CIS FreeBSD 14 Benchmark

v1.0.1 - 11-19-2024

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/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (CISLegal@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ (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 and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

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

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To ensure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for FreeBSD systems running on amd64 platforms and arm64/aarch64.
This guide was developed and tested against FreeBSD 14.0
The guidance within broadly assumes that operations are being performed as the `root` user and executed under the default POSIX compliant shell(`/bin/sh`) 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 FreeBSD 14 on amd64 and arm64/aarch64 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, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

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**

  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**

  This profile extends the "Level 1" 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.

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/Unix 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 FreeBSD benchmarks.

Contributor
Allan Jude

Editor
Eric Pinnell
Justin Brown
Moin Rahman
Carole Fennelly

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

FreeBSD ships with support for multiple different filesystems but FreeBSD defaults to being installed with one of either UFS (Unix File System) or ZFS (Zettabyte File System). ZFS should not be confused with zFS(Z/OS File System) from IBM which is a different and unrelated file systems. FreeBSD also has the necessary support for reading and writing to traditional Linux file system specifically ext2, ext3 and ext4 with the help of the `ext2fs` kernel module.

A single FreeBSD RELEASE comes with a number of artifacts. Those serves different purposes and also has a large effect in terms of file systems. The `dvd1`, `disc1`, `bootonly`, `memstick` and `mini-memstick` release artifacts are installer images and can be used to install FreeBSD on any bare metal hosts with either `UFS` or `ZFS` as `root` partitions. There are also `arm-sd-card-images` which only allow installing on `UFS` root partition. `VM-IMAGES` comes in multiple flavors for different Virtualization Technologies including but not limited to Vmware Workstation/Player/Fusion/ESXi, Virtualbox, qemu and bhyve. These `VM-IMAGES` also has two different flavors of `UFS` and `ZFS`. Depending on requirements either of the images can be utilized to suite the need. FreeBSD RELEASE artifacts are also available in Amazon Web Services, Microsoft Azure and Google Cloud Platform in either `UFS` or `ZFS` flavor.

UFS is a battle tested file system in the UNIX history line and is suitable for embedded devices in today's context. Whereas ZFS is suitable for large systems specially with large number of storage disks. Although ZFS is memory hungry the tradeoff between the price performance is huge. Depending on the usage type FreeBSD can be installed in either UFS or ZFS. For most of the recommendations in this chapter UFS will be preferred over ZFS. As there are a large number of Cloud Users who often do not need to run large systems often prefer UFS over ZFS too. Clients often need to run micro services on smaller cloud instances where ZFS cannot scale. Although for bare metal servers ZFS is preferred.

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 UFS and ZFS 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.

Start up scripts

UFS is by default loaded statically into the kernel and ZFS can be loaded optionally with the startup script `zfs`. UFS cannot be disabled from being loaded into the kernel.

1.1.1.1 Ensure ext2fs kernel module is not available (Manual)

Profile Applicability:

- Level 1

Description:

The `ext2fs` filesystem module is used for reading or writing the traditional Linux filesystems like `ext2`/`ext3`/`ext4`.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. This module should be required only to temporarily read/write to `ext2`/`ext3`/`ext4` filesystems. If this filesystem type is not needed, disable it.

Audit:

Run the following script to verify the `ext2fs` module is disabled:
-IF- the module is available in the running kernel:

- The module is not loaded in the kernel

```
# kldstat -q -m ext2fs && printf "ext2fs kernel module is loaded\n" || printf
"ext2fs kernel module is NOT loaded\n"
```

Remediation:

Run the following script to disable the `ext2fs` module:
-IF- the module is available in the running kernel:

- Disable loading the kernel module
- Unload `ext2fs` from the kernel

```
# kldunload -f ext2fs
# printf "ext2fs_load=\"NO\"\n" >> /boot/loader.conf
```

Default Value:

ext2fs kernel module is NOT loaded

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 msdosfs kernel module is not available (Manual)

Profile Applicability:

- Level 1

Description:

The `msdosfs` driver will permit the FreeBSD kernel to read and write MS-DOS based file systems.

Rationale:

Removing support for unneeded file system types reduces the local attack surface of the system. This module is required only when reading or writing from MS-DOS based filesystems such as FAT16 or FAT32 file systems. These types of file systems are used on flash and other memory cards but have mostly been replaced with NTFS on Microsoft systems. It is recommended that support for these file system types these be disabled.

Audit:

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

- The module is not loaded in the kernel

```
# kldstat -q -m msdosfs && printf "msdosfs kernel module is loaded\n" ||
printf "msdosfs kernel module is NOT loaded\n"
```

Remediation:

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

- Disable loading the kernel module
- Unload `msdosfs` from the kernel

```
# kldunload -f msdosfs
# printf "msdosfs_load=\"NO\"\n" >> /boot/loader.conf
```

Default Value:

msdosfs kernel module is NOT loaded

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 zfs kernel module is not available (Manual)

Profile Applicability:

- Level 1

Description:

The `zfs` filesystem is a highly scalable filesystem used in FreeBSD for larger systems with huge disk spaces.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. This module is only required when ZFS storage systems are used, or FreeBSD has been installed in ZFS partitions. Disable the module if the system is an embedded device or smaller subsystem that does not use ZFS.

Audit:

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

- The module is not loaded in the kernel

```
# kldstat -q -m zfs && printf "zfs kernel module is loaded\n" || printf "zfs
kernel module is NOT loaded\n"
```

Remediation:

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

- Stop the `zfs` service
- Disable the `zfs` service
- Disable loading the kernel module
- Unload `zfs` from the kernel

```
# service zfs stop
# sysrc zfs_enable="NO"
# kldunload -f zfs
# printf "zfs_load=\"NO\"\n" >> /boot/loader.conf
```

Default Value:

zfs kernel module is NOT loaded

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

1.1.2 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/ada0p3 /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/da1 /var/tmp`
    - Update `/etc/fstab` with the new mountpoint. e.g. `/dev/ada0p3 /var/tmp ufs rw,nosuid,noexec 0 0`

1.1.2.1 Configure /tmp

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/tmp` its own file system allows an administrator to set 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 hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink 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.

1.1.2.1.1 Ensure /tmp is a separate partition (Manual)

Profile Applicability:

- Level 1

Description:

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

`/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 "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 two mount options for sizing:

- `size`: Specifies the total file system size in bytes. If zero (the default) or a value larger than SIZE_MAX - PAGE_SIZE is given, the available amount of memory (including main memory and swap space) will be used.
- `inodes`: Specifies the maximum number of nodes available to the file system. If not specified, the file system chooses a reasonable maximum based on the file system size, which can be limited with the size option.

These parameters accept a suffix k, m, g, t, or p, which denote byte, kilobyte, megabyte, gigabyte, terabyte and petabyte respectively and can be changed on remount.

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 attackers would have their own copy of the program. If the program happened to have a security vulnerability, the attackers 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.

```
# mount -p | grep -E '\s\/tmp'
```

Example output:

```
tmpfs on /tmp (tmpfs, local)
```

Ensure that rc will mount the `/tmp` partition at boot time.

```
# sysrc tmpmfs=YES
```

Example output:

```
tmpmfs: YES -> YES
```

Note: By default a `tmpfs` filesystem size of 20b is created. If the size needs to adjusted it should be configured with `sysrc tmpsize=<SIZE>`. The filesystem should also be remounted for the new size to take effect or be the system should be rebooted.

Remediation:

-If- `tmpfs` is being used First ensure that system will create a `tmpfs` file system at startup.

```
# sysrc tmpmfs="YES"
# sysrc tmpsize="2g"
```

For specific configuration requirements of the `/tmp` mount for your environment, modify `/etc/fstab` rather than utilizing `sysrc`.
Example of using `tmpfs` with specific mount options:

```
tmpfs   /tmp    tmpfs      rw,nosuid,noatime,size=2g   0 0
```

Note: the `size=2g` is an example of setting a specific size for `tmpfs`.
Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment:

```
<device> /tmp    <fstype>    rw,nosuid,noatime    0 0
```

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
T1499, T1499.001	TA0005	M1022

1.1.2.1.2 Ensure nosuid option set on /tmp partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

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` without the type `tmpfs`, verify that the `nosuid` option is set.
Run the following command to verify that the `nosuid` mount option is set.
Example:

```
# mount | grep -E '\s\/tmp.*tmpfs' | grep -v nosuid

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp` without the type tmpfs.
Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/tmp` partition.
Example:

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

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

```
# mount -u -o nosuid /tmp
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.1.3 Ensure noexec option set on /tmp partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING: This option was not designed as a security feature and no guarantee is made that it will prevent malicious code execution; for example, it is still possible to execute scripts which reside on a noexec mounted partition.

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`.

Audit:

- IF - a separate partition exists for `/tmp` without the type `tmpfs`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# mount | grep -E '\s\/tmp' | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp` without the type `tmpfs`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition.
Example:

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

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

```
# mount -u -o noexec /tmp
```

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
T1204, T1204.002	TA0005	M1022

1.1.2.2 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`.

1.1.2.2.1 Ensure separate partition exists for /home (Manual)

Profile Applicability:

- Level 2

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.

Control mount options 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:

```
# mount | grep -E '\s\/home'
/dev/ada0p8 on /home (ufs, local, soft-updates, journaled soft-updates)
```

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. 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

1.1.2.2.2 Ensure nosuid option set on /home partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

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:

```
# mount | grep -E '\s\/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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o nosuid /home
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.3 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.

1.1.2.3.1 Ensure separate partition exists for /var (Manual)

Profile Applicability:

- Level 2

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.

Control mount options 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:

```
# mount | grep -E '\s\/var\s'
/dev/ada0p4 on /var (ufs, local, nosuid, noexec, soft-updates, journaled
soft-updates)
```

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. 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

1.1.2.3.2 Ensure nosuid option set on /var partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

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:

```
# mount | grep -E '\s\/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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o nosuid /var
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.4 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.

1.1.2.4.1 Ensure separate partition exists for /var/tmp (Manual)

Profile Applicability:

- Level 2

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.

