensure X window server services are not in use (Automated)	☐	☐
2.2.21	Ensure mail transfer agents are configured for local-only mode (Automated)	☐	☐
2.2.22	Ensure only approved services are listening on a network interface (Manual)	☐	☐
2.3	**Configure Service Clients**		
2.3.1	Ensure ftp client is not installed (Automated)	☐	☐
2.3.2	Ensure ldap client is not installed (Automated)	☐	☐
2.3.3	Ensure nis client is not installed (Automated)	☐	☐
2.3.4	Ensure telnet client is not installed (Automated)	☐	☐
2.3.5	Ensure tftp client is not installed (Automated)	☐	☐
3	**Network**		
3.1	**Configure Network Devices**		
3.1.1	Ensure IPv6 status is identified (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.2	Ensure wireless interfaces are disabled (Automated)	☐	☐
3.1.3	Ensure bluetooth services are not in use (Automated)	☐	☐
3.2	**Configure Network Kernel Modules**		
3.2.1	Ensure dccp kernel module is not available (Automated)	☐	☐
3.2.2	Ensure tipc kernel module is not available (Automated)	☐	☐
3.2.3	Ensure rds kernel module is not available (Automated)	☐	☐
3.2.4	Ensure sctp kernel module is not available (Automated)	☐	☐
3.3	**Configure Network Kernel Parameters**		
3.3.1	Ensure ip forwarding is disabled (Automated)	☐	☐
3.3.2	Ensure packet redirect sending is disabled (Automated)	☐	☐
3.3.3	Ensure bogus icmp responses are ignored (Automated)	☐	☐
3.3.4	Ensure broadcast icmp requests are ignored (Automated)	☐	☐
3.3.5	Ensure icmp redirects are not accepted (Automated)	☐	☐
3.3.6	Ensure secure icmp redirects are not accepted (Automated)	☐	☐
3.3.7	Ensure reverse path filtering is enabled (Automated)	☐	☐
3.3.8	Ensure source routed packets are not accepted (Automated)	☐	☐
3.3.9	Ensure suspicious packets are logged (Automated)	☐	☐
3.3.10	Ensure tcp syn cookies is enabled (Automated)	☐	☐
3.3.11	Ensure ipv6 router advertisements are not accepted (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4	**Configure Host Based Firewall**		
3.4.1	**Configure firewall utility**		
3.4.1.1	Ensure iptables is installed (Automated)	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use (Automated)	☐	☐
3.4.2	**Configure firewalld**		
3.4.2.1	Ensure firewalld is installed (Automated)	☐	☐
3.4.2.2	Ensure firewalld service enabled and running (Automated)	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports (Manual)	☐	☐
3.4.2.4	Ensure network interfaces are assigned to appropriate zone (Manual)	☐	☐
3.4.3	**Configure nftables**		
3.4.3.1	Ensure nftables is installed (Automated)	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables (Manual)	☐	☐
3.4.3.3	Ensure an nftables table exists (Automated)	☐	☐
3.4.3.4	Ensure nftables base chains exist (Automated)	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured (Automated)	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured (Manual)	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy (Automated)	☐	☐
3.4.3.8	Ensure nftables service is enabled and active (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4.3.9	Ensure nftables rules are permanent (Automated)	☐	☐
3.4.4	**Configure iptables**		
3.4.4.1	**Configure iptables software**		
3.4.4.1.1	Ensure iptables packages are installed (Automated)	☐	☐
3.4.4.2	**Configure iptables**		
3.4.4.2.1	Ensure iptables loopback traffic is configured (Automated)	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured (Manual)	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports (Automated)	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy (Automated)	☐	☐
3.4.4.2.5	Ensure iptables rules are saved (Automated)	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active (Automated)	☐	☐
3.4.4.3	**Configure ip6tables**		
3.4.4.3.1	Ensure ip6tables loopback traffic is configured (Automated)	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured (Manual)	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports (Automated)	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy (Automated)	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved (Automated)	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	**Access, Authentication and Authorization**		
4.1	**Configure job schedulers**		
4.1.1	**Configure cron**		
4.1.1.1	Ensure cron daemon is enabled and active (Automated)	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured (Automated)	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	☐	☐
4.1.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users (Automated)	☐	☐
4.1.2	**Configure at**		
4.1.2.1	Ensure at is restricted to authorized users (Automated)	☐	☐
4.2	**Configure SSH Server**		
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.3	Ensure permissions on SSH public host key files are configured (Automated)	☐	☐
4.2.4	Ensure sshd access is configured (Automated)	☐	☐
4.2.5	Ensure sshd Banner is configured (Automated)	☐	☐
4.2.6	Ensure sshd Ciphers are configured (Automated)	☐	☐
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled (Automated)	☐	☐
4.2.9	Ensure sshd GSSAPIAuthentication is disabled (Automated)	☐	☐
4.2.10	Ensure sshd HostbasedAuthentication is disabled (Automated)	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled (Automated)	☐	☐
4.2.12	Ensure sshd KexAlgorithms is configured (Automated)	☐	☐
4.2.13	Ensure sshd LoginGraceTime is configured (Automated)	☐	☐
4.2.14	Ensure sshd LogLevel is configured (Automated)	☐	☐
4.2.15	Ensure sshd MACs are configured (Automated)	☐	☐
4.2.16	Ensure sshd MaxAuthTries is configured (Automated)	☐	☐
4.2.17	Ensure sshd MaxSessions is configured (Automated)	☐	☐
4.2.18	Ensure sshd MaxStartups is configured (Automated)	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled (Automated)	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.21	Ensure sshd PermitUserEnvironment is disabled (Automated)	☐	☐
4.2.22	Ensure sshd UsePAM is enabled (Automated)	☐	☐
4.3	**Configure privilege escalation**		
4.3.1	Ensure sudo is installed (Automated)	☐	☐
4.3.2	Ensure sudo commands use pty (Automated)	☐	☐
4.3.3	Ensure sudo log file exists (Automated)	☐	☐
4.3.4	Ensure users must provide password for escalation (Automated)	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally (Automated)	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly (Automated)	☐	☐
4.3.7	Ensure access to the su command is restricted (Automated)	☐	☐
4.4	**Configure Pluggable Authentication Modules**		
4.4.1	**Configure PAM software packages**		
4.4.1.1	Ensure latest version of pam is installed (Automated)	☐	☐
4.4.1.2	Ensure libpwquality is installed (Automated)	☐	☐
4.4.2	**Configure pluggable module arguments**		
4.4.2.1	**Configure pam_faillock module**		
4.4.2.1.1	Ensure pam_faillock module is enabled (Automated)	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.4.2.1.3	Ensure password unlock time is configured (Automated)	☐	☐
4.4.2.1.4	Ensure password failed attempts lockout includes root account (Automated)	☐	☐
4.4.2.2	**Configure pam_pwquality module**		
4.4.2.2.1	Ensure pam_pwquality module is enabled (Automated)	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured (Automated)	☐	☐
4.4.2.2.3	Ensure password length is configured (Automated)	☐	☐
4.4.2.2.4	Ensure password complexity is configured (Manual)	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured (Automated)	☐	☐
4.4.2.2.6	Ensure password maximum sequential characters is configured (Automated)	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled (Automated)	☐	☐
4.4.2.3	**Configure pam_pwhistory module**		
4.4.2.3.1	Ensure pam_pwhistory module is enabled (Automated)	☐	☐
4.4.2.3.2	Ensure password history remember is configured (Automated)	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user (Automated)	☐	☐
4.4.2.3.4	Ensure pam_pwhistory includes use_authtok (Automated)	☐	☐
4.4.2.4	**Configure pam_unix module**		
4.4.2.4.1	Ensure pam_unix does not include nullok (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.4.2.4.2	Ensure pam_unix does not include remember (Automated)	☐	☐
4.4.2.4.3	Ensure pam_unix includes a strong password hashing algorithm (Automated)	☐	☐
4.4.2.4.4	Ensure pam_unix includes use_authtok (Automated)	☐	☐
4.5	**User Accounts and Environment**		
4.5.1	**Configure shadow password suite parameters**		
4.5.1.1	Ensure strong password hashing algorithm is configured (Automated)	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less (Automated)	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more (Automated)	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	☐	☐
4.5.1.5	Ensure all users last password change date is in the past (Automated)	☐	☐
4.5.2	**Configure root and system accounts and environment**		
4.5.2.1	Ensure default group for the root account is GID 0 (Automated)	☐	☐
4.5.2.2	Ensure root user umask is configured (Automated)	☐	☐
4.5.2.3	Ensure system accounts are secured (Automated)	☐	☐
4.5.2.4	Ensure root password is set (Automated)	☐	☐
4.5.3	**Configure user default environment**		
4.5.3.1	Ensure nologin is not listed in /etc/shells (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.3.2	Ensure default user shell timeout is configured (Automated)	☐	☐
4.5.3.3	Ensure default user umask is configured (Automated)	☐	☐
5	**Logging and Auditing**		
5.1	**Configure Logging**		
5.1.1	**Configure rsyslog**		
5.1.1.1	Ensure rsyslog is installed (Automated)	☐	☐
5.1.1.2	Ensure rsyslog service is enabled (Manual)	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog (Manual)	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured (Automated)	☐	☐
5.1.1.5	Ensure logging is configured (Manual)	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host (Manual)	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client (Automated)	☐	☐
5.1.2	**Configure journald**		
5.1.2.1	**Ensure journald is configured to send logs to a remote log host**		
5.1.2.1.1	Ensure systemd-journal-remote is installed (Manual)	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured (Manual)	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled (Manual)	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.2.2	Ensure journald service is enabled (Automated)	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files (Automated)	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk (Automated)	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog (Manual)	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy (Manual)	☐	☐
5.1.3	Ensure logrotate is configured (Manual)	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured (Automated)	☐	☐
5.2	**Configure System Accounting (auditd)**		
5.2.1	**Ensure auditing is enabled**		
5.2.1.1	Ensure audit is installed (Automated)	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled (Automated)	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient (Automated)	☐	☐
5.2.1.4	Ensure auditd service is enabled (Automated)	☐	☐
5.2.2	**Configure Data Retention**		
5.2.2.1	Ensure audit log storage size is configured (Automated)	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted (Automated)	☐	☐
5.2.2.3	Ensure system is disabled when audit logs are full (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.2.4	Ensure system warns when audit logs are low on space (Automated)	☐	☐
5.2.3	**Configure auditd rules**		
5.2.3.1	Ensure changes to system administration scope (sudoers) is collected (Automated)	☐	☐
5.2.3.2	Ensure actions as another user are always logged (Automated)	☐	☐
5.2.3.3	Ensure events that modify the sudo log file are collected (Automated)	☐	☐
5.2.3.4	Ensure events that modify date and time information are collected (Automated)	☐	☐
5.2.3.5	Ensure events that modify the system's network environment are collected (Automated)	☐	☐
5.2.3.6	Ensure use of privileged commands are collected (Automated)	☐	☐
5.2.3.7	Ensure unsuccessful file access attempts are collected (Automated)	☐	☐
5.2.3.8	Ensure events that modify user/group information are collected (Automated)	☐	☐
5.2.3.9	Ensure discretionary access control permission modification events are collected (Automated)	☐	☐
5.2.3.10	Ensure successful file system mounts are collected (Automated)	☐	☐
5.2.3.11	Ensure session initiation information is collected (Automated)	☐	☐
5.2.3.12	Ensure login and logout events are collected (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.3.13	Ensure file deletion events by users are collected (Automated)	☐	☐
5.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected (Automated)	☐	☐
5.2.3.20	Ensure the audit configuration is immutable (Automated)	☐	☐
5.2.3.21	Ensure the running and on disk configuration is the same (Manual)	☐	☐
5.2.4	**Configure auditd file access**		
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive (Automated)	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive (Automated)	☐	☐
5.2.4.3	Ensure only authorized users own audit log files (Automated)	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files (Automated)	☐	☐
5.2.4.5	Ensure audit configuration files are 640 or more restrictive (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.4.6	Ensure audit configuration files are owned by root (Automated)	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root (Automated)	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive (Automated)	☐	☐
5.2.4.9	Ensure audit tools are owned by root (Automated)	☐	☐
5.2.4.10	Ensure audit tools belong to group root (Automated)	☐	☐
5.3	**Configure Integrity Checking**		
5.3.1	Ensure AIDE is installed (Automated)	☐	☐
5.3.2	Ensure filesystem integrity is regularly checked (Automated)	☐	☐
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Ensure permissions on /etc/passwd are configured (Automated)	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured (Automated)	☐	☐
6.1.3	Ensure permissions on /etc/group are configured (Automated)	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured (Automated)	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured (Automated)	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1.7	Ensure permissions on /etc/gshadow are configured (Automated)	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured (Automated)	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured (Automated)	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured (Automated)	☐	☐
6.1.11	Ensure world writable files and directories are secured (Automated)	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist (Automated)	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed (Manual)	☐	☐
6.1.14	Audit system file permissions (Manual)	☐	☐
6.2	**Local User and Group Settings**		
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords (Automated)	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty (Automated)	☐	☐
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	☐	☐
6.2.4	Ensure no duplicate UIDs exist (Automated)	☐	☐
6.2.5	Ensure no duplicate GIDs exist (Automated)	☐	☐
6.2.6	Ensure no duplicate user names exist (Automated)	☐	☐
6.2.7	Ensure no duplicate group names exist (Automated)	☐	☐
6.2.8	Ensure root path integrity (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2.9	Ensure root is the only UID 0 account (Automated)	☐	☐
6.2.10	Ensure local interactive user home directories are configured (Automated)	☐	☐
6.2.11	Ensure local interactive user dot files access is configured (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.15	Ensure telnet server services are not in use	☐	☐
2.3.2	Ensure ldap client is not installed	☐	☐
2.3.4	Ensure telnet client is not installed	☐	☐
3.3.9	Ensure suspicious packets are logged	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.3.6	Ensure use of privileged commands are collected	☐	☐
5.2.3.12	Ensure login and logout events are collected	☐	☐
5.2.3.13	Ensure file deletion events by users are collected	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	☐	☐
1.1.1.2	Ensure freevxfs kernel module is not available	☐	☐
1.1.1.3	Ensure hfs kernel module is not available	☐	☐
1.1.1.4	Ensure hfsplus kernel module is not available	☐	☐
1.1.1.5	Ensure jffs2 kernel module is not available	☐	☐
1.1.1.6	Ensure squashfs kernel module is not available	☐	☐
1.1.1.7	Ensure udf kernel module is not available	☐	☐
1.1.1.8	Ensure usb-storage kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nodev option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure /dev/shm is a separate partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/log	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.4.2	Ensure ptrace_scope is restricted	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.6	Ensure no unconfined services exist	☐	☐
1.5.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.7.1	Ensure GNOME Display Manager is removed	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
1.7.10	Ensure XDMCP is not enabled	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.1.2	Ensure chrony is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure avahi daemon services are not in use	☐	☐
2.2.3	Ensure dhcp server services are not in use	☐	☐
2.2.4	Ensure dns server services are not in use	☐	☐
2.2.5	Ensure dnsmasq services are not in use	☐	☐
2.2.6	Ensure samba file server services are not in use	☐	☐
2.2.7	Ensure ftp server services are not in use	☐	☐
2.2.8	Ensure message access server services are not in use	☐	☐
2.2.9	Ensure network file system services are not in use	☐	☐
2.2.10	Ensure nis server services are not in use	☐	☐
2.2.11	Ensure print server services are not in use	☐	☐
2.2.12	Ensure rpcbind services are not in use	☐	☐
2.2.13	Ensure rsync services are not in use	☐	☐
2.2.14	Ensure snmp services are not in use	☐	☐
2.2.15	Ensure telnet server services are not in use	☐	☐
2.2.16	Ensure tftp server services are not in use	☐	☐
2.2.17	Ensure web proxy server services are not in use	☐	☐
2.2.18	Ensure web server services are not in use	☐	☐
2.2.19	Ensure xinetd services are not in use	☐	☐
2.2.20	Ensure X window server services are not in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.21	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.22	Ensure only approved services are listening on a network interface	☐	☐
2.3.1	Ensure ftp client is not installed	☐	☐
2.3.2	Ensure ldap client is not installed	☐	☐
2.3.3	Ensure nis client is not installed	☐	☐
2.3.4	Ensure telnet client is not installed	☐	☐
2.3.5	Ensure tftp client is not installed	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.1.3	Ensure bluetooth services are not in use	☐	☐
3.2.1	Ensure dccp kernel module is not available	☐	☐
3.2.2	Ensure tipc kernel module is not available	☐	☐
3.2.3	Ensure rds kernel module is not available	☐	☐
3.2.4	Ensure sctp kernel module is not available	☐	☐
3.3.1	Ensure ip forwarding is disabled	☐	☐
3.3.2	Ensure packet redirect sending is disabled	☐	☐
3.3.3	Ensure bogus icmp responses are ignored	☐	☐
3.3.4	Ensure broadcast icmp requests are ignored	☐	☐
3.3.5	Ensure icmp redirects are not accepted	☐	☐
3.3.6	Ensure secure icmp redirects are not accepted	☐	☐
3.3.7	Ensure reverse path filtering is enabled	☐	☐
3.3.8	Ensure source routed packets are not accepted	☐	☐
3.3.9	Ensure suspicious packets are logged	☐	☐
3.3.10	Ensure tcp syn cookies is enabled	☐	☐
3.3.11	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.12	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.15	Ensure sshd MACs are configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.22	Ensure sshd UsePAM is enabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.3	Ensure sudo log file exists	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.4.1.2	Ensure libpwquality is installed	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured	☐	☐
4.4.2.1.3	Ensure password unlock time is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.2.1.4	Ensure password failed attempts lockout includes root account	☐	☐
4.4.2.2.1	Ensure pam_pwquality module is enabled	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured	☐	☐
4.4.2.2.3	Ensure password length is configured	☐	☐
4.4.2.2.4	Ensure password complexity is configured	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured	☐	☐
4.4.2.2.6	Ensure password maximum sequential characters is configured	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled	☐	☐
4.4.2.3.1	Ensure pam_pwhistory module is enabled	☐	☐
4.4.2.3.2	Ensure password history remember is configured	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user	☐	☐
4.4.2.3.4	Ensure pam_pwhistory includes use_authtok	☐	☐
4.4.2.4.1	Ensure pam_unix does not include nullok	☐	☐
4.4.2.4.2	Ensure pam_unix does not include remember	☐	☐
4.4.2.4.3	Ensure pam_unix includes a strong password hashing algorithm	☐	☐
4.4.2.4.4	Ensure pam_unix includes use_authtok	☐	☐
4.5.1.1	Ensure strong password hashing algorithm is configured	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less	☐	☐
4.5.1.5	Ensure all users last password change date is in the past	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.3	Ensure logrotate is configured	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.2.1	Ensure audit log storage size is configured	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted	☐	☐
5.2.3.1	Ensure changes to system administration scope (sudoers) is collected	☐	☐
5.2.3.2	Ensure actions as another user are always logged	☐	☐
5.2.3.3	Ensure events that modify the sudo log file are collected	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.3.4	Ensure events that modify date and time information are collected	☐	☐
5.2.3.5	Ensure events that modify the system's network environment are collected	☐	☐
5.2.3.6	Ensure use of privileged commands are collected	☐	☐
5.2.3.8	Ensure events that modify user/group information are collected	☐	☐
5.2.3.9	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.10	Ensure successful file system mounts are collected	☐	☐
5.2.3.11	Ensure session initiation information is collected	☐	☐
5.2.3.12	Ensure login and logout events are collected	☐	☐
5.2.3.13	Ensure file deletion events by users are collected	☐	☐
5.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected	☐	☐
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.3.21	Ensure the running and on disk configuration is the same	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	☐	☐
1.1.1.2	Ensure freevxfs kernel module is not available	☐	☐
1.1.1.3	Ensure hfs kernel module is not available	☐	☐
1.1.1.4	Ensure hfsplus kernel module is not available	☐	☐
1.1.1.5	Ensure jffs2 kernel module is not available	☐	☐
1.1.1.6	Ensure squashfs kernel module is not available	☐	☐
1.1.1.7	Ensure udf kernel module is not available	☐	☐
1.1.1.8	Ensure usb-storage kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nodev option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure /dev/shm is a separate partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/log	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.4.2	Ensure ptrace_scope is restricted	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.6	Ensure no unconfined services exist	☐	☐
1.5.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.7.1	Ensure GNOME Display Manager is removed	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
1.7.10	Ensure XDMCP is not enabled	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.1.2	Ensure chrony is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure avahi daemon services are not in use	☐	☐
2.2.3	Ensure dhcp server services are not in use	☐	☐
2.2.4	Ensure dns server services are not in use	☐	☐
2.2.5	Ensure dnsmasq services are not in use	☐	☐
2.2.6	Ensure samba file server services are not in use	☐	☐
2.2.7	Ensure ftp server services are not in use	☐	☐
2.2.8	Ensure message access server services are not in use	☐	☐
2.2.9	Ensure network file system services are not in use	☐	☐
2.2.10	Ensure nis server services are not in use	☐	☐
2.2.11	Ensure print server services are not in use	☐	☐
2.2.12	Ensure rpcbind services are not in use	☐	☐
2.2.13	Ensure rsync services are not in use	☐	☐
2.2.14	Ensure snmp services are not in use	☐	☐
2.2.15	Ensure telnet server services are not in use	☐	☐
2.2.16	Ensure tftp server services are not in use	☐	☐
2.2.17	Ensure web proxy server services are not in use	☐	☐
2.2.18	Ensure web server services are not in use	☐	☐
2.2.19	Ensure xinetd services are not in use	☐	☐
2.2.20	Ensure X window server services are not in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.21	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.22	Ensure only approved services are listening on a network interface	☐	☐
2.3.1	Ensure ftp client is not installed	☐	☐
2.3.2	Ensure ldap client is not installed	☐	☐
2.3.3	Ensure nis client is not installed	☐	☐
2.3.4	Ensure telnet client is not installed	☐	☐
2.3.5	Ensure tftp client is not installed	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.1.2	Ensure wireless interfaces are disabled	☐	☐
3.1.3	Ensure bluetooth services are not in use	☐	☐
3.2.1	Ensure dccp kernel module is not available	☐	☐
3.2.2	Ensure tipc kernel module is not available	☐	☐
3.2.3	Ensure rds kernel module is not available	☐	☐
3.2.4	Ensure sctp kernel module is not available	☐	☐
3.3.1	Ensure ip forwarding is disabled	☐	☐
3.3.2	Ensure packet redirect sending is disabled	☐	☐
3.3.3	Ensure bogus icmp responses are ignored	☐	☐
3.3.4	Ensure broadcast icmp requests are ignored	☐	☐
3.3.5	Ensure icmp redirects are not accepted	☐	☐
3.3.6	Ensure secure icmp redirects are not accepted	☐	☐
3.3.7	Ensure reverse path filtering is enabled	☐	☐
3.3.8	Ensure source routed packets are not accepted	☐	☐
3.3.9	Ensure suspicious packets are logged	☐	☐
3.3.10	Ensure tcp syn cookies is enabled	☐	☐
3.3.11	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.12	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.15	Ensure sshd MACs are configured	☐	☐
4.2.16	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.22	Ensure sshd UsePAM is enabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.3	Ensure sudo log file exists	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.4.1.2	Ensure libpwquality is installed	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured	☐	☐
4.4.2.1.3	Ensure password unlock time is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.2.1.4	Ensure password failed attempts lockout includes root account	☐	☐
4.4.2.2.1	Ensure pam_pwquality module is enabled	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured	☐	☐
4.4.2.2.3	Ensure password length is configured	☐	☐
4.4.2.2.4	Ensure password complexity is configured	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured	☐	☐
4.4.2.2.6	Ensure password maximum sequential characters is configured	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled	☐	☐
4.4.2.3.1	Ensure pam_pwhistory module is enabled	☐	☐
4.4.2.3.2	Ensure password history remember is configured	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user	☐	☐
4.4.2.3.4	Ensure pam_pwhistory includes use_authtok	☐	☐
4.4.2.4.1	Ensure pam_unix does not include nullok	☐	☐
4.4.2.4.2	Ensure pam_unix does not include remember	☐	☐
4.4.2.4.3	Ensure pam_unix includes a strong password hashing algorithm	☐	☐
4.4.2.4.4	Ensure pam_unix includes use_authtok	☐	☐
4.5.1.1	Ensure strong password hashing algorithm is configured	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less	☐	☐
4.5.1.5	Ensure all users last password change date is in the past	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.3	Ensure logrotate is configured	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.2.1	Ensure audit log storage size is configured	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted	☐	☐