Control mount options Configuring `/var/tmp` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid`. 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 waiting for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have their 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:

```
# mount | grep -E '\s\/var\/tmp\s'
/dev/ada0p5 on /var/tmp (ufs, local, soft-updates, journaled soft-updates)
```

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. 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

1.1.2.4.2 Ensure nosuid option set on /var/tmp partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

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:

```
# mount | grep -E '\s\/var\/tmp\s' | 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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o nosuid /var/tmp
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.4.3 Ensure noexec option set on /var/tmp partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option was not designed as a security feature and no guarantee is made that it will prevent malicious code execution; for example, it is still possible to execute scripts which reside on a noexec mounted partition.

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:

```
# mount | grep -E '\s\/var\/tmp\s' | 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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o noexec /var/tmp
```

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
T1204, T1204.002	TA0005	M1022

1.1.2.5 Configure /var/log

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

1.1.2.5.1 Ensure separate partition exists for /var/log (Manual)

Profile Applicability:

- Level 2

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.

Control mount options Configuring `/var/log` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid`. 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:

```
# mount | grep -E '\s\/var\/log\s'
/dev/ada0p6 on /var/log (ufs, local, soft-updates, journaled soft-updates)
```

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. 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

1.1.2.5.2 Ensure nosuid option set on /var/log partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

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:

```
# mount | grep -E '\s\/var\/log\s' | 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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o nosuid /var/log
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.5.3 Ensure noexec option set on /var/log partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option was not designed as a security feature and no guarantee is made that it will prevent malicious code execution; for example, it is still possible to execute scripts which reside on a noexec mounted partition.

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:

```
# mount | grep -E '\s\/var\/log\s' | 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>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o noexec /var/log
```

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
T1204, T1204.002	TA0005	M1022

1.1.2.6 Configure /var/audit

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

1.1.2.6.1 Ensure separate partition exists for /var/audit (Manual)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Protection from resource exhaustion The default installation only creates a single `/` partition. Since the `/var/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/audit`.

Control mount options Configuring `/var/audit` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid`. 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/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/audit` is mounted:

```
# mount | grep -E '\s\/var\/audit\s'
/dev/ada0p7 on /var/audit (ufs, local, soft-updates, journaled soft-updates)
```

Remediation:

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

References:

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

Additional Information:

When modifying `/var/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

1.1.2.6.2 Ensure nosuid option set on /var/audit partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option is worthless if a publicly available suid or sgid wrapper is installed on your system. It is set automatically when the user does not have super-user privileges.

Rationale:

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

Audit:

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

```
# mount | grep -E '\s\/var\/audit\s' | grep -v nosuid

Nothing should be returned
```

Remediation:

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

```
<device> /var/audit    <fstype>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o nosuid /var/audit
```

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
T1548, T1548.001	TA0005	M1022

1.1.2.6.3 Ensure noexec option set on /var/audit partition (Manual)

Profile Applicability:

- Level 1

Description:

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

WARNING This option was not designed as a security feature and no guarantee is made that it will prevent malicious code execution; for example, it is still possible to execute scripts which reside on a `noexec` mounted partition.

Rationale:

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

Audit:

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

```
# mount | grep -E '\s\/var\/audit\s' | grep -v noexec

Nothing should be returned
```

Remediation:

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

```
<device> /var/audit    <fstype>     rw,nosuid,noexec  0 0
```

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

```
# mount -u -o noexec /var/audit
```

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
T1204, T1204.002	TA0005	M1022

1.2 Configure Software and Patch Management

FreeBSD uses the `freebsd-update` utility to update the base operating system and `pkg` to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install local updates to a server that can be used in place of their distributions servers, whereas a single deployment of a system may get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

Outdated software is vulnerable to attack. Promptly updating software reduces the risk to your organization. The software update release notes often reveal the patched exploitable entry points to the public. Public knowledge of these exploits makes your organization more vulnerable to malicious attackers 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 update server certificate key fingerprints are configured (Manual)

Profile Applicability:

- Level 1

Description:

FreeBSD downloads binary updates from an update server and uses Public Key Infrastructure to verify the downloads. This key fingerprint is used in the file `/etc/freebsd-update.conf`. This key fingerprint varies between different versions of FreeBSD and must be validated manually.

Rationale:

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. Verify the key fingerprint being used is correctly configured in the file `/etc/freebsd-update.conf`.

Impact:

By downloading updates from the wrong server there is the possibility that someone is injecting malicious content in the base operating system.

Audit:

Download the certificate files manually and verify.
Get the public key. Verify the signature yourself [*]

```
$ fetch http://update.freebsd.org/14.0-RELEASE/amd64/pub.ssl
```

Get metadata

```
$ fetch http://update.freebsd.org/14.0-RELEASE/amd64/latest.ssl
```

Verify

```
$ openssl rsautl -pubin -inkey pub.ssl -verify <latest.ssl
```

The output looks like this:

```
freebsd-update|amd64|14.0-
RELEASE|5|d2152f1824dd0cda99d7c83899f27d4dca5f47cac4469444fc2e1aaae8a5de47|17
38281600
```

"5" in the output of this example refers to p5, the 5th patch level for 14.0-RELEASE amd64
The following compares the server's pub.ssl with the hash value that exists on the system:

```
$ sha256 -q pub.ssl
$ grep KeyPrint /etc/freebsd-update.conf | cut -f 2 -w
```

The outputs of the commands should be identical, indicating the signature is "good" (verified)

Remediation:

If the previous outputs of the commands are not identical, there is a high possibility that something is wrong with the system. The verification of certificates might fail for various reasons, but the most common issue is improper date and time. Or in case the version of FreeBSD is too old and the specific running version has not been updated for a long time. Check the date and time before proceeding further.

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.	●	●	●

1.2.2 Ensure package manager repositories are configured (Manual)

Profile Applicability:

- Level 1

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:

```
# ❯ pkg -vv | sed  '1, /^Repositories/d'
  FreeBSD: {
    url             : "pkg+http://pkg.FreeBSD.org/FreeBSD:14:amd64/latest",
    enabled         : no,
    priority        : 0,
    mirror_type     : "SRV",
    signature_type  : "FINGERPRINTS",
    fingerprints    : "/usr/share/keys/pkg"
  }
```

For the repositories in use, inspect the configuration file to ensure all settings are correctly applied according to site policy.
Example:
Depending on situation like custom pkg repos file name might differ.

```
# cat /etc/pkg/*.conf
# cat /usr/local/etc/pkg/repos/*.conf
```

Remediation:

Configure your package manager repositories according to site policy.

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.	●	●	●
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

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

Profile Applicability:

- Level 1

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 for the base system:

```
# freebsd-update updatesready
```

If there are updates available it will prompt for installing those updates and if required also ask for rebooting.

Remediation:

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

```
# freebsd-update fetch install
```

Once the update process is complete, verify if reboot is required to load changes or not. The system will prompt for reboot.
The following command will install all available updates for the third party softwares:

```
# pkg update
# pkg upgrade
```

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.	●	●	●
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.

1.3.1 Ensure bootloader password is set (Automated)

Profile Applicability:

- Level 1

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. reducing kernel security level at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a Boot Menu.

If Boot menu 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.

Audit:

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

```
# grep ^password /boot/loader.conf
```

Output should be similar to:

```
password=Jmklvqqq8MCqg91L
```

WARNING The password is saved in plaintext.

Remediation:

Add password to the `/boot/loader.conf` file by having an entry like the following:

```
password=Jmklvqqq8MCqg91L
```

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
T1542, T1542.000	TA0003	M1046

1.3.2 Ensure permissions on bootloader config are configured (Manual)

Profile Applicability:

- Level 1

Description:

The `loader.conf` file 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 `loader.conf` file:

- Mode is `0600` or more restrictive
- Owner is the user `root`
- Group owner is group `wheel`

```
# stat -Lf 'Access: (%Lp/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)'
/boot/loader.conf
Access: (600/-rw-------)  Uid: ( 0/ root) Gid: ( 0/ wheel)
# [ -e /boot/loader.conf.local ] && stat -Lf 'Access: (%Lp/%Sp)  Uid: ( %u/
%Su) Gid: ( %g/ %Sg)' /boot/loader.conf.local
```

Remediation:

Run the following to update the mode, ownership, and group ownership of the `/boot/loader.conf` configuration file:

```
# [ -f /boot/loader.conf ] && chown root:wheel /boot/loader.conf
# [ -f /boot/loader.conf ] && chmod u-x,go-rwx /boot/loader.conf
# [ -e /boot/loader.conf.local ] && chown root:wheel /boot/loader.conf.local
# [ -e /boot/loader.conf.local ] && chmod u-x,go-rwx /boot/loader.conf.local
```

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
T1542, T1542.000	TA0005, TA0007	M1022

1.4 Configure Additional Process Hardening

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

Profile Applicability:

- Level 1

Description:

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

NOTE Starting from FreeBSD 13.2 ASLR is enabled by default.

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:

- `kern.elf64.aslr.enable` is set to `1`

```
#  [ $(sysctl -nq kern.elf64.aslr.enable) -eq 1 ] && printf "ASLR is
enabled\n" || printf "ASLR is disabled\n"
```

Remediation:

Set the following parameter in `/etc/sysctl.conf`:

- `kern.elf64.aslr.enable=1`

Example:

```
# printf "
kern.elf64.aslr.enable=1
" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl kern.elf64.aslr.enable=1
```

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

Default Value:

kern.elf64.aslr.enable=1

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 core dump backtraces are disabled (Manual)

Profile Applicability:

- Level 1

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 to determine whether the service that dumps the core is disabled. :

```
# sysrc -n savecore_enable
YES
```

The service is enabled by default.

Remediation:

Disable the service using `service`

```
# service savecore onestop
# service savecore disable
```

Default Value:

`savecore_enable=YES`

References:

1. NIST SP 800-53 Rev. 5: CM-6b

MITRE ATT&CK Mappings:

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

1.4.3 Ensure core dump storage is disabled (Manual)

Profile Applicability:

- Level 1

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 script to verify `dumpdev` is set to `NO`:

```
# sysrc -n dumpdev
```

Remediation:

Disable the `dumpdev` by setting it to `NO`.

```
sysrc dumpdev=NO
```

Default Value:

`dumpdev=NO`

MITRE ATT&CK Mappings:

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

1.5 Mandatory Access Control

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

FreeBSD supports security extensions based on the POSIX®.1e draft. These security mechanisms include file system Access Control Lists (“Access Control Lists”) and Mandatory Access Control (MAC). MAC allows access control modules to be loaded to implement security policies. Some modules protect a narrow subset of the system, hardening a particular service. Others provide comprehensive labeled security across all subjects and objects. The mandatory part of the definition indicates that administrators and the operating system enforce controls. This contrasts the default security mechanism of Discretionary Access Control (DAC) where enforcement is left to users' discretion.

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.

WARNING: Improper MAC configuration may cause loss of system access, aggravation of users, or inability to access the features provided by Xorg. More importantly, MAC should not be relied upon to secure a system completely. The MAC framework only augments an existing security policy. The system will never be completely secure without sound security practices and regular security checks.

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`, and `/etc/issue` 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 (Manual)

Profile Applicability:

- Level 1

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.

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 system exploits. Once logged in, authorized users can easily get this information by running the " `uname -a` " command.

FreeBSD, by default, uses a service `motd` to generate the running FreeBSD version and add it to the `/etc/motd` file.

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 "$(grep '^VERSION=' /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 references to the `OS platform`.
-OR-
-IF- the `motd` is not used, this file can be removed.
Run the following command to disable the `motd` service:

```
# rm -f /etc/motd
# service motd stop
# service motd disable
# cat /etc/mot
```

Add the default template without any version-specific information:

```
# cp /etc/motd.template /etc/motd
```

-OR-
Edit the file `/etc/motd` with content that is appropriate to your site policy.

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 (Manual)

Profile Applicability:

- Level 1

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Unix-based systems typically display information about the OS release and patch level upon logging in. This information can be useful to developers who are developing software for a particular OS platform. FreeBSD does not use the `issue` file by default. `sshd` needs to be configured properly to utilize the `/etc/issue` file.

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 system exploits. Once logged in, authorized users can easily get this information by running the " `uname -a` " command.

Audit:

Run the following command and verify that the contents match site policy:

```
# [ -f /etc/issue ] && cat /etc/issue
```

Run the following command and verify no results are returned:

```
# [ -f /etc/issue] && grep -E -i "$(grep '^VERSION=' /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 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 (Manual)

Profile Applicability:

- Level 1

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.

FreeBSD does not specifically utilizes `issue.net`. This is only required for `telnetd` or `ftpd`.

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:

```
# [ -f /etc/issue.net ] && cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# [ -f /etc/issue.net ] && grep -E -i "$(grep '^VERSION=' /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 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 (Manual)

Profile Applicability:

- Level 1

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 `0/root` and `0/wheel` respectively:

```
# [ -e /etc/motd ] && stat -L -f 'Access: (%Lp/%Sp)  Uid: ( %u/ %Su) Gid: (
%g/ %Sg)' /etc/motd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ wheel)
  -- OR --
Nothing is returned
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/motd`:

```
# chown root:wheel $(readlink -f /etc/motd)
# chmod u-x,go-wx $(readlink -f /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 (Manual)

Profile Applicability:

- Level 1

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 `0/root` and `0/wheel` respectively:

```
# [ -e /etc/issue ] && stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: (
%g/ %Sg)' /etc/issue

Access: (644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

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: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ wheel)

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

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. This section also covers secure configuration for services that need to be enabled.

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 `ntpd`.

2.1.1 Ensure time synchronization is in use (Manual)

Profile Applicability:

- Level 1

Description:

Synchronize system time between all systems in an environment using a service such as the Network Time Protocol (NTP) daemon, ntpd or chrony which are designed to synchronize system clocks across a variety of systems using a source that is accurate. NTP can be configured to be a client and/or a server.

Note: If another method for time synchronization is being used, this section may be skipped.

Rationale:

Time synchronization enables support of time sensitive security mechanisms, such as Kerberos. Time synchronization also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

Run the following commands to verify that `ntpd` is running:

```
# service ntpd status
```

Remediation:

Run the following command to enable and start `ntpd` service:

```
# service ntpd enable
# sysrc ntpd_sync_on_start="YES"
# service ntpd start
```

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 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	

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 disable the service:

```
# service <service_name> onestop
# service <service_name> onedisable
```

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 (Manual)

Profile Applicability:

- Level 1

Description:

The `autofs` service allows automatic mounting of devices, which typically includes 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.

`autofs` is part of the base system and is disabled by default.

Audit:

Run the following command to verify `autofs` is not enabled:

```
# sysrc -q -n autofs_enable | grep 'YES'

Nothing should be returned
```

Remediation:

Run the following commands to stop `automount` and disable `automount` service:

```
# service automount onestop
# service automount onedisable
```

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		

2.2.2 Ensure ftp server services are not in use (Manual)

Profile Applicability:

- Level 1

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). FreeBSD ships with one basic `ftpd` in the base system and there is also the famous `vsftpd` available through package.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. 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 deleted to reduce the potential attack surface.

Impact:

`ftpd` from the base system is run through `inetd` server which cannot be removed but disabled.

There may be packages that are dependent on the `vsftpd-ext` or `vsftpd-ssl` package. If the packages are removed, these dependent packages will be removed as well. Before removing the packages, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and disable the `vsftpd` and `vsftpd6` services leaving the packages installed.

Audit:

Run the following command to verify `ftpd` is not enabled through `inetd`:

```
# grep -E '^ftp\s' /etc/inetd.conf

Nothing should be returned
```

-IF- anything is returned the `ftpd` service should be disabled:

```
# sed -i '' -e 's|^ftp|#ftp|g' /etc/inetd.conf
# service inetd restart
```

-OR-
Run the following command to verify `vsftpd` is not installed:

```
# pkg query -g %n 'vsftpd*'

Nothing should be returned
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `vsftpd` service is not enabled:

```
# sysrc -q -n vsftpd | grep 'YES'
# sysrc -q -n vsftpd6 | grep 'YES'

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` / `vsftpd6` and remove `vsftpd` packages:

```
# service onestop vsftpd
# service onestop vsftpd6
# pkg remove -g 'vsftpd*'
```

-OR-
-IF- the packages is required as a dependency:
Run the following commands to stop and disable the `vsftpd` or `vsftpd6` service:

```
# service vsftpd onestop
# service vsftpd6 onestop
# service vsftpd onedisable
# service vsftpd6 onedisable
```

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 disabled.

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

2.2.3 Ensure message access server services are not in use (Manual)

Profile Applicability:

- Level 1

Description:

The dovecot and cyrus-imapd services are open source IMAP and POP3 server packages.

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 disable `dovecot` and `cyrus_imapd` leaving `dovecot` and `cyrus-imapd` packages installed.

Audit:

Run the following command to verify `dovecot` and `cyrus-imapd` are not installed:

```
# pkg query -g %n 'dovecot*'
# pkg query -g %n 'cyrus-imapd*'

Nothing should be returned
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to verify `dovecot` and `cyrus_imapd` are not enabled:

```
# sysrc -q -n dovecot_enable | grep YES
# sysrc -q -n cyrus_imapd_enable | grep YES

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` and `cyrus_imapd`, and remove `dovecot` and `cyrus-imapd` packages:

```
# service dovecot onestop
# service cyrus_imapd onestop
# pkg remove -g 'dovecot*' 'cyrus-imap*'
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to stop and disable `dovecot` and `cyrus_imapd`:

```
# service dovecot onestop
# service cyrus_imapd onestop
# service dovecot onedisable
# service cyrus_imapd onedisable
```

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

2.2.4 Ensure network file system services are not in use (Manual)

Profile Applicability:

- Level 1

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. FreeBSD ships with an NFS Server in disabled state in the base system.

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 `nfsd` service be disabled to reduce the attack surface of the system.

Audit:

Run the following command to verify `nfsd` is disabled:

```
# sysrc -q -n nfs_server_enable | grep YES

Nothing should be returned
```

Remediation:

Run the following command to stop and disable the `nfsd` service:

```
# service nfsd onestop
# service nfsd onedisable
```

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, T1210, T1210.000	TA0008	M1042

2.2.5 Ensure nis server services are not in use (Manual)

Profile Applicability:

- Level 1

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). FreeBSD ships with a NIS server in base installation which is disabled by default.

Audit:

Run the following command to verify `ypserv` is not enabled:

```
# sysrc -q -n nis_server_enable | grep YES

Nothing should be returned
```

Remediation:

Run the following commands to stop `ypserv` and disable `ypserv`:

```
# service ypserv onestop
# service ypserv onedisable
```

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 rpcbind services are not in use (Manual)

Profile Applicability:

- Level 1

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` 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. FreeBSD ships with `rpcbind` in the base system and is by default disabled.

Audit:

Run the following command to verify `rpcbind` is not enabled:

```
# sysrc -q -n rpcbind_enable | grep YES

Nothing should be returned
```

Remediation:

Run the following commands to stop and disable `rpcbind`:

```
# service rpcbind onestop
# service rpcbind onedisable
```

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

2.2.7 Ensure snmp services are not in use (Manual)

Profile Applicability:

- Level 1

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, remove the net-snmp package 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 disable the `snmpd` leaving the `net-snmp` package installed.

Audit:

Run the following command to verify `net-snmp` package is not installed:

```
# pkg query %n net-snmp

Nothing should be returned
```

-OR- If the package is required for dependencies:
Run the following command to verify the `snmpd.service` is not enabled:

```
# sysrc -q -n snmpd_enable  | grep YES

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` and remove `net-snmp` package:

```
# service snmpd onestop
# pkg remove net-snmp
```

-OR- If the package is required for dependencies:
Run the following commands to stop and disable the `snmpd`:

```
# service snmpd onestop
# service snmpd onedisable
```

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

2.2.8 Ensure telnet server services are not in use (Manual)

Profile Applicability:

- Level 1

Description:

The `freebsd-telnetd` 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` service provides an encrypted session and stronger security.

Impact:

There may be packages that are dependent on the `freebsd-telnetd` package. If the `freebsd-telnetd` package is removed, these dependent packages will be removed as well. Before removing the `freebsd-telnetd` package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and disable the `telnet` service leaving the `freebsd-telnetd` package installed.

Audit:

Run the following command to verify the `freebsd-telnetd` package is not installed:

```
# pkg query %n freebsd-telnetd

Nothing should be returned
```

-OR-
-IF- a package is installed **and** is required for dependencies:
Run the following command to verify `telnet` is not enabled:

```
# grep -E '^telnet\s' /etc/inetd.conf

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 and disable `telnet`:

```
# sed -i '' -e 's|^telnet|#telnet|g' /etc/inetd.conf
# service inetd restart
```

-AND-
-IF- a package is installed **and** is required for dependencies:
Run the following commands to remove the `freebsd-telnetd` package:

```
# pkg remove freebsd-telnetd
```

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

2.2.9 Ensure tftp server services are not in use (Manual)

Profile Applicability:

- Level 1

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 service is disabled 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.