5.2.3.1	Ensure changes to system administration scope (sudoers) is collected	☐	☐
5.2.3.2	Ensure actions as another user are always logged	☐	☐
5.2.3.3	Ensure events that modify the sudo log file are collected	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.3.4	Ensure events that modify date and time information are collected	☐	☐
5.2.3.5	Ensure events that modify the system's network environment are collected	☐	☐
5.2.3.6	Ensure use of privileged commands are collected	☐	☐
5.2.3.7	Ensure unsuccessful file access attempts are collected	☐	☐
5.2.3.8	Ensure events that modify user/group information are collected	☐	☐
5.2.3.9	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.10	Ensure successful file system mounts are collected	☐	☐
5.2.3.11	Ensure session initiation information is collected	☐	☐
5.2.3.12	Ensure login and logout events are collected	☐	☐
5.2.3.13	Ensure file deletion events by users are collected	☐	☐
5.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected	☐	☐
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.3.21	Ensure the running and on disk configuration is the same	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
5.3.1	Ensure AIDE is installed	☐	☐
5.3.2	Ensure filesystem integrity is regularly checked	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.4.3	Ensure core dump backtraces are disabled	☐	☐
1.4.4	Ensure core dump storage is disabled	☐	☐
1.6.1	Ensure message of the day is configured properly	☐	☐
1.6.2	Ensure local login warning banner is configured properly	☐	☐
1.6.3	Ensure remote login warning banner is configured properly	☐	☐
1.7.2	Ensure GDM login banner is configured	☐	☐
1.7.3	Ensure GDM disable-user-list option is enabled	☐	☐
2.1.3	Ensure chrony is not run as the root user	☐	☐
4.1.1.1	Ensure cron daemon is enabled and active	☐	☐
4.2.5	Ensure sshd Banner is configured	☐	☐
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	☐	☐
4.2.9	Ensure sshd GSSAPIAuthentication is disabled	☐	☐
4.2.10	Ensure sshd HostbasedAuthentication is disabled	☐	☐
4.2.13	Ensure sshd LoginGraceTime is configured	☐	☐
4.2.17	Ensure sshd MaxSessions is configured	☐	☐
4.2.21	Ensure sshd PermitUserEnvironment is disabled	☐	☐
4.4.1.1	Ensure latest version of pam is installed	☐	☐
4.4.2.1.1	Ensure pam_faillock module is enabled	☐	☐
4.5.3.1	Ensure nologin is not listed in /etc/shells	☐	☐
5.2.2.3	Ensure system is disabled when audit logs are full	☐	☐
5.2.2.4	Ensure system warns when audit logs are low on space	☐	☐
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group	☐	☐
6.2.4	Ensure no duplicate UIDs exist	☐	☐
6.2.5	Ensure no duplicate GIDs exist	☐	☐
6.2.6	Ensure no duplicate user names exist	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.7	Ensure no duplicate group names exist	☐	☐
6.2.8	Ensure root path integrity	☐	☐
6.2.9	Ensure root is the only UID 0 account	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.8	Ensure usb-storage kernel module is not available	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.6	Ensure no unconfined services exist	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.22	Ensure sshd UsePAM is enabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.4.1.2	Ensure libpwquality is installed	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured	☐	☐
4.4.2.1.3	Ensure password unlock time is configured	☐	☐
4.4.2.1.4	Ensure password failed attempts lockout includes root account	☐	☐
4.4.2.2.1	Ensure pam_pwquality module is enabled	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured	☐	☐
4.4.2.2.3	Ensure password length is configured	☐	☐
4.4.2.2.4	Ensure password complexity is configured	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.2.2.6	Ensure password maximum sequential characters is configured	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled	☐	☐
4.4.2.3.1	Ensure pam_pwhistory module is enabled	☐	☐
4.4.2.3.2	Ensure password history remember is configured	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user	☐	☐
4.4.2.4.1	Ensure pam_unix does not include nullok	☐	☐
4.4.2.4.2	Ensure pam_unix does not include remember	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less	☐	☐
4.5.1.5	Ensure all users last password change date is in the past	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.3	Ensure logrotate is configured	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.2.1	Ensure audit log storage size is configured	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted	☐	☐
5.2.2.3	Ensure system is disabled when audit logs are full	☐	☐
5.2.2.4	Ensure system warns when audit logs are low on space	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	☐	☐
1.1.1.2	Ensure freevxfs kernel module is not available	☐	☐
1.1.1.3	Ensure hfs kernel module is not available	☐	☐
1.1.1.4	Ensure hfsplus kernel module is not available	☐	☐
1.1.1.5	Ensure jffs2 kernel module is not available	☐	☐
1.1.1.6	Ensure squashfs kernel module is not available	☐	☐
1.1.1.7	Ensure udf kernel module is not available	☐	☐
1.1.1.8	Ensure usb-storage kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nodev option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure /dev/shm is a separate partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/log	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.4.2	Ensure ptrace_scope is restricted	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.6	Ensure no unconfined services exist	☐	☐
1.5.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.7.1	Ensure GNOME Display Manager is removed	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
1.7.10	Ensure XDMCP is not enabled	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.1.2	Ensure chrony is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure avahi daemon services are not in use	☐	☐
2.2.3	Ensure dhcp server services are not in use	☐	☐
2.2.4	Ensure dns server services are not in use	☐	☐
2.2.5	Ensure dnsmasq services are not in use	☐	☐
2.2.6	Ensure samba file server services are not in use	☐	☐
2.2.7	Ensure ftp server services are not in use	☐	☐
2.2.8	Ensure message access server services are not in use	☐	☐
2.2.9	Ensure network file system services are not in use	☐	☐
2.2.10	Ensure nis server services are not in use	☐	☐
2.2.11	Ensure print server services are not in use	☐	☐
2.2.12	Ensure rpcbind services are not in use	☐	☐
2.2.13	Ensure rsync services are not in use	☐	☐
2.2.14	Ensure snmp services are not in use	☐	☐
2.2.15	Ensure telnet server services are not in use	☐	☐
2.2.16	Ensure tftp server services are not in use	☐	☐
2.2.17	Ensure web proxy server services are not in use	☐	☐
2.2.18	Ensure web server services are not in use	☐	☐
2.2.19	Ensure xinetd services are not in use	☐	☐
2.2.20	Ensure X window server services are not in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.21	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.22	Ensure only approved services are listening on a network interface	☐	☐
2.3.1	Ensure ftp client is not installed	☐	☐
2.3.2	Ensure ldap client is not installed	☐	☐
2.3.3	Ensure nis client is not installed	☐	☐
2.3.4	Ensure telnet client is not installed	☐	☐
2.3.5	Ensure tftp client is not installed	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.1.2	Ensure wireless interfaces are disabled	☐	☐
3.1.3	Ensure bluetooth services are not in use	☐	☐
3.2.1	Ensure dccp kernel module is not available	☐	☐
3.2.2	Ensure tipc kernel module is not available	☐	☐
3.2.3	Ensure rds kernel module is not available	☐	☐
3.2.4	Ensure sctp kernel module is not available	☐	☐
3.3.1	Ensure ip forwarding is disabled	☐	☐
3.3.2	Ensure packet redirect sending is disabled	☐	☐
3.3.3	Ensure bogus icmp responses are ignored	☐	☐
3.3.4	Ensure broadcast icmp requests are ignored	☐	☐
3.3.5	Ensure icmp redirects are not accepted	☐	☐
3.3.6	Ensure secure icmp redirects are not accepted	☐	☐
3.3.7	Ensure reverse path filtering is enabled	☐	☐
3.3.8	Ensure source routed packets are not accepted	☐	☐
3.3.9	Ensure suspicious packets are logged	☐	☐
3.3.10	Ensure tcp syn cookies is enabled	☐	☐
3.3.11	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.12	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.15	Ensure sshd MACs are configured	☐	☐
4.2.16	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.22	Ensure sshd UsePAM is enabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.3	Ensure sudo log file exists	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.4.1.2	Ensure libpwquality is installed	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured	☐	☐
4.4.2.1.3	Ensure password unlock time is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.2.1.4	Ensure password failed attempts lockout includes root account	☐	☐
4.4.2.2.1	Ensure pam_pwquality module is enabled	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured	☐	☐
4.4.2.2.3	Ensure password length is configured	☐	☐
4.4.2.2.4	Ensure password complexity is configured	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured	☐	☐
4.4.2.2.6	Ensure password maximum sequential characters is configured	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled	☐	☐
4.4.2.3.1	Ensure pam_pwhistory module is enabled	☐	☐
4.4.2.3.2	Ensure password history remember is configured	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user	☐	☐
4.4.2.3.4	Ensure pam_pwhistory includes use_authtok	☐	☐
4.4.2.4.1	Ensure pam_unix does not include nullok	☐	☐
4.4.2.4.2	Ensure pam_unix does not include remember	☐	☐
4.4.2.4.3	Ensure pam_unix includes a strong password hashing algorithm	☐	☐
4.4.2.4.4	Ensure pam_unix includes use_authtok	☐	☐
4.5.1.1	Ensure strong password hashing algorithm is configured	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less	☐	☐
4.5.1.5	Ensure all users last password change date is in the past	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.3	Ensure logrotate is configured	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.2.1	Ensure audit log storage size is configured	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted	☐	☐
5.2.2.3	Ensure system is disabled when audit logs are full	☐	☐
5.2.2.4	Ensure system warns when audit logs are low on space	☐	☐
5.2.3.1	Ensure changes to system administration scope (sudoers) is collected	☐	☐
5.2.3.2	Ensure actions as another user are always logged	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.3.3	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.4	Ensure events that modify date and time information are collected	☐	☐
5.2.3.5	Ensure events that modify the system's network environment are collected	☐	☐
5.2.3.6	Ensure use of privileged commands are collected	☐	☐
5.2.3.7	Ensure unsuccessful file access attempts are collected	☐	☐
5.2.3.8	Ensure events that modify user/group information are collected	☐	☐
5.2.3.9	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.10	Ensure successful file system mounts are collected	☐	☐
5.2.3.11	Ensure session initiation information is collected	☐	☐
5.2.3.12	Ensure login and logout events are collected	☐	☐
5.2.3.13	Ensure file deletion events by users are collected	☐	☐
5.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected	☐	☐
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.3.21	Ensure the running and on disk configuration is the same	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure cramfs kernel module is not available	☐	☐
1.1.1.2	Ensure freevxfs kernel module is not available	☐	☐
1.1.1.3	Ensure hfs kernel module is not available	☐	☐
1.1.1.4	Ensure hfsplus kernel module is not available	☐	☐
1.1.1.5	Ensure jffs2 kernel module is not available	☐	☐
1.1.1.6	Ensure squashfs kernel module is not available	☐	☐
1.1.1.7	Ensure udf kernel module is not available	☐	☐
1.1.1.8	Ensure usb-storage kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nodev option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.4	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure /dev/shm is a separate partition	☐	☐
1.1.2.2.2	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.2.2.3	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.2.2.4	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /home	☐	☐
1.1.2.3.2	Ensure nodev option set on /home partition	☐	☐
1.1.2.3.3	Ensure nosuid option set on /home partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var	☐	☐
1.1.2.4.2	Ensure nodev option set on /var partition	☐	☐
1.1.2.4.3	Ensure nosuid option set on /var partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.5.2	Ensure nodev option set on /var/tmp partition	☐	☐
1.1.2.5.3	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.5.4	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/log	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.1.2.6.2	Ensure nodev option set on /var/log partition	☐	☐
1.1.2.6.3	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.6.4	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.7.1	Ensure separate partition exists for /var/log/audit	☐	☐
1.1.2.7.2	Ensure nodev option set on /var/log/audit partition	☐	☐
1.1.2.7.3	Ensure nosuid option set on /var/log/audit partition	☐	☐
1.1.2.7.4	Ensure noexec option set on /var/log/audit partition	☐	☐
1.2.1	Ensure GPG keys are configured	☐	☐
1.2.2	Ensure gpgcheck is globally activated	☐	☐
1.2.3	Ensure repo_gpgcheck is globally activated	☐	☐
1.2.4	Ensure package manager repositories are configured	☐	☐
1.2.5	Ensure updates, patches, and additional security software are installed	☐	☐
1.3.1	Ensure bootloader password is set	☐	☐
1.3.2	Ensure permissions on bootloader config are configured	☐	☐
1.3.3	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.4.2	Ensure ptrace_scope is restricted	☐	☐
1.5.1.1	Ensure SELinux is installed	☐	☐
1.5.1.2	Ensure SELinux is not disabled in bootloader configuration	☐	☐
1.5.1.3	Ensure SELinux policy is configured	☐	☐
1.5.1.4	Ensure the SELinux mode is not disabled	☐	☐