FreeBSD ships with a `tftpd` in the base system which is served through `inetd` and is disabled by default.

Impact:

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

Audit:

Run the following command to verify `tftp` is not enabled:

```
# grep -E '^tftp\s' /etc/inetd.conf

Nothing should be returned
```

Remediation:

Run the following commands to stop and disable `tftp`:

```
# sed -i '' -e 's|^tftp|#tftp|g' /etc/inetd.conf
# service inetd restart
```

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

2.2.10 Ensure web proxy server services are not in use (Manual)

Profile Applicability:

- Level 1

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 disable the `squid` leaving the `squid` package installed.

Audit:

Run the following command to verify `squid` package is not installed:

```
# pkg query -g %n 'squid*'

Nothing should be returned
```

-OR-
-IF- the package is required for dependencies:
Run the following command to verify `squid` is not enabled:

```
# sysrc -q -n squid_enable | grep YES

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` and remove the `squid` package:

```
# service squid onestop
# pkg remove squid
```

-OR- If the `squid` package is required as a dependency:
Run the following commands to stop and disable the `squid`:

```
# service squid onestop
# service squid onedisable
```

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

2.2.11 Ensure mail transfer agents are configured for local-only mode (Automated)

Profile Applicability:

- Level 1

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`)

```
#  sockstat -46L | grep -E ':25\b|:465\b|:587\b'
```

Nothing should be returned

Remediation:

Edit `/usr/local/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 = localhost
```

Run the following command to restart `postfix`:

```
# service 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

2.2.12 Ensure only approved services are listening on a network interface (Manual)

Profile Applicability:

- Level 1

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. Review these services, and if not required, stop the service, and remove the package containing the service.

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.

Audit:

Run the following command:

```
# sockstat -46L
```

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:
    - Disable the service
    - Remove the package containing the service
    - **-IF-** the service's package is required for a dependency, stop and disable the service and/or socket

Remediation:

Run the following commands to stop the service and remove the package containing the service:

```
# service <service_name> stop
# pkg remove <service_name>
```

-OR- If required packages have a dependency:
Run the following commands to stop and mask the service and socket:

```
# service <service_name> stop
# service <service_name> disable
```

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

3 Network

This section provides guidance for secure network and firewall configuration.

3.1 Configure Network Devices

Disable unused devices to reduce the attack surface of the system.

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

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 340,282,366,920,938,463,463,374,607,431,768,211,456 unique 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:

```
# [ $(sysctl -nq kern.features.inet6) -eq 1 ] && printf "IPv6 is enabled\n"
|| printf "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

3.2 Configure Network Kernel Modules

The FreeBSD 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 sctp kernel module is not available (Manual)

Profile Applicability:

- Level 2

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:

By default FreeBSD kernel ships with the option to load `sctp` module dynamically. Run the following script to verify the `sctp` module is disabled:

```
# kldstat -q -m sctp && printf "sctp kernel module is loaded\n" || printf
"sctp kernel module is NOT loaded\n"
```

Remediation:

Run the following script to disable the `sctp` module:

```
# printf 'module_blacklist="sctp"\n' >> /boot/loader.conf
```

A system reboot is preferred to make sure that `sctp` kernel was not loaded and active.

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 `/etc/sysctl.conf` and `/etc/sysctl.conf.local`.
- The paths where sysctl preload files usually exist
  - `/etc/sysctl.kld.d/*.conf`
  - `/etc/sysctl.conf.local`
  - `/etc/sysctl.conf`
- Files must have the "`.conf`" extension
- The command `sysctl -A` produces output containing The system's loaded kernel parameters and the files they're configured in:
  - 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

The system's loaded kernel parameters and the files they're configured in can be viewed by running the following command:

```
# sysctl -A
```

3.3.1 Ensure ip forwarding is disabled (Manual)

Profile Applicability:

- Level 1

Description:

The `net.inet.ip.forwarding` and `net.inet6.ip.forwarding` flags tell the system whether it can forward packets.

In FreeBSD, there are also two other services, mainly `gateway` and `ipv6_gateway`, that enable the same behind the scenes.

Rationale:

Setting `net.inet.ip.forwarding` and `net.inet6.ip.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. Also make sure that the `gateway` and `ipv6_gateway` services are disabled.

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 runs 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.inet.ip.forwarding` is set to `0`
- `net.inet6.ip.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

```
#  [ $(sysctl -nq net.inet.ip.forwarding) -eq 1 ] && printf "IPv4 Forwarding
is Enabled\n" || printf "IPv4 Forwarding is Disabled\n"
#  [ $(sysctl -nq net.inet6.ip.forwarding) -eq 1 ] && printf "IPv6 Forwarding
is Enabled\n" || printf "IPv6 Forwarding is Disabled\n"
```

Also run the following commands to check if the `gateway` and `ipv6_gateway` services are enabled:

```
# sysrc -q -n gateway_enable | grep YES
# sysrc -q -n ipv6_gateway_enable | grep YES
```

Remediation:

FreeBSD ships with default disabled. Stop and disable the `gateway` and `ipv6_gateway` services.
Example:

```
# service gateway stop
# service gateway disable
```

-IF- IPv6 is enabled on the system:
Example:

```
# service ipv6_gateway stop
# service ipv6_gateway disable
```

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

Default Value:

net.inet.ip.forwarding = 0

net.inet6.ip.forwarding = 0

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	4.8 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 (Manual)

Profile Applicability:

- Level 1

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.inet.ip.redirect` is set to `0`
- `net.inet6.ip6.redirect` 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.

```
#  [ $(sysctl -nq net.inet.ip.redirect) -eq 1 ] && printf "IPv4 Redirect is
Enabled\n" || printf "IPv4 Redirect is disabled\n"
#  [ $(sysctl -nq net.inet6.ip6.redirect) -eq 1 ] && printf "IPv6 Redirect is
Enabled\n" || printf "IPv6 Redirect is disabled\n"
```

Remediation:

Set the following parameters in `/etc/sysctl.conf`:

- `net.inet.ip.redirect=0`
- `net.inet6.ip6.redirect=0`

Example:

```
# printf "
net.inet.ip.redirect=0
net.inet6.ip6.redirect=0
" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {
   sysctl net.inet.ip.redirect=0
   sysctl net.inet6.ip6.redirect=0
}
```

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

Default Value:

net.inet.ip.redirect=0

net.inet6.ip6.redirect=0

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	4.8 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 broadcast & multicast icmp requests are ignored (Manual)

Profile Applicability:

- Level 1

Description:

Broadcast ICMP request is an ICMP packet sent to all hosts in a subnet, used for network diagnostics like discovering hosts or testing connectivity, but often disabled for security reasons. Multicast ICMP request targets a specific group of subscribed hosts, allowing efficient data distribution for applications like streaming media, reducing bandwidth usage by sending data to multiple recipients simultaneously.

This 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.inet.icmp.bmcastecho` is set to `0`
- `net.inet.icmp.tstamprepl` 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.

```
# [ $(sysctl -nq net.inet.icmp.bmcastecho) -eq 1 ] && printf "Broadcast and
Multicast ICMP ECHO requests are accepted\n" || printf "Broadcast and
Multicast ICMP ECHO requests are not accepted\n"
# [ $(sysctl -nq net.inet.icmp.tstamprepl) -eq 1 ] && printf "Broadcast and
Multicast ICMP TIMESTAMP requests are accepted\n" || printf "Broadcast and
Multicast ICMP TIMESTAMP requests are not accepted\n"
```

Remediation:

Set the following parameter in `/etc/sysctl.conf`:

- `net.inet.icmp.bmcastecho=0`
- `net.inet.icmp.tstamprepl=0`

Example:

```
# printf "
net.inet.icmp.bmcastecho=0
net.inet.icmp.tstamprepl=0
" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet.icmp.bmcastecho=0
# sysctl net.inet.icmp.tstamprepl=0
```

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

Default Value:

net.inet.icmp.bmcastecho = 0

net.inet.icmp.tstamprepl = 1

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	4.8 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

3.3.4 Ensure icmp redirects are not accepted (Manual)

Profile Applicability:

- Level 1

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.inet.icmp.drop_redirect` to `1` and `net.inet6.icmp6.rediraccept` 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.inet.icmp.drop_redirect` is set to `1`
- `net.inet6.icmp6.rediraccept` 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

```
#  [ $(sysctl -nq net.inet.icmp.drop_redirect) -eq 1 ] && printf "IPv4 ICMP
Redirects are dropped\n" || printf "IPv4 ICMP Redirects are NOT dropped\n"
#  [ $(sysctl -nq net.inet6.icmp6.rediraccept) -eq 0 ] && printf "IPv6 ICMP
Redirects are dropped\n" || printf "IPv6 ICMP Redirects are NOT dropped\n"
```

Remediation:

Set the following parameters in `/etc/sysctl.conf`:

- `net.inet.icmp.drop_redirect=1`

Example:

```
# printf "
net.inet.icmp.drop_redirect: 1
" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet.icmp.drop_redirect=1
```

-IF- IPv6 is enabled on the system:
Set the following parameters in `/etc/sysctl.conf`:

- `net.inet6.ip6.redirect=0`

Example:

```
# printf "
net.inet6.icmp6.rediraccept: 0
" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet6.icmp6.rediraccept=0
```

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

Default Value:

net.inet.icmp.drop_redirect = 1

net.inet6.icmp6.rediraccept = 0

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	4.8 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

3.3.5 Ensure source routed packets are not accepted (Manual)

Profile Applicability:

- Level 1

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.inet.ip.accept_sourceroute` 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.inet.ip.accept_sourceroute` 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.

```
# [ $(sysctl -nq net.inet.ip.accept_sourceroute) -eq 1 ] && printf "IP Source
Routes are accepted\n" || printf "IP Source Routes are not accepted\n"
```

Remediation:

Set the following parameters in `/etc/sysctl.conf`:

- `net.inet.ip.accept_sourceroute=0`

Example:

```
# printf "net.inet.ip.accept_sourceroute=0\n" >> /etc/sysctlconf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet.ip.accept_sourceroute=0
```

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

Default Value:

net.inet.ip.accept_sourceroute = 0

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	4.8 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	

3.3.6 Ensure tcp syn cookies is enabled (Manual)

Profile Applicability:

- Level 1

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.inet.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.inet.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.

```
# [ $(sysctl -nq net.inet.tcp.syncookies) -eq 1 ] && printf "TCP syncookies
are enabled\n" || printf "TCP syncookies are NOT enabled\n"
```

Remediation:

Set the following parameter in `/etc/sysctl.conf`:

- `net.inet.tcp.syncookies=1`

Example:

```
# printf "net.inet.tcp.syncookies=1\n" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet.tcp_syncookies=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

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

3.3.7 Ensure ipv6 router advertisements are not accepted (Manual)

Profile Applicability:

- Level 1

Description:

ICMPv6 RAs(Router Advertisements) are intended to help facilitate bootstrapping the connectivity of an IPv6 node on a network. They tell the hosts on the LAN how they should go about acquiring their global unicast IPv6 address and become productive members of the network. The RA also provides the end-node information about the local router and its ability to be the default gateway. This process is well documented in Section 4 of the IETF RFC 4861 “Neighbor Discovery for IP version 6 (IPv6)”.

Unfortunately, there are some security risks related to ICMPv6 RA messages. On networks that do not yet use IPv6, the dual-stack hosts sit dormant waiting for an eventual RA message to awaken their IPv6 connectivity. An attacker can craft a “rogue RA” message on these networks, get the dual-protocol nodes on the network to configure their IPv6 addresses and utilize the attacker’s system as their default gateway. The attacker can then easily perform a Man-In-The-Middle (MITM) attack without the user’s knowledge using this technique. This issue is documented in RFC 6104 “Rogue IPv6 Router Advertisement Problem Statement”. On networks that already have IPv6 running, rogue RAs can destabilize the network (and still perform a MITM attack).

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.inet6.ip6.accept_rtadv` to `0` disables the system's ability to accept IPv6 router advertisements. This is the default in FreeBSD system.

Audit:

Run the following to verify the following kernel parameters are set:

```
#  [ $(sysctl -nq net.inet6.ip6.accept_rtadv) -eq 1 ] && printf "IPv6 Router
Advertisements are accepted\n" || printf "IPv6 Router Advertisements are not
accepted\n"
```

Remediation:

-IF- IPv6 is enabled on the system:
Set the following parameters in `/etc/sysctl.conf`:

```
net.inet6.ip6.accept_rtadv=0
```

Example:

```
# printf "net.inet6.ip6.accept_rtadv=0\n" >> /etc/sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# sysctl net.inet6.ip6.accept_rtadv=0
```

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

Default Value:

net.inet6.ip6.accept_rtadv=0

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	4.8 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 Host Based Firewall, on a FreeBSD system, 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, FreeBSD ships with three different firewall utilities which are ipfw, pf and ipfilter.

Only one of the firewall utilities should be utilized. People coming from an OpenBSD background prefer pf although the pf of FreeBSD vastly differs with the syntax from the OpenBSD pf syntax. For this documentation we will keep the recommendations within ipfw only. In case some other choices are made, firewall rules should be carefully checked to ensure that they match the same recommendations.

3.4.1 Configure a firewall utility

In order to configure firewall rules for ipfw, a firewall service needs to be enabled. Guidance has been included for the `ipfw` firewall utility:

IPFW is a stateful firewall written for FreeBSD which supports both IPv4 and IPv6. It is comprised of several components: the kernel firewall filter rule processor and its integrated packet accounting facility, the logging facility, NAT, the dummynet traffic shaper, a forward facility, a bridge facility, and an ipstealth facility.

FreeBSD provides a sample ruleset in `/etc/rc.firewall` which defines several firewall types for common scenarios to assist novice users in generating an appropriate ruleset. IPFW provides a powerful syntax which advanced users can use to craft customized rulesets that meet the security requirements of a given environment.

3.4.1.1 Ensure ipfw is enabled and configured (Manual)

Profile Applicability:

- Level 1

Description:

The ipfw interface provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and an ipfw userspace command line tool.

The ipfw interface reuses the existing dummynet subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Rationale:

The ipfw is a subsystem of the FreeBSD 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 `ipfw` is enabled:

```
# service ipfw status
ipfw is not enabled
```

Remediation:

Run the following command to install and enable `ipfw`. The firewall profile `workstation` comes with sane and secure configurations for a single host.

```
# sysrc firewall_enable="YES"
# sysrc firewall_type="workstation"
# firewall_myservices+="22/tcp"
# firewall_allowservices="any"
```

This configuration will allow incoming connections on `tcp` port `22` or `ssh` from `any` IPv4 or IPv6 addresses.
If this is the first time configuration, and the system is on a remote location, it is best to reboot the system to load the kernel modules properly:

```
# reboot
```

Or in case new rules are added run the following commands to restart the `ipfw` service:

```
# service ipfw restart
```

For an example if we want to allow incoming traffic for `tcp` port `443` or `https` run the following commands:

```
# firewall_myservices+="443/tcp"
firewall_myservices: 22/tcp -> 22/tcp 443/tcp
# service ipfw restart
Flushed all rules.
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00300 deny ip from 127.0.0.0/8 to any
00400 deny ip from any to ::1
00500 deny ip from ::1 to any
00600 allow ipv6-icmp from :: to ff02::/16
00700 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 allow ipv6-icmp from any to any icmp6types 1
01000 allow ipv6-icmp from any to any icmp6types 2,135,136
00000 check-state :default
01200 allow tcp from me to any established
00000 allow tcp from me to any setup keep-state :default
00000 allow udp from me to any keep-state :default
00000 allow icmp from me to any keep-state :default
00000 allow ipv6-icmp from me to any keep-state :default
01700 allow udp from 0.0.0.0 68 to 255.255.255.255 67 out
01800 allow udp from any 67 to me 68 in
01900 allow udp from any 67 to 255.255.255.255 68 in
02000 allow udp from fe80::/10 to me 546 in
02100 allow icmp from any to any icmptypes 8
02200 allow ipv6-icmp from any to any icmp6types 128,129
02300 allow icmp from any to any icmptypes 3,4,11
02400 allow ipv6-icmp from any to any icmp6types 3
02600 allow tcp from any to me 22
02700 allow tcp from any to me 443
65000 count ip from any to any
65100 deny { tcp or udp } from any to any 135-139,445 in
65200 deny { tcp or udp } from any to any 1026,1027 in
65300 deny { tcp or udp } from any to any 1433,1434 in
65400 deny ip from any to 255.255.255.255
65500 deny ip from any to 224.0.0.0/24 in
65500 deny udp from any to any 520 in
65500 deny tcp from any 80,443 to any 1024-65535 in
65500 deny ip from any to any
Firewall rules loaded.
```

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 utility is in use (Manual)

Profile Applicability:

- Level 1

Description:

FreeBSD ships with multiple firewall utilities, providing uses with options to best suit their environment. This section provides guidance to ensure that only one firewall utility is implemented.

Rationale:

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:

```
# sysrc -q -n firewall_enable | grep 'YES'
# sysrc -q -n ipfilter_enable | grep 'YES'
# sysrc -q -n pf_enable | grep 'YES'

At least one should return 'YES'
```

Remediation:

Run the following script to ensure that a single firewall utility is in use on the system. If more than one firewall utility was found to be running then all other services except the desired one should be stopped and disabled.
For `ipfilter` run:

```
# service ipfilter stop
# service ipfilter disable
```

For `ipfw` run:

```
# service firewall stop
# service firewall disable
```

For `pf` run:

```
# service pf stop
# service pf disable
```

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

4 Access, Authentication and Authorization

This section provides guidance to secure access, authentication, and authorization controls for job schedulers and users.

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 used to execute batch jobs on the system and is enabled by default on FreeBSD. `cron` must be running to ensure system maintenance jobs, such as security monitoring, are executed.

4.1.1.1 Ensure permissions on /etc/crontab are configured (Automated)

Profile Applicability:

- Level 1

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 respectively `0/root` and `0/wheel`; `Access` does not grant permissions to `group` or `other` :

```
# stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: { %g/ %Sg)' /etc/crontab
Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:wheel /etc/crontab
# chmod og-rwx /etc/crontab
```

Default Value:

```
Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

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

4.1.1.2 Ensure permissions on /etc/cron.d are configured (Automated)

Profile Applicability:

- Level 1

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 respectively `0/root` and `0/wheel`; `Access` does not grant permissions to `group` or `other`:

```
stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: { %g/ %Sg)' /etc/cron.d
Access: (40755/drwxr-xr-x)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:wheel /etc/cron.d/
# chmod og-rwx /etc/cron.d/
```

Default Value:

```
Access: (40755/drwxr-xr-x)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

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 crontab is restricted to authorized users (Manual)

Profile Applicability:

- Level 1

Description:

`crontab` is the program used to install, deinstall, or list the tables that drive the cron daemon. Each user can have their crontab, and though these are files in `/var/cron/tabs`, they are not intended to be edited directly.

If the `/var/cron/allow` file exists, you must be listed (one user per line) therein to be allowed to use this command. If the `/var/cron/allow` file does not exist but the `/var/cron/deny` file does exist, then you must not be listed in the `/var/cron/deny` file to use this command.

If both files exist, `/var/cron/allow` precedents. This means that `/var/cron/deny` is not considered when using the crontab.

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.

Regardless of the existence of any of these files, the root administrative user is always allowed to set up a crontab.

If the files `/var/cron/allow` and `/var/cron/deny` exist, they must be world-readable. If they are not, cron will only allow access to all users once the permissions are fixed.

Under the `/var/cron/tabs` directory, there is one file for each user's crontab. Users cannot 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.

Note:

- Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user
- The files `/var/cron/allow` and `/var/cron/deny`, if they exist, only control 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 `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 `/var/cron/allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root`
- Is group owned by the group `wheel`

```
stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: { %g/ %Sg)'
/var/cron/allow
Access: (100640/-rw-r-----)  Uid: ( 0/ root) Gid: { 0/ wheel)
```

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 `wheel`

```
# [ -e "/var/cron/deny" ] && stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su)
Gid: { %g/ %Sg)' /var/cron/deny
Access: (100640/-rw-r-----)  Uid: ( 0/ root) Gid: { 0/ wheel)

-OR-
Nothing is returned
```

Remediation:

-IF- cron is installed on the system:
Run the following commands to:

- Create `/var/cron/allow` if it doesn't exist
- Change owner or user `root`
- Change group owner to group `wheel`
- Change mode to `640` or more restrictive

```
# [ ! -e "/var/cron/allow" ] && touch /var/cron/allow
# chown root:wheel /var/cron/allow
# chmod u-x,g-wx,o-rwx /var/cron/allow
```

Run the following commands to:
-IF- `/var/cron/deny` exists:

- Change owner or user `root`
- Change group owner to group `wheel`
- Change mode to `640` or more restrictive

```
# [ -e "/var/cron/deny" ] && chown root:wheel /var/cron/deny
# [ -e "/var/cron/deny" ] && chmod u-x,g-wx,o-rwx /var/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

The `at` daemon works with the cron daemon to allow non-privileged users to submit one-time-only jobs at their convenience. `at` is a command-line utility used to schedule a job for later execution. `at` is available in the FreeBSD base system.