1.5.1.5	Ensure the SELinux mode is enforcing	☐	☐
1.5.1.6	Ensure no unconfined services exist	☐	☐
1.5.1.7	Ensure the MCS Translation Service (mcstrans) is not installed	☐	☐
1.5.1.8	Ensure SETroubleshoot is not installed	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
1.6.6	Ensure access to /etc/issue.net is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.7.1	Ensure GNOME Display Manager is removed	☐	☐
1.7.4	Ensure GDM screen locks when the user is idle	☐	☐
1.7.5	Ensure GDM screen locks cannot be overridden	☐	☐
1.7.6	Ensure GDM automatic mounting of removable media is disabled	☐	☐
1.7.7	Ensure GDM disabling automatic mounting of removable media is not overridden	☐	☐
1.7.8	Ensure GDM autorun-never is enabled	☐	☐
1.7.9	Ensure GDM autorun-never is not overridden	☐	☐
1.7.10	Ensure XDMCP is not enabled	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.1.2	Ensure chrony is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure avahi daemon services are not in use	☐	☐
2.2.3	Ensure dhcp server services are not in use	☐	☐
2.2.4	Ensure dns server services are not in use	☐	☐
2.2.5	Ensure dnsmasq services are not in use	☐	☐
2.2.6	Ensure samba file server services are not in use	☐	☐
2.2.7	Ensure ftp server services are not in use	☐	☐
2.2.8	Ensure message access server services are not in use	☐	☐
2.2.9	Ensure network file system services are not in use	☐	☐
2.2.10	Ensure nis server services are not in use	☐	☐
2.2.11	Ensure print server services are not in use	☐	☐
2.2.12	Ensure rpcbind services are not in use	☐	☐
2.2.13	Ensure rsync services are not in use	☐	☐
2.2.14	Ensure snmp services are not in use	☐	☐
2.2.15	Ensure telnet server services are not in use	☐	☐
2.2.16	Ensure tftp server services are not in use	☐	☐
2.2.17	Ensure web proxy server services are not in use	☐	☐
2.2.18	Ensure web server services are not in use	☐	☐
2.2.19	Ensure xinetd services are not in use	☐	☐
2.2.20	Ensure X window server services are not in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.21	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.22	Ensure only approved services are listening on a network interface	☐	☐
2.3.1	Ensure ftp client is not installed	☐	☐
2.3.2	Ensure ldap client is not installed	☐	☐
2.3.3	Ensure nis client is not installed	☐	☐
2.3.4	Ensure telnet client is not installed	☐	☐
2.3.5	Ensure tftp client is not installed	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.1.2	Ensure wireless interfaces are disabled	☐	☐
3.1.3	Ensure bluetooth services are not in use	☐	☐
3.2.1	Ensure dccp kernel module is not available	☐	☐
3.2.2	Ensure tipc kernel module is not available	☐	☐
3.2.3	Ensure rds kernel module is not available	☐	☐
3.2.4	Ensure sctp kernel module is not available	☐	☐
3.3.1	Ensure ip forwarding is disabled	☐	☐
3.3.2	Ensure packet redirect sending is disabled	☐	☐
3.3.3	Ensure bogus icmp responses are ignored	☐	☐
3.3.4	Ensure broadcast icmp requests are ignored	☐	☐
3.3.5	Ensure icmp redirects are not accepted	☐	☐
3.3.6	Ensure secure icmp redirects are not accepted	☐	☐
3.3.7	Ensure reverse path filtering is enabled	☐	☐
3.3.8	Ensure source routed packets are not accepted	☐	☐
3.3.9	Ensure suspicious packets are logged	☐	☐
3.3.10	Ensure tcp syn cookies is enabled	☐	☐
3.3.11	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure iptables is installed	☐	☐
3.4.1.2	Ensure a single firewall configuration utility is in use	☐	☐
3.4.2.1	Ensure firewalld is installed	☐	☐
3.4.2.2	Ensure firewalld service enabled and running	☐	☐
3.4.2.3	Ensure firewalld drops unnecessary services and ports	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.2.4	Ensure network interfaces are assigned to appropriate zone	☐	☐
3.4.3.1	Ensure nftables is installed	☐	☐
3.4.3.2	Ensure iptables are flushed with nftables	☐	☐
3.4.3.3	Ensure an nftables table exists	☐	☐
3.4.3.4	Ensure nftables base chains exist	☐	☐
3.4.3.5	Ensure nftables loopback traffic is configured	☐	☐
3.4.3.6	Ensure nftables outbound and established connections are configured	☐	☐
3.4.3.7	Ensure nftables default deny firewall policy	☐	☐
3.4.3.8	Ensure nftables service is enabled and active	☐	☐
3.4.3.9	Ensure nftables rules are permanent	☐	☐
3.4.4.1.1	Ensure iptables packages are installed	☐	☐
3.4.4.2.1	Ensure iptables loopback traffic is configured	☐	☐
3.4.4.2.2	Ensure iptables outbound and established connections are configured	☐	☐
3.4.4.2.3	Ensure iptables rules exist for all open ports	☐	☐
3.4.4.2.4	Ensure iptables default deny firewall policy	☐	☐
3.4.4.2.5	Ensure iptables rules are saved	☐	☐
3.4.4.2.6	Ensure iptables service is enabled and active	☐	☐
3.4.4.3.1	Ensure ip6tables loopback traffic is configured	☐	☐
3.4.4.3.2	Ensure ip6tables outbound and established connections are configured	☐	☐
3.4.4.3.3	Ensure ip6tables firewall rules exist for all open ports	☐	☐
3.4.4.3.4	Ensure ip6tables default deny firewall policy	☐	☐
3.4.4.3.5	Ensure ip6tables rules are saved	☐	☐
3.4.4.3.6	Ensure ip6tables is enabled and active	☐	☐
4.1.1.2	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.3	Ensure permissions on /etc/cron.hourly are configured	☐	☐
4.1.1.4	Ensure permissions on /etc/cron.daily are configured	☐	☐
4.1.1.5	Ensure permissions on /etc/cron.weekly are configured	☐	☐
4.1.1.6	Ensure permissions on /etc/cron.monthly are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.7	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.8	Ensure crontab is restricted to authorized users	☐	☐
4.1.2.1	Ensure at is restricted to authorized users	☐	☐
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured	☐	☐
4.2.4	Ensure sshd access is configured	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.11	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.12	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.14	Ensure sshd LogLevel is configured	☐	☐
4.2.15	Ensure sshd MACs are configured	☐	☐
4.2.16	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.18	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.20	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.22	Ensure sshd UsePAM is enabled	☐	☐
4.3.1	Ensure sudo is installed	☐	☐
4.3.2	Ensure sudo commands use pty	☐	☐
4.3.3	Ensure sudo log file exists	☐	☐
4.3.4	Ensure users must provide password for escalation	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly	☐	☐
4.3.7	Ensure access to the su command is restricted	☐	☐
4.4.1.2	Ensure libpwquality is installed	☐	☐
4.4.2.1.2	Ensure password failed attempts lockout is configured	☐	☐
4.4.2.1.3	Ensure password unlock time is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.2.1.4	Ensure password failed attempts lockout includes root account	☐	☐
4.4.2.2.1	Ensure pam_pwquality module is enabled	☐	☐
4.4.2.2.2	Ensure password number of changed characters is configured	☐	☐
4.4.2.2.3	Ensure password length is configured	☐	☐
4.4.2.2.4	Ensure password complexity is configured	☐	☐
4.4.2.2.5	Ensure password same consecutive characters is configured	☐	☐
4.4.2.2.6	Ensure password maximum sequential characters is configured	☐	☐
4.4.2.2.7	Ensure password dictionary check is enabled	☐	☐
4.4.2.3.1	Ensure pam_pwhistory module is enabled	☐	☐
4.4.2.3.2	Ensure password history remember is configured	☐	☐
4.4.2.3.3	Ensure password history is enforced for the root user	☐	☐
4.4.2.3.4	Ensure pam_pwhistory includes use_authtok	☐	☐
4.4.2.4.1	Ensure pam_unix does not include nullok	☐	☐
4.4.2.4.2	Ensure pam_unix does not include remember	☐	☐
4.4.2.4.3	Ensure pam_unix includes a strong password hashing algorithm	☐	☐
4.4.2.4.4	Ensure pam_unix includes use_authtok	☐	☐
4.5.1.1	Ensure strong password hashing algorithm is configured	☐	☐
4.5.1.2	Ensure password expiration is 365 days or less	☐	☐
4.5.1.3	Ensure password expiration warning days is 7 or more	☐	☐
4.5.1.4	Ensure inactive password lock is 30 days or less	☐	☐
4.5.1.5	Ensure all users last password change date is in the past	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.2.4	Ensure root password is set	☐	☐
4.5.3.2	Ensure default user shell timeout is configured	☐	☐
4.5.3.3	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure rsyslog is installed	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.2	Ensure rsyslog service is enabled	☐	☐
5.1.1.3	Ensure journald is configured to send logs to rsyslog	☐	☐
5.1.1.4	Ensure rsyslog default file permissions are configured	☐	☐
5.1.1.5	Ensure logging is configured	☐	☐
5.1.1.6	Ensure rsyslog is configured to send logs to a remote log host	☐	☐
5.1.1.7	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2.1.1	Ensure systemd-journal-remote is installed	☐	☐
5.1.2.1.2	Ensure systemd-journal-remote is configured	☐	☐
5.1.2.1.3	Ensure systemd-journal-remote is enabled	☐	☐
5.1.2.1.4	Ensure journald is not configured to receive logs from a remote client	☐	☐
5.1.2.2	Ensure journald service is enabled	☐	☐
5.1.2.3	Ensure journald is configured to compress large log files	☐	☐
5.1.2.4	Ensure journald is configured to write logfiles to persistent disk	☐	☐
5.1.2.5	Ensure journald is not configured to send logs to rsyslog	☐	☐
5.1.2.6	Ensure journald log rotation is configured per site policy	☐	☐
5.1.3	Ensure logrotate is configured	☐	☐
5.1.4	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure audit is installed	☐	☐
5.2.1.2	Ensure auditing for processes that start prior to auditd is enabled	☐	☐
5.2.1.3	Ensure audit_backlog_limit is sufficient	☐	☐
5.2.1.4	Ensure auditd service is enabled	☐	☐
5.2.2.1	Ensure audit log storage size is configured	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted	☐	☐
5.2.2.3	Ensure system is disabled when audit logs are full	☐	☐
5.2.2.4	Ensure system warns when audit logs are low on space	☐	☐
5.2.3.1	Ensure changes to system administration scope (sudoers) is collected	☐	☐
5.2.3.2	Ensure actions as another user are always logged	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.3.3	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.4	Ensure events that modify date and time information are collected	☐	☐
5.2.3.5	Ensure events that modify the system's network environment are collected	☐	☐
5.2.3.6	Ensure use of privileged commands are collected	☐	☐
5.2.3.7	Ensure unsuccessful file access attempts are collected	☐	☐
5.2.3.8	Ensure events that modify user/group information are collected	☐	☐
5.2.3.9	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.10	Ensure successful file system mounts are collected	☐	☐
5.2.3.11	Ensure session initiation information is collected	☐	☐
5.2.3.12	Ensure login and logout events are collected	☐	☐
5.2.3.13	Ensure file deletion events by users are collected	☐	☐
5.2.3.14	Ensure events that modify the system's Mandatory Access Controls are collected	☐	☐
5.2.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded	☐	☐
5.2.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded	☐	☐
5.2.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded	☐	☐
5.2.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
5.2.3.19	Ensure kernel module loading unloading and modification is collected	☐	☐
5.2.3.20	Ensure the audit configuration is immutable	☐	☐
5.2.3.21	Ensure the running and on disk configuration is the same	☐	☐
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive	☐	☐
5.2.4.3	Ensure only authorized users own audit log files	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.5	Ensure audit configuration files are 640 or more restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group root	☐	☐
5.2.4.8	Ensure audit tools are 755 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group root	☐	☐
5.3.1	Ensure AIDE is installed	☐	☐
5.3.2	Ensure filesystem integrity is regularly checked	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/group- are configured	☐	☐
6.1.5	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.1.9	Ensure permissions on /etc/shells are configured	☐	☐
6.1.10	Ensure permissions on /etc/security/opasswd are configured	☐	☐
6.1.11	Ensure world writable files and directories are secured	☐	☐
6.1.12	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.13	Ensure SUID and SGID files are reviewed	☐	☐
6.1.14	Audit system file permissions	☐	☐
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty	☐	☐
6.2.10	Ensure local interactive user home directories are configured	☐	☐
6.2.11	Ensure local interactive user dot files access is configured	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.4.3	Ensure core dump backtraces are disabled	☐	☐
1.4.4	Ensure core dump storage is disabled	☐	☐
1.6.1	Ensure message of the day is configured properly	☐	☐
1.6.2	Ensure local login warning banner is configured properly	☐	☐
1.6.3	Ensure remote login warning banner is configured properly	☐	☐
1.7.2	Ensure GDM login banner is configured	☐	☐
1.7.3	Ensure GDM disable-user-list option is enabled	☐	☐
2.1.3	Ensure chrony is not run as the root user	☐	☐
4.1.1.1	Ensure cron daemon is enabled and active	☐	☐
4.2.5	Ensure sshd Banner is configured	☐	☐
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	☐	☐
4.2.9	Ensure sshd GSSAPIAuthentication is disabled	☐	☐
4.2.10	Ensure sshd HostbasedAuthentication is disabled	☐	☐
4.2.13	Ensure sshd LoginGraceTime is configured	☐	☐
4.2.17	Ensure sshd MaxSessions is configured	☐	☐
4.2.21	Ensure sshd PermitUserEnvironment is disabled	☐	☐
4.4.1.1	Ensure latest version of pam is installed	☐	☐
4.4.2.1.1	Ensure pam_faillock module is enabled	☐	☐
4.5.3.1	Ensure nologin is not listed in /etc/shells	☐	☐
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group	☐	☐
6.2.4	Ensure no duplicate UIDs exist	☐	☐
6.2.5	Ensure no duplicate GIDs exist	☐	☐
6.2.6	Ensure no duplicate user names exist	☐	☐
6.2.7	Ensure no duplicate group names exist	☐	☐
6.2.8	Ensure root path integrity	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.9	Ensure root is the only UID 0 account	☐	☐