4.1.2.1 Ensure at is restricted to authorized users (Manual)

Profile Applicability:

- Level 1

Description:

The `at` utility allows some moderately complex time specifications. It accepts times of the form HHMM or HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) As an alternative, the following keywords may be specified: midnight, noon, or teatime (4pm) and time-of-day may be suffixed with AM or PM for running in the morning or the evening. The day on which the job is to be run may also be specified by giving a date in the form month-name day with an optional year, or giving a date of the forms DD.MM.YYYY, DD.MM.YY, MM/DD/YYYY, MM/DD/YY, MMDDYYYY, or MMDDYY. The specification of a date must follow the specification of the time of day. Time can also be specified as: [now] + count time-units, where the time-units can be minutes, hours, days, weeks, months or years and at may be told to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

For example, to run a job at 4pm three days from now, use at 4pm + 3 days, to run a job at 10:00am on July 31, use at 10am Jul 31 and to run a job at 1am tomorrow, use at 1am tomorrow.

The superuser may use these commands in any case. For other users, permission to use at is determined by the files `/var/at/at.allow` and `/var/at/at.deny`.

If the file `/var/at/at.allow` exists, only usernames mentioned in it are allowed to use at. In these two files, a user is considered to be listed only if the user name has no blank or other characters before it on its line and a newline character immediately after the name, even at the end of the file. Other lines are ignored and may be used for comments.

If `/var/at/at.allow` does not exist, `/var/at/at.deny` is checked, every username not mentioned in it is then allowed to use at.

If neither exists, only the superuser is allowed use of at. This is the default configuration.

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:

Run the following command to verify `/var/at/at.allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root` or `daemon`
- Is group owned by the group `wheel`

```
stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: { %g/ %Sg)'
/var/at/at.allow
Access: (100640/-rw-r-----)  Uid: ( 0/ root) Gid: { 0/ wheel)
or
Access: (100640/-rw-r-----)  Uid: ( 1/ daemon) Gid: { 0/ wheel)
```

Verify mode is `640` or more restrictive, owner is `root` or `daemon`, and group is `wheel`
Run the following command to verify `at.deny` doesn't exist, **-OR-** is:

- Mode `0640` or more restrictive
- Owned by the user `root` or `daemon`
- Group owned by the group `wheel`

```
# [ -e "/var/at/at.deny" ] && stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su)
Gid: { %g/ %Sg)' /var/at/at.allow
Access: (100640/-rw-r-----)  Uid: ( 0/ root) Gid: { 0/ wheel)
or
Access: (100640/-rw-r-----)  Uid: ( 1/ daemon) Gid: { 0/ wheel)
-OR-
Nothing is returned
```

If a value is returned, verify mode is 640 or more restrictive, owner is `root` o `daemon`, and group is `wheel`

Remediation:

Run the following script to:

- `/var/at/at.allow`:
  - Create the file if it doesn't exist
  - Change owner or user `root` or `daemon`
  - Change group to `wheel`
  - Change mode to `640` or more restrictive
- **-IF-** `/var/at/at.deny` exists:
  - Change owner or user `root`
  - Change group to `wheel`
  - Change mode to `640` or more restrictive

```
#!/bin/sh

{
   [ ! -e "/var/at/at.allow" ] && touch /var/at/at.allow
   chown root:wheel /var/at/at.allow
   chmod u-x,g-wx,o-rwx /var/at/at.allow
   [ -e "/var/at/at.deny" ] && chown root:wheel /var/at/at.deny
   [ -e "/var/at/at.deny" ] && chmod u-x,g-wx,o-rwx /var/at/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 remote access is required, if remote access is **not** required this section can be skipped.
- It is recommended that these options only be used if they're needed and fully understood. If these options are configured in accordance with local site policy, they should be accounted for when following the recommendations in this section.
- The audits of the running 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

Command to enable the SSH daemon:

```
# service sshd enable
```

Command to re-load the SSH daemon configuration:

```
# service sshd reload
```

4.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Manual)

Profile Applicability:

- Level 1

Description:

The file `/etc/ssh/sshd_config` contains configuration specifications for `sshd`.

Rationale:

Configuration specifications for `sshd` must be protected from unauthorized changes by non-privileged users.

Audit:

Run the following script and verify `/etc/ssh/sshd_config` are:

- Mode `0644` or more restrictive
- Owned by the `root` user
- Group owned by the group `wheel`.

```
# stat -Lf 'Access: (%Lp/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)'
/etc/ssh/sshd_config
```

Remediation:

Run the following script to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chmod u-x,og-rwx /etc/ssh/sshd_config
# chown root:wheel /etc/ssh/sshd_config
```

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 (Manual)

Profile Applicability:

- Level 1

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 wheel and mode 0600 or more restrictive

- OR -

- owned by the group designated to own openSSH private keys and mode 0600 or more restrictive

```
# find /etc/ssh  -type f -name "ssh_host_*_key" -exec stat -Lf 'Access:
(%Lp/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg) File: %N' {} \;
```

Remediation:

Run the following script to set mode, ownership, and group on the private SSH host key files:

```
# find /etc/ssh  -type f -name "ssh_host_*_key" -exec sh -c "chown -vv
root:wheel {}; chmod -vv 600 {}" \;
```

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 (Manual)

Profile Applicability:

- Level 1

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 `wheel` group:

```
# find /etc/ssh  -type f -name "ssh_host_*_key.pub" -exec stat -Lf 'Access:
(%Lp/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg) File: %N' {} \;
```

Remediation:

Run the following script to set mode, ownership, and group on the public SSH host key files:

```
# find /etc/ssh  -type f -name "ssh_host_*_key.pub" -exec sh -c "chown -vv
root:wheel {}; chmod -vv 644 {}" \;
```

Default Value:

644 0/root 0/wheel

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 (Manual)

Profile Applicability:

- Level 1

Description:

Several options are available to limit which users and groups can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- `AllowUsers`: The `AllowUsers` variable allows the system administrator to allow 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 allows the system administrator to allow specific groups of users to `SSH` into the system. The list consists of space-separated group names. This variable does not recognize numeric group IDs.
- `DenyUsers`: The `DenyUsers` variable allows the system administrator to deny specific users the ability 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 denying a user access from a particular host, the entry can be specified as user@host.
- `DenyGroups`: The `DenyGroups` variable allows the system administrator to deny specific groups of users access to the system via SSH. The list consists of space-separated group names; this variable does not recognize numeric group IDs.

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 commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Ei
'^\s*(allow|deny)(users|groups)\s+\S+(\s+.*)?$'

# grep -Ei '^\s*(allow|deny)(users|groups)\s+\S+(\s+.*)?$'
/etc/ssh/sshd_config
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>
-OR-
allowgroups <grouplist>
-OR-
denyusers <userlist>
-OR-
denygroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter above any `Include` entries as follows:

```
AllowUsers <userlist>
-OR-
AllowGroups <grouplist>
-OR-
DenyUsers <userlist>
-OR-
DenyGroups <grouplist>
```

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 (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep banner
```

Verify the output matches:

```
banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
Banner /etc/issue.net
```

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 (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep ciphers
```

Verify that output does not contain any of the following weak ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
```

Remediation:

Edit the /etc/ssh/sshd_config file and add/modify the `Ciphers` line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a `-` above any `Include` entries:
Example:

```
Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-
cbc@lysator.liu.se
```

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

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 (Manual)

Profile Applicability:

- Level 1

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="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep clientaliveinterval
```

Example output:

```
clientaliveinterval 0
```

Run the following command and verify `ClientAliveCountMax` is greater than zero:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep clientalivecountmax
```

Example output:

```
clientalivecountmax 3
```

Run the following command:

```
# grep -Pis '^\h*ClientAliveCountMax\h+"?0\b' /etc/ssh/sshd_config
/etc/ssh/sshd_config.d/*.conf

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters above any `Include` entries according to site policy.
Example:

```
ClientAliveInterval 15
ClientAliveCountMax 3
```

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 (Manual)

Profile Applicability:

- Level 1

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 allows tunneling X11 traffic through the connection to enable remote graphic connections.
- `ssh-agent` is a program that holds private keys used for public key authentication. Environment variables allow the agent to 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 to add encryption to legacy applications and pass through firewalls. Some system administrators and IT professionals use it to open 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 other users on the X11 server could compromise the remote X11 servers of users who are logged in via SSH with X11 forwarding. Even if X11 forwarding is disabled, users can always install their forwarders.

Anyone with root privileges on the intermediate server can use ssh-agent to authenticate to other servers for free.

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 potential risk if 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 security support. By tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without modifying the applications.

Audit:

Run the following command:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i disableforwarding
```

Verify the output matches:

```
disableforwarding yes
```

Run the following command:

```
# grep -Ei '^\s*DisableForwarding\s+\"?no\"?\b' /etc/ssh/sshd_config
```

Nothing is returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
DisableForwarding yes
```

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 HostbasedAuthentication is disabled (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep hostbasedauthentication
```

Verify the output matches:

```
hostbasedauthentication no
```

Run the following command:

```
# grep -Ei '^\s*HostbasedAuthentication\s+"?yes"?\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
HostbasedAuthentication no
```

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

4.2.10 Ensure sshd IgnoreRhosts is enabled (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep ignorerhosts
```

Verify the output matches:

```
ignorerhosts yes
```

Run the following command:

```
# grep -Ei '^\s*IgnoreRhosts\s+"?no"?\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Include entries as follows:

```
IgnoreRhosts yes
```

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

4.2.11 Ensure sshd KexAlgorithms is configured (Manual)

Profile Applicability:

- Level 1

Description:

Key exchange is any cryptography method that exchanges cryptographic keys between two parties, allowing the 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 comply 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 and verify that the output does not contain any of the listed weak Key Exchange algorithms:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the `KexAlgorithms` line to contain a comma-separated list of the site unapproved (weak) KexAlgorithms preceded with a `-` above any `Include` entries:
Example:

```
KexAlgorithms -diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-
hellman-group-exchange-sha1
```

Default Value:

kexalgorithms sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,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

References:

1. 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, T1557.000	TA0006	M1041

4.2.12 Ensure sshd LoginGraceTime is configured (Manual)

Profile Applicability:

- Level 1

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 on the SSH server and 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 or `1m`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep logingracetime

logingracetime 60
```

Run the following command and verify the output:

```
# grep -E '^\s*LoginGraceTime\s+"?(0|6[1-9]|[7-9][0-9]|[1-9][0-9][0-
9]+|[^1]m)\b' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
LoginGraceTime 60
```

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

4.2.13 Ensure sshd LogLevel is configured (Manual)

Profile Applicability:

- Level 1

Description:

`LogLevel` gives the verbosity level 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 users' privacy 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 critical security information and may violate users' privacy. Also, improper usage of `DEBUG` may quickly fill up the available hard disk space, making the system unavailable.

The `INFO` level is the basic level that only records the login activity of SSH users. In many situations, such as Incident Response, it is essential to determine when a particular user was active on a system. The logout record can eliminate disconnected users, which helps narrow the field.

The `VERBOSE` level specifies that login and logout activity and the key fingerprint for any SSH key used for login will be logged. This information is essential for SSH key management, especially in legacy environments.

Audit:

Run the following command and verify that the output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep loglevel

loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -Ei '^\s*loglevel\s+' /etc/ssh/sshd_config | grep -Evi
'(VERBOSE|INFO)'

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
LogLevel VERBOSE

-OR-

LogLevel INFO
```

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	

4.2.14 Ensure sshd MACs are configured (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i "MACs"
```

Verify that output does not contain any of the listed weak MAC algorithms:

```
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 unapproved (weak) MACs preceded with a `-` above any `Include` entries:
Example:

```
MACs -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
```

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

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

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

4.2.15 Ensure sshd MaxAuthTries is configured (Manual)

Profile Applicability:

- Level 1

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 output `MaxAuthTries` is `4` or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep maxauthtries

maxauthtries 6
```

Note: If Include locations besides, or in addition to /etc/ssh/sshd_config.d/*.conf and/or Match set statements are used in your environment, those locations should be checked for the correct configuration as well.
Run the following command and verify that the output:

```
# grep -Pis '^\s*maxauthtries\s+"?([5-9]|[1-9][0-9]+)\b' /etc/ssh/sshd_config

Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxAuthTries 4
```

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

4.2.16 Ensure sshd MaxSessions is configured (Manual)

Profile Applicability:

- Level 1

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 output `MaxSessions` is `10` or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i maxsessions

maxsessions 10
```

Run the following command and verify the output:

```
grep -E '^\s*MaxSessions\s+"?(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+)\b'
/etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxSessions 10
```

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	

4.2.17 Ensure sshd MaxStartups is configured (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i ^maxstartups
```

Verify that output `MaxStartups` is `10:30:60` or more restrictive:

```
maxstartups 10:30:100
```

Run the following command and verify the output:

```
# grep -E '^\s*maxstartups\s+"?(((1[1-9]|[1-9][0-9][0-9]+):([0-9]+):([0-
9]+))|(([0-9]+):(3[1-9]|[4-9][0-9]|[1-9][0-9][0-9]+):([0-9]+))|(([0-9]+):([0-
9]+):(6[1-9]|[7-9][0-9]|[1-9][0-9][0-9]+)))\b' /etc/ssh/sshd_config
/etc/ssh/sshd_config.d/*.conf
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
MaxStartups 10:30:60
```

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	

4.2.18 Ensure sshd PermitEmptyPasswords is disabled (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep permitemptypasswords
```

Verify the output matches:

```
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -E '^\s*PermitEmptyPasswords\s+"?yes\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitEmptyPasswords no
```

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

4.2.19 Ensure sshd PermitRootLogin is disabled (Manual)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep permitrootlogin
```

Verify the output matches:

```
permitrootlogin no
```

Run the following command:

```
# grep -E '^\s*PermitRootLogin\s+"?(yes|prohibit-password|forced-commands-
only)"?\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any `Include` entries as follows:

```
PermitRootLogin no
```

Default Value:

PermitRootLogin no

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

4.2.20 Ensure sshd PermitUserEnvironment is disabled (Automated)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep permituserenvironment
```

Verify the output matches:

```
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -E '^\sPermitUserEnvironment\syes\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Include entries as follows:

```
sed -i '' 's|^#PermitUserEnvironment.*|PermitUserEnvironment no'
/etc/ssh/sshd_config
```

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

4.2.21 Ensure sshd UsePAM is enabled (Automated)

Profile Applicability:

- Level 1

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i usepam
```

Verify the output matches:

```
usepam yes
```

Run the following command:

```
# grep -Ei '^\s*UsePAM\s+"?no"?\b' /etc/ssh/sshd_config
```

Nothing should be returned.

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
sed -i '' -e 's|^#UsePAM.*yes|UsePAM yes|g' /etc/ssh/sshd_config
```

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

Various tools allow 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 determines the user name 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 policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, configured via the file `/usr/local/etc/sudoers` and any entries in `/usr/local/etc/sudoers.d`.

4.3.1 Ensure sudo is installed (Manual)

Profile Applicability:

- Level 1

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 `/usr/local/etc/sudoers` and any entries in `/usr/local/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:

```
# pkg info sudo

pkg: No package(s) matching sudo
```

Remediation:

Run the following command to install sudo

```
# pkg install -y 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.	●	●	●

4.3.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1

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 -rEi '^\s*Defaults\s+([^#\n\r]+,)?use_pty(,\s*\s+\s*)*\s*(#.*)?$'
/usr/local/etc/sudoers*
```

Remediation:

Edit the file `/usr/local/etc/sudoers` with `visudo` or a file in `/usr/local/etc/sudoers.d/` with `visudo -f` <*PATH_TO_FILE*> and add the following line:

```
Defaults use_pty
```

Note:

- sudo will read each file in `/usr/local/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, `/usr/local/etc/sudoers.d/01_first` will be parsed before `/usr/local/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/usr/local/etc/sudoers.d/1_whoops` would be loaded after `/usr/local/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 (Manual)

Profile Applicability:

- Level 1

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: incorrectly Editing the `sudo` configuration can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

If not correctly managed, the creation of additional log files can exhaust disk space. Configure `logrotate` to manage the sudo log in accordance with your local policy.

Audit:

Run the following command to verify that sudo configures a custom log file.

```
# grep -rEsi
"^\s*Defaults\s+([^#]+,\s*)?logfile\s*=\s*(\"|\')?\S+(\"|\')?(,\s*\S+\s*)*\s*
(#.*)?$" /usr/local/etc/sudoers*
```

Example output:

```
Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/usr/local/etc/sudoers` or a file in `/usr/local/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 `/usr/local/etc/sudoers.d`, skipping file names that end in `~` or contain a `.` character to avoid causing problems with the package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/usr/local/etc/sudoers.d/01_first` will be parsed before `/usr/local/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/usr/local/etc/sudoers.d/1_whoops` would be loaded after `/usr/local/etc/sudoers.d/10_second`.
- 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 safely, 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 asking you 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 (Manual)

Profile Applicability:

- Level 2

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.

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 `/usr/local/etc/sudoers` and `/usr/local/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*NOPASSWD" /usr/local/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 (Manual)

Profile Applicability:

- Level 1

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 `/usr/local/etc/sudoers` and `/usr/local/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*\!authenticate" /usr/local/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 (Manual)

Profile Applicability:

- Level 1

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 -roE "timestamp_timeout=[0-9]*" /usr/local/etc/sudoers*
```

If there is no `timestamp_timeout` configured in `/usr/local/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 (Manual)

Profile Applicability:

- Level 1

Description:

The `su` command allows a user to run a command or shell as another user. 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 and verify the output matches the line:

```
# grep -Ei
'^auth\s+(required|requisite)+\s+pam_group\.so\s+\S+\s(group=\S+\b)'
/etc/pam.d/su

auth            requisite       pam_group.so            no_warn group=wheel
root_only fail_safe ruser
```

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:

```
# pw groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:

```
auth           requisite      pam_group.so           no_warn group=sugroup
root_only fail_safe ruser
```

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 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.

4.4.1.1 Configure pam_passwdqc module

The `pam_passwdqc.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 using the module arguments.

4.4.1.1.1 Ensure password length is configured (Manual)

Profile Applicability:

- Level 1

Description:

`minlen` - Minimum acceptable size for the new password.

Below are the minimum allowed password lengths for different kinds of passwords/passphrases. The keyword `disabled` can be used to disallow passwords of a given kind regardless of length. Each subsequent number must be no larger than the preceding one.

N0 is used for passwords consisting of characters from one character class only. The character classes are digits, lower-case, upper-case, and other characters. There is also a special class for non-ASCII characters that cannot be classified but are assumed to be non-digits.

N1 is used for passwords consisting of characters from two character classes that do not meet the requirements for a passphrase.

N2 is used for passphrases. A passphrase must consist of sufficient words.

N3 and **N4** are used for passwords of characters from three and four-character classes, respectively.

In addition to being sufficiently long, passwords must contain enough different characters for the character classes and the minimum length they have been checked against.

Rationale:

Strong passwords protect systems from being hacked through brute-force methods.

Audit:

Run the following command to verify that the password length is 14 or more characters and conforms to local site policy:

```
# grep -Ei -- '\bminlen=.*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b' /etc/pam.d/*
```

Example output:

```
/etc/pam.d/passwd:password     requisite      pam_passwdqc.so
        enforce=everyone minlen=disabled,14,12,8,6
```

Verify returned value(s) are no less than 14 characters for N1 and meet local site policy
Run the following command to verify that minlen is not set, or is 14 or more characters, and conforms to local site policy:

```
grep -Ei --
'^\s*password\s+(requisite|required|sufficient)\s+pam_passwdqc\.so.*minlen=.*
([0-9]|1[0-3])' /etc/pam.d/*

Nothing should be returned
```

Note:

- settings should be configured in only **one** location for clarity

Remediation:

Create or modify the file /etc/pam.d/passwd and add or modify the following line to set the password length of 14 or more characters. Ensure that password length conforms to local site policy:
Example:

```
password       requisite      pam_passwdqc.so        enforce=everyone
minlen=disabled,14,12,8,6
```

Default Value:

minlen = 8

References:

1. pam_passwdqc(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

4.4.1.1.2 Ensure password quality is enforced for the root user (Manual)

Profile Applicability:

- Level 1

Description:

If the `pam_passwdqc enforce=everyone` option is enabled, the module will return an error on the failed check, even if the user changing the password is the root.