Appendix: Change History

Date	Version	Changes for this version
ADDED ITEMS:		
12/22/2023	4.0.0	ADDED SECTION: 1.1 - Filesystem
12/22/2023	4.0.0	ADDED SECTION: 1.1.1 - Configure Filesystem Kernel Modules
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.1 - Ensure cramfs kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.2 - Ensure freevxfs kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.3 - Ensure hfs kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.4 - Ensure hfsplus kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.5 - Ensure jffs2 kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.6 - Ensure squashfs kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.7 - Ensure udf kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.1.8 - Ensure usb-storage kernel module is not available
12/22/2023	4.0.0	ADDED SECTION: 1.1.2 - Configure Filesystem Partitions
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.1 - Configure /tmp
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.1.1 - Ensure /tmp is a separate partition
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.2 - Configure /dev/shm
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.2.1 - Ensure /dev/shm is a separate partition

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.3 - Configure /home
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.3.2 - Ensure nodev option set on /home partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.3.3 - Ensure nosuid option set on /home partition
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.4 - Configure /var
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.4.2 - Ensure nodev option set on /var partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.4.3 - Ensure nosuid option set on /var partition
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.5 - Configure /var/tmp
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.5.2 - Ensure nodev option set on /var/tmp partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.5.3 - Ensure nosuid option set on /var/tmp partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.5.4 - Ensure noexec option set on /var/tmp partition
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.6 - Configure /var/log
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.6.2 - Ensure nodev option set on /var/log partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.6.3 - Ensure nosuid option set on /var/log partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.6.4 - Ensure noexec option set on /var/log partition
12/22/2023	4.0.0	ADDED SECTION: 1.1.2.7 - Configure /var/log/audit
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.7.2 - Ensure nodev option set on /var/log/audit partition
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.7.3 - Ensure nosuid option set on /var/log/audit partition

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.1.2.7.4 - Ensure noexec option set on /var/log/audit partition
12/22/2023	4.0.0	ADDED SECTION: 1.2 - Configure Software and Patch Management
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.2.3 - Ensure repo_gpgcheck is globally activated
12/22/2023	4.0.0	ADDED SECTION: 1.3 - Configure Secure Boot Settings
12/22/2023	4.0.0	ADDED SECTION: 1.4 - Configure Additional Process Hardening
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.4.2 - Ensure ptrace_scope is restricted
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.4.3 - Ensure core dump backtraces are disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.4.4 - Ensure core dump storage is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.5.1.4 - Ensure the SELinux mode is not disabled
12/22/2023	4.0.0	ADDED SECTION: 1.6 - Configure Command Line Warning Banners
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.6.4 - Ensure access to /etc/motd is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.6.5 - Ensure access to /etc/issue is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.6.6 - Ensure access to /etc/issue.net is configured
12/22/2023	4.0.0	ADDED SECTION: 1.7 - Configure GNOME Display Manager
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.3 - Ensure GDM disable-user-list option is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.4 - Ensure GDM screen locks when the user is idle

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.5 - Ensure GDM screen locks cannot be overridden
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.6 - Ensure GDM automatic mounting of removable media is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.7 - Ensure GDM disabling automatic mounting of removable media is not overridden
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.8 - Ensure GDM autorun-never is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.9 - Ensure GDM autorun-never is not overridden
12/22/2023	4.0.0	ADDED RECOMMENDATION: 1.7.10 - Ensure XDMCP is not enabled
12/22/2023	4.0.0	ADDED SECTION: 2.1 - Configure Time Synchronization
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.1.3 - Ensure chrony is not run as the root user
12/22/2023	4.0.0	ADDED SECTION: 2.2 - Configure Special Purpose Services
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.1 - Ensure autofs services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.2 - Ensure avahi daemon services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.3 - Ensure dhcp server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.4 - Ensure dns server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.5 - Ensure dnsmasq services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.6 - Ensure samba file server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.7 - Ensure ftp server services are not in use

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.8 - Ensure message access server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.9 - Ensure network file system services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.10 - Ensure nis server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.11 - Ensure print server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.12 - Ensure rpcbind services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.13 - Ensure rsync services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.14 - Ensure snmp services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.15 - Ensure telnet server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.16 - Ensure tftp server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.17 - Ensure web proxy server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.18 - Ensure web server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.19 - Ensure xinetd services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.20 - Ensure X window server services are not in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.21 - Ensure mail transfer agents are configured for local-only mode
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.2.22 - Ensure only approved services are listening on a network interface

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED SECTION: 2.3 - Configure Service Clients
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.3.1 - Ensure ftp client is not installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.3.2 - Ensure ldap client is not installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.3.3 - Ensure nis client is not installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 2.3.5 - Ensure tftp client is not installed
12/22/2023	4.0.0	ADDED SECTION: 3 - Network
12/22/2023	4.0.0	ADDED SECTION: 3.1 - Configure Network Devices
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.1.1 - Ensure IPv6 status is identified
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.1.3 - Ensure bluetooth services are not in use
12/22/2023	4.0.0	ADDED SECTION: 3.2 - Configure Network Kernel Modules
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.2.1 - Ensure dccp kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.2.2 - Ensure tipc kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.2.3 - Ensure rds kernel module is not available
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.2.4 - Ensure sctp kernel module is not available
12/22/2023	4.0.0	ADDED SECTION: 3.3 - Configure Network Kernel Parameters
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.1 - Ensure ip forwarding is disabled

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.3 - Ensure bogus icmp responses are ignored
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.4 - Ensure broadcast icmp requests are ignored
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.5 - Ensure icmp redirects are not accepted
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.6 - Ensure secure icmp redirects are not accepted
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.7 - Ensure reverse path filtering is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.10 - Ensure tcp syn cookies is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.3.11 - Ensure ipv6 router advertisements are not accepted
12/22/2023	4.0.0	ADDED SECTION: 3.4 - Configure Host Based Firewall
12/22/2023	4.0.0	ADDED SECTION: 3.4.1 - Configure firewall utility
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.4.1.1 - Ensure iptables is installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.4.1.2 - Ensure a single firewall configuration utility is in use
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.4.3.8 - Ensure nftables service is enabled and active
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.4.4.2.6 - Ensure iptables service is enabled and active
12/22/2023	4.0.0	ADDED SECTION: 3.4.4.3 - Configure ip6tables
12/22/2023	4.0.0	ADDED RECOMMENDATION: 3.4.4.3.6 - Ensure ip6tables is enabled and active
12/22/2023	4.0.0	ADDED SECTION: 4.1 - Configure job schedulers
12/22/2023	4.0.0	ADDED SECTION: 4.1.1 - Configure cron

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.1.1.1 - Ensure cron daemon is enabled and active
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.1.1.8 - Ensure crontab is restricted to authorized users
12/22/2023	4.0.0	ADDED SECTION: 4.1.2 - Configure at
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.4 - Ensure sshd access is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.5 - Ensure sshd Banner is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.6 - Ensure sshd Ciphers are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.7 - Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.8 - Ensure sshd DisableForwarding is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.9 - Ensure sshd GSSAPIAuthentication is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.10 - Ensure sshd HostbasedAuthentication is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.11 - Ensure sshd IgnoreRhosts is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.12 - Ensure sshd KexAlgorithms is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.13 - Ensure sshd LoginGraceTime is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.14 - Ensure sshd LogLevel is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.15 - Ensure sshd MACs are configured

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.16 - Ensure sshd MaxAuthTries is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.17 - Ensure sshd MaxSessions is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.18 - Ensure sshd MaxStartups is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.19 - Ensure sshd PermitEmptyPasswords is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.20 - Ensure sshd PermitRootLogin is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.21 - Ensure sshd PermitUserEnvironment is disabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.2.22 - Ensure sshd UsePAM is enabled
12/22/2023	4.0.0	ADDED SECTION: 4.3 - Configure privilege escalation
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.3.4 - Ensure users must provide password for escalation
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.3.5 - Ensure re-authentication for privilege escalation is not disabled globally
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.3.6 - Ensure sudo authentication timeout is configured correctly
12/22/2023	4.0.0	ADDED SECTION: 4.4 - Configure Pluggable Authentication Modules
12/22/2023	4.0.0	ADDED SECTION: 4.4.1 - Configure PAM software packages
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.1.1 - Ensure latest version of pam is installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.1.2 - Ensure libpwquality is installed
12/22/2023	4.0.0	ADDED SECTION: 4.4.2 - Configure pluggable module arguments

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED SECTION: 4.4.2.1 - Configure pam_faillock module
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.1.1 - Ensure pam_faillock module is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.1.2 - Ensure password failed attempts lockout is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.1.3 - Ensure password unlock time is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.1.4 - Ensure password failed attempts lockout includes root account
12/22/2023	4.0.0	ADDED SECTION: 4.4.2.2 - Configure pam_pwquality module
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.1 - Ensure pam_pwquality module is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.2 - Ensure password number of changed characters is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.3 - Ensure password length is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.4 - Ensure password complexity is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.5 - Ensure password same consecutive characters is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.6 - Ensure password maximum sequential characters is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.2.7 - Ensure password dictionary check is enabled
12/22/2023	4.0.0	ADDED SECTION: 4.4.2.3 - Configure pam_pwhistory module
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.3.1 - Ensure pam_pwhistory module is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.3.2 - Ensure password history remember is configured

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.3.3 - Ensure password history is enforced for the root user
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.3.4 - Ensure pam_pwhistory includes use_authtok
12/22/2023	4.0.0	ADDED SECTION: 4.4.2.4 - Configure pam_unix module
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.4.1 - Ensure pam_unix does not include nullok
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.4.2 - Ensure pam_unix does not include remember
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.4.3 - Ensure pam_unix includes a strong password hashing algorithm
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.4.2.4.4 - Ensure pam_unix includes use_authtok
12/22/2023	4.0.0	ADDED SECTION: 4.5.1 - Configure shadow password suite parameters
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.5.1.1 - Ensure strong password hashing algorithm is configured
12/22/2023	4.0.0	ADDED SECTION: 4.5.2 - Configure root and system accounts and environment
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.5.2.2 - Ensure root user umask is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.5.2.4 - Ensure root password is set
12/22/2023	4.0.0	ADDED SECTION: 4.5.3 - Configure user default environment
12/22/2023	4.0.0	ADDED RECOMMENDATION: 4.5.3.1 - Ensure nologin is not listed in /etc/shells
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.4 - Ensure all logfiles have appropriate access configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.1.2 - Ensure rsyslog service is enabled

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.1.4 - Ensure rsyslog default file permissions are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.1.7 - Ensure rsyslog is not configured to receive logs from a remote client
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.2 - Ensure journald service is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.5 - Ensure journald is not configured to send logs to rsyslog
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.6 - Ensure journald log rotation is configured per site policy
12/22/2023	4.0.0	ADDED SECTION: 5.1.2.1 - Ensure journald is configured to send logs to a remote log host
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.1.1 - Ensure systemd-journal-remote is installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.1.2 - Ensure systemd-journal-remote is configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.1.3 - Ensure systemd-journal-remote is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.1.2.1.4 - Ensure journald is not configured to receive logs from a remote client
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.1.1 - Ensure audit is installed
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.1.4 - Ensure auditd service is enabled
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.2.4 - Ensure system warns when audit logs are low on space
12/22/2023	4.0.0	ADDED SECTION: 5.2.3 - Configure auditd rules
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.2 - Ensure actions as another user are always logged

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.3 - Ensure events that modify the sudo log file are collected
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.6 - Ensure use of privileged commands are collected
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.7 - Ensure unsuccessful file access attempts are collected
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.15 - Ensure successful and unsuccessful attempts to use the chcon command are recorded
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.16 - Ensure successful and unsuccessful attempts to use the setfacl command are recorded
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.17 - Ensure successful and unsuccessful attempts to use the chacl command are recorded
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.18 - Ensure successful and unsuccessful attempts to use the usermod command are recorded
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.19 - Ensure kernel module loading unloading and modification is collected
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.3.21 - Ensure the running and on disk configuration is the same
12/22/2023	4.0.0	ADDED SECTION: 5.2.4 - Configure auditd file access
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.1 - Ensure the audit log directory is 0750 or more restrictive
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.2 - Ensure audit log files are mode 0640 or less permissive
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.3 - Ensure only authorized users own audit log files
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.4 - Ensure only authorized groups are assigned ownership of audit log files

Date	Version	Changes for this version
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.5 - Ensure audit configuration files are 640 or more restrictive
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.6 - Ensure audit configuration files are owned by root
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.7 - Ensure audit configuration files belong to group root
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.8 - Ensure audit tools are 755 or more restrictive
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.9 - Ensure audit tools are owned by root
12/22/2023	4.0.0	ADDED RECOMMENDATION: 5.2.4.10 - Ensure audit tools belong to group root
12/22/2023	4.0.0	ADDED SECTION: 5.3 - Configure Integrity Checking
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.1.9 - Ensure permissions on /etc/shells are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.1.10 - Ensure permissions on /etc/security/opasswd are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.1.11 - Ensure world writable files and directories are secured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.1.12 - Ensure no unowned or ungrouped files or directories exist
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.1.13 - Ensure SUID and SGID files are reviewed
12/22/2023	4.0.0	ADDED SECTION: 6.2 - Local User and Group Settings
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.2.8 - Ensure root path integrity
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.2.10 - Ensure local interactive user home directories are configured
12/22/2023	4.0.0	ADDED RECOMMENDATION: 6.2.11 - Ensure local interactive user dot files access is configured

Date	Version	Changes for this version
DROPPED ITEMS:		
12/22/2023	4.0.0	DROPPED SECTION: 1.1 - Filesystem Configuration
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.2 - Ensure /tmp is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.6 - Ensure /dev/shm is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.12 - Ensure /var/tmp partition includes the noexec option
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.13 - Ensure /var/tmp partition includes the nodev option
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.14 - Ensure /var/tmp partition includes the nosuid option
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.18 - Ensure /home partition includes the nodev option
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.19 - Ensure removable media partitions include noexec option
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.20 - Ensure nodev option set on removable media partitions
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.21 - Ensure nosuid option set on removable media partitions
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.22 - Ensure sticky bit is set on all world-writable directories
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.23 - Disable Automounting
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.24 - Disable USB Storage
12/22/2023	4.0.0	DROPPED SECTION: 1.1.1 - Disable unused filesystems
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.1.1 - Ensure mounting of cramfs filesystems is disabled

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.1.2 - Ensure mounting of squashfs filesystems is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.1.1.3 - Ensure mounting of udf filesystems is disabled
12/22/2023	4.0.0	DROPPED SECTION: 1.2 - Configure Software Updates
12/22/2023	4.0.0	DROPPED SECTION: 1.3 - Filesystem Integrity Checking
12/22/2023	4.0.0	DROPPED SECTION: 1.4 - Secure Boot Settings
12/22/2023	4.0.0	DROPPED SECTION: 1.5 - Additional Process Hardening
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.5.1 - Ensure core dumps are restricted
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.5.2 - Ensure XD/NX support is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.5.4 - Ensure prelink is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.6.1.4 - Ensure the SELinux mode is enforcing or permissive
12/22/2023	4.0.0	DROPPED SECTION: 1.7 - Command Line Warning Banners
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.7.4 - Ensure permissions on /etc/motd are configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.7.5 - Ensure permissions on /etc/issue are configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.7.6 - Ensure permissions on /etc/issue.net are configured
12/22/2023	4.0.0	DROPPED SECTION: 1.8 - GNOME Display Manager
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.8.3 - Ensure last logged in user display is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 1.8.4 - Ensure XDCMP is not enabled

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.4 - Ensure nonessential services are removed or masked
12/22/2023	4.0.0	DROPPED SECTION: 2.1 - inetd Services
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.1.1 - Ensure xinetd is not installed
12/22/2023	4.0.0	DROPPED SECTION: 2.2 - Special Purpose Services
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.2 - Ensure X11 Server components are not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.3 - Ensure Avahi Server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.4 - Ensure CUPS is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.5 - Ensure DHCP Server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.6 - Ensure LDAP server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.7 - Ensure DNS Server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.8 - Ensure FTP Server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.9 - Ensure HTTP server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.10 - Ensure IMAP and POP3 server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.11 - Ensure Samba is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.12 - Ensure HTTP Proxy Server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.13 - Ensure net-snmp is not installed

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.14 - Ensure NIS server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.15 - Ensure telnet-server is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.16 - Ensure mail transfer agent is configured for local-only mode
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.17 - Ensure nfs-utils is not installed or the nfs-server service is masked
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.18 - Ensure rpcbind is not installed or the rpcbind services are masked
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.19 - Ensure rsync is not installed or the rsyncd service is masked
12/22/2023	4.0.0	DROPPED SECTION: 2.2.1 - Time Synchronization
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.2.1.3 - Ensure ntp is configured
12/22/2023	4.0.0	DROPPED SECTION: 2.3 - Service Clients
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.3.1 - Ensure NIS Client is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.3.2 - Ensure rsh client is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.3.3 - Ensure talk client is not installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 2.3.5 - Ensure LDAP client is not installed
12/22/2023	4.0.0	DROPPED SECTION: 3 - Network Configuration
12/22/2023	4.0.0	DROPPED SECTION: 3.1 - Disable unused network protocols and devices
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.1.1 - Disable IPv6
12/22/2023	4.0.0	DROPPED SECTION: 3.2 - Network Parameters (Host Only)

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.2.1 - Ensure IP forwarding is disabled
12/22/2023	4.0.0	DROPPED SECTION: 3.3 - Network Parameters (Host and Router)
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.2 - Ensure ICMP redirects are not accepted
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.3 - Ensure secure ICMP redirects are not accepted
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.5 - Ensure broadcast ICMP requests are ignored
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.6 - Ensure bogus ICMP responses are ignored
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.7 - Ensure Reverse Path Filtering is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.8 - Ensure TCP SYN Cookies is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.3.9 - Ensure IPv6 router advertisements are not accepted
12/22/2023	4.0.0	DROPPED SECTION: 3.4 - Uncommon Network Protocols
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.4.1 - Ensure DCCP is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.4.2 - Ensure SCTP is disabled
12/22/2023	4.0.0	DROPPED SECTION: 3.5 - Firewall Configuration
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.1.2 - Ensure iptables-services not installed with firewalld
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.1.3 - Ensure nftables either not installed or masked with firewalld
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.1.5 - Ensure firewalld default zone is set

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.2.2 - Ensure firewalld is either not installed or masked with nftables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.2.3 - Ensure iptables-services not installed with nftables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.2.10 - Ensure nftables service is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.3.1.2 - Ensure nftables is not installed with iptables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.3.1.3 - Ensure firewalld is either not installed or masked with iptables
12/22/2023	4.0.0	DROPPED SECTION: 3.5.3.2 - Configure IPv4 iptables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.3.2.6 - Ensure iptables is enabled and running
12/22/2023	4.0.0	DROPPED SECTION: 3.5.3.3 - Configure IPv6 ip6tables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 3.5.3.3.6 - Ensure ip6tables is enabled and running
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.10 - Ensure unsuccessful unauthorized file access attempts are collected
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.11 - Ensure use of privileged commands is collected
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.15 - Ensure system administrator command executions (sudo) are collected
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.16 - Ensure kernel module loading and unloading is collected
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.1.1 - Ensure auditd is installed
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.1.1.2 - Ensure auditd service is enabled and running
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.2.3 - Ensure permissions on all logfiles are configured

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.2.1.2 - Ensure rsyslog Service is enabled and running
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.2.1.3 - Ensure rsyslog default file permissions configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 4.2.1.6 - Ensure remote rsyslog messages are only accepted on designated log hosts.
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.6 - Ensure root login is restricted to system console
12/22/2023	4.0.0	DROPPED SECTION: 5.1 - Configure time-based job schedulers
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.1.1 - Ensure cron daemon is enabled and running
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.1.8 - Ensure cron is restricted to authorized users
12/22/2023	4.0.0	DROPPED SECTION: 5.2 - Configure sudo
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.4 - Ensure SSH access is limited
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.5 - Ensure SSH LogLevel is appropriate
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.6 - Ensure SSH X11 forwarding is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.7 - Ensure SSH MaxAuthTries is set to 4 or less
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.8 - Ensure SSH IgnoreRhosts is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.9 - Ensure SSH HostbasedAuthentication is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.10 - Ensure SSH root login is disabled

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.11 - Ensure SSH PermitEmptyPasswords is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.12 - Ensure SSH PermitUserEnvironment is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.13 - Ensure only strong Ciphers are used
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.14 - Ensure only strong MAC algorithms are used
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.15 - Ensure only strong Key Exchange algorithms are used
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.16 - Ensure SSH Idle Timeout Interval is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.17 - Ensure SSH LoginGraceTime is set to one minute or less
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.18 - Ensure SSH warning banner is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.19 - Ensure SSH PAM is enabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.20 - Ensure SSH AllowTcpForwarding is disabled
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.21 - Ensure SSH MaxStartups is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.3.22 - Ensure SSH MaxSessions is limited
12/22/2023	4.0.0	DROPPED SECTION: 5.4 - Configure PAM
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.4.1 - Ensure password creation requirements are configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.4.2 - Ensure lockout for failed password attempts is configured

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.4.3 - Ensure password hashing algorithm is SHA-512
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.4.4 - Ensure password reuse is limited
12/22/2023	4.0.0	DROPPED SECTION: 5.5.1 - Set Shadow Password Suite Parameters
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 5.5.1.2 - Ensure minimum days between password changes is configured
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.1.10 - Ensure no world writable files exist
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.1.11 - Ensure no unowned files or directories exist
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.1.12 - Ensure no ungrouped files or directories exist
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.1.13 - Audit SUID executables
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.1.14 - Audit SGID executables
12/22/2023	4.0.0	DROPPED SECTION: 6.2 - User and Group Settings
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.4 - Ensure shadow group is empty
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.10 - Ensure root PATH Integrity
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.11 - Ensure all users' home directories exist
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.12 - Ensure users own their home directories
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.13 - Ensure users' home directories permissions are 750 or more restrictive

Date	Version	Changes for this version
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.14 - Ensure users' dot files are not group or world writable
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.15 - Ensure no users have .forward files
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.16 - Ensure no users have .netrc files
12/22/2023	4.0.0	DROPPED RECOMMENDATION: 6.2.17 - Ensure no users have .rhosts files
MOVED ITEMS:		
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition moved from 1.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition moved from 1.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition moved from 1.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition moved from 1.1.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition moved from 1.1.9 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition moved from 1.1.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home moved from 1.1.17 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var moved from 1.1.10 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp moved from 1.1.11 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log moved from 1.1.15 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit moved from 1.1.16 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.2.2 - Ensure gpgcheck is globally activated moved from 1.2.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.2.4 - Ensure package manager repositories are configured moved from 1.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.2.5 - Ensure updates, patches, and additional security software are installed moved from 1.9 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.3.1 - Ensure bootloader password is set moved from 1.4.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.3.2 - Ensure permissions on bootloader config are configured moved from 1.4.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.3.3 - Ensure authentication required for single user mode moved from 1.4.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.4.1 - Ensure address space layout randomization (ASLR) is enabled moved from 1.5.3 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 1.5 - Mandatory Access Control moved from 1.6 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 1.5.1 - Configure SELinux moved from 1.6.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.1 - Ensure SELinux is installed moved from 1.6.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.2 - Ensure SELinux is not disabled in bootloader configuration moved from 1.6.1.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.3 - Ensure SELinux policy is configured moved from 1.6.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.5 - Ensure the SELinux mode is enforcing moved from 1.6.1.5 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.6 - Ensure no unconfined services exist moved from 1.6.1.6 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.7 - Ensure the MCS Translation Service (mcstrans) is not installed moved from 1.6.1.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.5.1.8 - Ensure SETroubleshoot is not installed moved from 1.6.1.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.6.1 - Ensure message of the day is configured properly moved from 1.7.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.6.2 - Ensure local login warning banner is configured properly moved from 1.7.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.6.3 - Ensure remote login warning banner is configured properly moved from 1.7.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.7.1 - Ensure GNOME Display Manager is removed moved from 1.8.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 1.7.2 - Ensure GDM login banner is configured moved from 1.8.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 2.1.1 - Ensure time synchronization is in use moved from 2.2.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 2.1.2 - Ensure chrony is configured moved from 2.2.1.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled moved from 3.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted moved from 3.3.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged moved from 3.3.4 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 3.4.2 - Configure firewalld moved from 3.5.1 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.2.1 - Ensure firewalld is installed moved from 3.5.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.2.2 - Ensure firewalld service enabled and running moved from 3.5.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.2.3 - Ensure firewalld drops unnecessary services and ports moved from 3.5.1.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.2.4 - Ensure network interfaces are assigned to appropriate zone moved from 3.5.1.6 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 3.4.3 - Configure nftables moved from 3.5.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.1 - Ensure nftables is installed moved from 3.5.2.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.2 - Ensure iptables are flushed with nftables moved from 3.5.2.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.3 - Ensure an nftables table exists moved from 3.5.2.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.4 - Ensure nftables base chains exist moved from 3.5.2.6 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.5 - Ensure nftables loopback traffic is configured moved from 3.5.2.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.6 - Ensure nftables outbound and established connections are configured moved from 3.5.2.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.7 - Ensure nftables default deny firewall policy moved from 3.5.2.9 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.3.9 - Ensure nftables rules are permanent moved from 3.5.2.11 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 3.4.4 - Configure iptables moved from 3.5.3 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED SECTION: 3.4.4.1 - Configure iptables software moved from 3.5.3.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.1.1 - Ensure iptables packages are installed moved from 3.5.3.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 3.4.4.2 - Configure iptables moved from 3.5.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.2.1 - Ensure iptables loopback traffic is configured moved from 3.5.3.2.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.2.2 - Ensure iptables outbound and established connections are configured moved from 3.5.3.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.2.3 - Ensure iptables rules exist for all open ports moved from 3.5.3.2.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.2.4 - Ensure iptables default deny firewall policy moved from 3.5.3.2.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.2.5 - Ensure iptables rules are saved moved from 3.5.3.2.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.3.1 - Ensure ip6tables loopback traffic is configured moved from 3.5.3.3.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.3.2 - Ensure ip6tables outbound and established connections are configured moved from 3.5.3.3.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.3.3 - Ensure ip6tables firewall rules exist for all open ports moved from 3.5.3.3.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.3.4 - Ensure ip6tables default deny firewall policy moved from 3.5.3.3.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 3.4.4.3.5 - Ensure ip6tables rules are saved moved from 3.5.3.3.5 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 4 - Access, Authentication and Authorization moved from 5 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.2 - Ensure permissions on /etc/crontab are configured moved from 5.1.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.3 - Ensure permissions on /etc/cron.hourly are configured moved from 5.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.4 - Ensure permissions on /etc/cron.daily are configured moved from 5.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.5 - Ensure permissions on /etc/cron.weekly are configured moved from 5.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.6 - Ensure permissions on /etc/cron.monthly are configured moved from 5.1.6 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.1.7 - Ensure permissions on /etc/cron.d are configured moved from 5.1.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.1.2.1 - Ensure at is restricted to authorized users moved from 5.1.9 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 4.2 - Configure SSH Server moved from 5.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.2.1 - Ensure permissions on /etc/ssh/sshd_config are configured moved from 5.3.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.2.2 - Ensure permissions on SSH private host key files are configured moved from 5.3.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.2.3 - Ensure permissions on SSH public host key files are configured moved from 5.3.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.3.1 - Ensure sudo is installed moved from 5.2.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.3.2 - Ensure sudo commands use pty moved from 5.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.3.3 - Ensure sudo log file exists moved from 5.2.3 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.3.7 - Ensure access to the su command is restricted moved from 5.7 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 4.5 - User Accounts and Environment moved from 5.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.1.2 - Ensure password expiration is 365 days or less moved from 5.5.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.1.3 - Ensure password expiration warning days is 7 or more moved from 5.5.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.1.4 - Ensure inactive password lock is 30 days or less moved from 5.5.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.1.5 - Ensure all users last password change date is in the past moved from 5.5.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.2.1 - Ensure default group for the root account is GID 0 moved from 5.5.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.2.3 - Ensure system accounts are secured moved from 5.5.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.3.2 - Ensure default user shell timeout is configured moved from 5.5.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 4.5.3.3 - Ensure default user umask is configured moved from 5.5.5 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5 - Logging and Auditing moved from 4 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.1 - Configure Logging moved from 4.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.3 - Ensure logrotate is configured moved from 4.2.4 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.1.1 - Configure rsyslog moved from 4.2.1 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.1.1 - Ensure rsyslog is installed moved from 4.2.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.1.3 - Ensure journald is configured to send logs to rsyslog moved from 4.2.2.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.1.5 - Ensure logging is configured moved from 4.2.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.1.6 - Ensure rsyslog is configured to send logs to a remote log host moved from 4.2.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.1.2 - Configure journald moved from 4.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.2.3 - Ensure journald is configured to compress large log files moved from 4.2.2.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.1.2.4 - Ensure journald is configured to write logfiles to persistent disk moved from 4.2.2.3 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.2 - Configure System Accounting (auditd) moved from 4.1 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.2.1 - Ensure auditing is enabled moved from 4.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.1.2 - Ensure auditing for processes that start prior to auditd is enabled moved from 4.1.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.1.3 - Ensure audit_backlog_limit is sufficient moved from 4.1.2.4 in 3.1.2
12/22/2023	4.0.0	MOVED SECTION: 5.2.2 - Configure Data Retention moved from 4.1.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.2.1 - Ensure audit log storage size is configured moved from 4.1.2.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.2.2 - Ensure audit logs are not automatically deleted moved from 4.1.2.2 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.2.3 - Ensure system is disabled when audit logs are full moved from 4.1.2.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.1 - Ensure changes to system administration scope (sudoers) is collected moved from 4.1.14 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.4 - Ensure events that modify date and time information are collected moved from 4.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.5 - Ensure events that modify the system's network environment are collected moved from 4.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.8 - Ensure events that modify user/group information are collected moved from 4.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.9 - Ensure discretionary access control permission modification events are collected moved from 4.1.9 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.10 - Ensure successful file system mounts are collected moved from 4.1.12 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.11 - Ensure session initiation information is collected moved from 4.1.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.12 - Ensure login and logout events are collected moved from 4.1.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.13 - Ensure file deletion events by users are collected moved from 4.1.13 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected moved from 4.1.6 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.2.3.20 - Ensure the audit configuration is immutable moved from 4.1.17 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.3.1 - Ensure AIDE is installed moved from 1.3.1 in 3.1.2

Date	Version	Changes for this version
12/22/2023	4.0.0	MOVED RECOMMENDATION: 5.3.2 - Ensure filesystem integrity is regularly checked moved from 1.3.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.1 - Ensure permissions on /etc/passwd are configured moved from 6.1.2 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.2 - Ensure permissions on /etc/passwd- are configured moved from 6.1.3 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.3 - Ensure permissions on /etc/group are configured moved from 6.1.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.4 - Ensure permissions on /etc/group- are configured moved from 6.1.9 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.5 - Ensure permissions on /etc/shadow are configured moved from 6.1.4 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.6 - Ensure permissions on /etc/shadow- are configured moved from 6.1.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.8 - Ensure permissions on /etc/gshadow- are configured moved from 6.1.6 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.1.14 - Audit system file permissions moved from 6.1.1 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.2.4 - Ensure no duplicate UIDs exist moved from 6.2.7 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.2.5 - Ensure no duplicate GIDs exist moved from 6.2.8 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.2.6 - Ensure no duplicate user names exist moved from 6.2.5 in 3.1.2
12/22/2023	4.0.0	MOVED RECOMMENDATION: 6.2.7 - Ensure no duplicate group names exist moved from 6.2.6 in 3.1.2
UPDATED ITEMS:		
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log - Sections Modified: Rationale Statement; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.2.1 - Ensure GPG keys are configured - Sections Modified: Description; Rationale Statement; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.2.2 - Ensure gpgcheck is globally activated - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.2.4 - Ensure package manager repositories are configured - Sections Modified: Description; Rationale Statement; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.2.5 - Ensure updates, patches, and additional security software are installed - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.3.1 - Ensure bootloader password is set - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.3.2 - Ensure permissions on bootloader config are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.3.3 - Ensure authentication required for single user mode - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.4.1 - Ensure address space layout randomization (ASLR) is enabled - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 1.5 - Mandatory Access Control - Sections Modified: Description
12/22/2023	4.0.0	UPDATED SECTION: 1.5.1 - Configure SELinux - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.1 - Ensure SELinux is installed - Sections Modified: Remediation Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.2 - Ensure SELinux is not disabled in bootloader configuration - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.3 - Ensure SELinux policy is configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.5 - Ensure the SELinux mode is enforcing - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.6 - Ensure no unconfined services exist - Sections Modified: Description; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.5.1.8 - Ensure SETroubleshoot is not installed - Sections Modified: Remediation Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.6.1 - Ensure message of the day is configured properly - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.6.2 - Ensure local login warning banner is configured properly - Sections Modified: Remediation Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.6.3 - Ensure remote login warning banner is configured properly - Sections Modified: Remediation Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.7.1 - Ensure GNOME Display Manager is removed - Sections Modified: Assessment Status; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 1.7.2 - Ensure GDM login banner is configured - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 2 - Services - Sections Modified: Description

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 2.1.1 - Ensure time synchronization is in use - Sections Modified: Assessment Status; Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 2.1.2 - Ensure chrony is configured - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.1.2 - Ensure wireless interfaces are disabled - Sections Modified: Profile; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 3.4.2 - Configure firewalld - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.2.1 - Ensure firewalld is installed - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.2.3 - Ensure firewalld drops unnecessary services and ports - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.3.5 - Ensure nftables loopback traffic is configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 3.4.4.1 - Configure iptables software - Sections Modified: Description
12/22/2023	4.0.0	UPDATED SECTION: 3.4.4.2 - Configure iptables - Sections Modified: Description

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.2.3 - Ensure iptables rules exist for all open ports - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.2.5 - Ensure iptables rules are saved - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.3.1 - Ensure ip6tables loopback traffic is configured - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.3.2 - Ensure ip6tables outbound and established connections are configured - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.3.3 - Ensure ip6tables firewall rules exist for all open ports - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.3.4 - Ensure ip6tables default deny firewall policy - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 3.4.4.3.5 - Ensure ip6tables rules are saved - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 4 - Access, Authentication and Authorization - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.2 - Ensure permissions on /etc/crontab are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.3 - Ensure permissions on /etc/cron.hourly are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.4 - Ensure permissions on /etc/cron.daily are configured - Sections Modified: Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.5 - Ensure permissions on /etc/cron.weekly are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.6 - Ensure permissions on /etc/cron.monthly are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.1.7 - Ensure permissions on /etc/cron.d are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.1.2.1 - Ensure at is restricted to authorized users - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 4.2 - Configure SSH Server - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.2.1 - Ensure permissions on /etc/ssh/sshd_config are configured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.2.2 - Ensure permissions on SSH private host key files are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.2.3 - Ensure permissions on SSH public host key files are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.3.1 - Ensure sudo is installed - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.3.2 - Ensure sudo commands use pty - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.3.3 - Ensure sudo log file exists - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.3.7 - Ensure access to the su command is restricted - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.1.2 - Ensure password expiration is 365 days or less - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.1.3 - Ensure password expiration warning days is 7 or more - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.1.4 - Ensure inactive password lock is 30 days or less - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.1.5 - Ensure all users last password change date is in the past - Sections Modified: Rationale Statement; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.2.1 - Ensure default group for the root account is GID 0 - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.2.3 - Ensure system accounts are secured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.3.2 - Ensure default user shell timeout is configured - Sections Modified: Description; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 4.5.3.3 - Ensure default user umask is configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 5 - Logging and Auditing - Sections Modified: Description
12/22/2023	4.0.0	UPDATED SECTION: 5.1 - Configure Logging - Sections Modified: Description

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.3 - Ensure logrotate is configured - Sections Modified: Description
12/22/2023	4.0.0	UPDATED SECTION: 5.1.1 - Configure rsyslog - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.1.1 - Ensure rsyslog is installed - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.1.3 - Ensure journald is configured to send logs to rsyslog - Sections Modified: Assessment Status; Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.1.5 - Ensure logging is configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.1.6 - Ensure rsyslog is configured to send logs to a remote log host - Sections Modified: Assessment Status; Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 5.1.2 - Configure journald - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.2.3 - Ensure journald is configured to compress large log files - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.1.2.4 - Ensure journald is configured to write logfiles to persistent disk - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED SECTION: 5.2 - Configure System Accounting (auditd) - Sections Modified: Description
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.1.2 - Ensure auditing for processes that start prior to auditd is enabled - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.1.3 - Ensure audit_backlog_limit is sufficient - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.2.1 - Ensure audit log storage size is configured - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.2.3 - Ensure system is disabled when audit logs are full - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.1 - Ensure changes to system administration scope (sudoers) is collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.4 - Ensure events that modify date and time information are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.5 - Ensure events that modify the system's network environment are collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.8 - Ensure events that modify user/group information are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.9 - Ensure discretionary access control permission modification events are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.10 - Ensure successful file system mounts are collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.11 - Ensure session initiation information is collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.12 - Ensure login and logout events are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.13 - Ensure file deletion events by users are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.2.3.20 - Ensure the audit configuration is immutable - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.3.1 - Ensure AIDE is installed - Sections Modified: Description; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 5.3.2 - Ensure filesystem integrity is regularly checked - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.1 - Ensure permissions on /etc/passwd are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.2 - Ensure permissions on /etc/passwd- are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.3 - Ensure permissions on /etc/group are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.4 - Ensure permissions on /etc/group- are configured - Sections Modified: Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.5 - Ensure permissions on /etc/shadow are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.6 - Ensure permissions on /etc/shadow- are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.7 - Ensure permissions on /etc/gshadow are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.8 - Ensure permissions on /etc/gshadow- are configured - Sections Modified: Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.1.14 - Audit system file permissions - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.1 - Ensure accounts in /etc/passwd use shadowed passwords - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.3 - Ensure all groups in /etc/passwd exist in /etc/group - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.4 - Ensure no duplicate UIDs exist - Sections Modified: Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.5 - Ensure no duplicate GIDs exist - Sections Modified: Description; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.6 - Ensure no duplicate user names exist - Sections Modified: Description; Audit Procedure
12/22/2023	4.0.0	UPDATED RECOMMENDATION: 6.2.7 - Ensure no duplicate group names exist - Sections Modified: Audit Procedure