This option is off by default, meaning only the message about the failed check is printed, but `root` can change the password anyway.

Note: The `root` user is not asked for an old password, so the checks that compare the old and new passwords are not performed.

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 `enforce_for_root` option is enabled in a pwquality configuration file:

```
# grep -Ei -- 'pam_passwdqc.so.*\benforce=everyone\b' /etc/pam.d/*
```

Example output:

```
/etc/pam.d/passwd:password    requisite    pam_passwdqc.so
enforce=everyone minlen=disabled,14,12,8,6
```

Remediation:

Create or modify the file `/etc/pam.d/passwd` and add or modify the following line to ensure that password quality is enforced for everyone including `root` user:
Example:

```
password        requisite       pam_passwdqc.so         enforce=everyone
minlen=disabled,14,12,8,6
```

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.		●	●

4.4.1.2 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.

4.4.1.2.1 Ensure pam_unix does not include nullok (Manual)

Profile Applicability:

- Level 1

Description:

The `nullok` argument overrides the default action of `pam_unix.so` to prevent users from gaining access to a service if their official password is blank.

Rationale:

A strong password is essential to help 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 -E --
'^\s*(auth|account|password|session)\s+(requisite|required|sufficient)\s+pam_
unix\.so\b' /etc/pam.d/{passwd,system} | grep -E -- '\bnullok\b'
```

Output should be similar to:

```
/etc/pam.d/system:account      required       pam_unix.so
/etc/pam.d/system:password     required       pam_unix.so           no_warn
try_first_pass
```

Remediation:

Run the following script to verify that the `system` and `password` files don't include the `nullok` option on the `pam_unix.so` module:

```
#  grep -E --
'^\s*(auth|account|password|session)\s+(requisite|required|sufficient)\s+pam_
unix\.so\b' /etc/pam.d/{passwd,system} | grep -E -- '\bnullok\b'
```

Example output:

```
/etc/pam.d/passwd:password     required       pam_unix.so            no_warn
try_first_pass nullok
/etc/pam.d/system:auth         required       pam_unix.so            no_warn
try_first_pass nullok
```

- IF - any line is returned with `nullok`, run the following script:

```
# find /etc/pam.d -type f -exec sed -i '' -E 's|[[:space:]]?nullok||g' {} \;
```

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

4.5 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.conf` 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 (Manual)

Profile Applicability:

- Level 1

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` algorithms provide a stronger hash than other algorithms used by FreeBSD 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:

Verify password hashing algorithm is sha512:
Run the following command to verify the hashing algorithm is `sha512` in `/etc/login.conf`:

```
# grep -E -- '^\s:passwd_format=sha512:' /etc/login.conf
        :passwd_format=sha512:\
```

Remediation:

Set password hashing algorithm to sha512.
Edit `/etc/login.conf` and edit or add a line like the following for the `default` configuration:

```
:passwd_format=sha512:
```

After editing the file regenerate the `login.conf.db` with the command:

```
# cap_mkdb /etc/login.conf
```

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 group passwords be updated to use the stronger hashing algorithm.

References:

1. NIST SP 800-53 Rev. 5: IA-5

Additional Information:

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.

```
# for i in $(awk -F: '($3>=1000)&&($1!="nobody"){print $1}' /etc/passwd); do
pw usermod -n $i -p +1d; done
```

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

Description:

The `passwordtime` parameter in `/etc/login.conf` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `passwordtime` 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 `passwordtime` conforms to site policy (no more than 365 days):

```
# grep -E -- '^\s:passwordtime=' /etc/login.conf
```

If nothing is returned that means that password expiry is not active.

Remediation:

Set the `passwordtime` parameter to conform to site policy in `/etc/login.conf` and add something similar to the following in the `default` class :

```
:passwordtime=365d:
```

After editing the file regenerate the `login.conf.db` with the command:

```
# cap_mkdb /etc/login.conf
```

Modify user parameters for all users with a password set to match:

```
# # for i in $(awk -F: '($3>=1000)&&($1!="nobody"){print $1}' /etc/passwd);
do pw usermod -n $i -p +365d; done
```

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	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 (Manual)

Profile Applicability:

- Level 1

Description:

The `warnpassword` parameter in `/etc/login.conf` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `warnpassword` parameter be set to 7 or more days.

Rationale:

Providing a warning that a password will expire 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 -E -- '^\s:warnpassword=' /etc/login.conf
```

Remediation:

Set the `warnpassword` parameter to `7d` in `/etc/login.conf` for the `default` class:

```
:warnpassword=7d:
```

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

4.5.2 Configure root and system accounts and environment

4.5.2.1 Ensure default group for the root account is GID 0 (Manual)

Profile Applicability:

- Level 1

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`:

```
# pw 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 (Manual)

Profile Applicability:

- Level 1

Description:

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In FreeBSD, the default permissions for any newly created directory is 0755 (`rwxr-xr-x`), and for any newly created file it is 0644 (`rw-r--r--`). The `umask` modifies the default FreeBSD 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/.profile` - Is executed to configure the root users' shell before the initial command prompt. **Is only read by login shells.**
- `/root/.shrc` - 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/.profile`
2. `/root/.shrc`
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 `755 (drwxr-xr-x)`, and a newly created file's permissions be `644 (rw-r--r--)`, or more restrictive:

```
grep -Esi -- '^\s*umask\s+(([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/.profile /root/.shrc

Nothing should be returned
```

Remediation:

Edit `/root/.profile` and `/root/.shrc` 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 (Manual)

Profile Applicability:

- Level 1

Description:

Several accounts are 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 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: '($1!~/^(root|toor|uucp)$/ || $3 == 65533) &&
$7!~/^(\/usr)?\/sbin\/nologin$/ { 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: '($2!="*" && $7~/^(\/usr)?\/sbin\/nologin$/) { print $1 }'
/etc/master.passwd
```

Verify no results are returned.

Remediation:

System accounts
Set the shell for any accounts returned by the audit to `nologin`:

```
# pw usermod -s $(command -v nologin) <user>
```

Disabled accounts
Lock any non-root accounts returned by the audit:

```
# pw lock <user>
```

References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

Additional Information:

The `root` user is 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

4.5.3 Configure user default environment

4.5.3.1 Ensure nologin is not listed in /etc/shells (Manual)

Profile Applicability:

- Level 2

Description:

`/etc/shells` is a text file that contains the full pathnames of valid login shells. This file is consulted by `chsh` and is available to be queried by other programs.

Be aware that there are programs that 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 umask is configured (Manual)

Profile Applicability:

- Level 1

Description:

The user file-creation mode mask (`umask`) determines the file permission for newly created directories and files. In FreeBSD, the default permission for any newly created directory is 0755 (`rwxr-xr-x`), and for any newly created file, it is 0644 (`rw-r--r--`). The `umask` modifies the default FreeBSD 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 three or four digits. ie `umask 022` or `umask 027`. If a four-digit umask is used, the first digit is ignored. The remaining three digits affect 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`. i.e. 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 use the login class capability database `/etc/login.conf` 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`, (`.cshrc` or `.shrc`), in their home directory.

Setting the default umask:

- Login class capability database:
  - will set the `umask` according to the system default in `/etc/login.conf` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions, etc.
  - The `umask=<mask>` value in the `/etc/login.conf` file is interpreted as Octal
- `System Wide Shell Configuration File`:
  - `/etc/profile` - used to set system-wide environmental variables on users' shells. The variables are sometimes the same ones in the `.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/csh.cshrc` - System-wide version of `.cshrc`.

User Shell Configuration Files:

- `~/.profile` - This is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- `~/.shrc` - Is executed for interactive shells if the user's shell is set to `/bin/sh`. **only read by a shell that's both interactive and non-login**
- `~/.cshrc` - Is executed for interactive shells if the user's shell is set to `/bin/csh`. **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. In the file `/etc/login.conf`

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 `755 (drwxr-xr-x)`, and a newly created file's permissions be `644 (rw-r--r--)`, or more restrictive:

```
#!/bin/sh

# Files to check
files="/etc/login.conf /etc/profile.d/* /etc/csh.cshrc"

# Pattern to search for (umask 022 or 22)
pattern="umask.*0?22"

# Iterate over each file
for file in $files; do
    if [ -f "$file" ]; then
        # Check if the umask is set to 022 or 22 in the file
        if grep -qE "$pattern" "$file"; then
            echo "Correct umask (022 or 22) found in $file"
        else
            echo "WARNING: Correct umask (022 or 22) not found in $file"
        fi
    else
        echo "File $file does not exist."
    fi
done
```

Remediation:

In case proper `umask` is not configured system-wide necessary measurements should be taken to define them in `/etc/login.conf` or system-wide shell configurations like a file in `/etc/profile.d/*.sh` or `/etc/csh.cshrc`.
Note:

- This method only applies to Bourne Again shell and C Shell. If other shells are supported on the system, it is recommended that their configuration files also be checked

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, (.shrc), 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 FreeBSD.

It is recommended that `syslog` be used for logging and `auditd` be used for auditing 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 Chronyd manual page for more information on configuring `chrony` or Clock Synchronization with NTP for more information on configuring `ntpd`.

All logs described in this section must be monitored regularly 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 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

Configure logging services to prevent information leaks and aggregate logs on a remote server so they can be reviewed in case of a system compromise. A centralized log server provides a single entry point for further analysis, monitoring, and filtering.

Security principles 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 `syslogd`.

- If your organization uses an enterprise-wide logging system completely outside of `syslogd`, then the following recommendations do not directly apply. However, follow the principles of the recommendations regardless of what solution is implemented. If an enterprise logging solution is deployed separate from `syslogd`, review the following recommendations to determine exactly what applies.
- If your organization uses anything other than `syslogd`, consider how the recommendations may or may not apply to it.

What is not covered:

- Enterprise logging systems not utilizing `syslogd`. As logging is very situational and dependent on the local environment, not everything can be covered here.
- Apply Transport Layer Security to all remote logging functionality. `syslogd` does not support secure transport and must be configured with other tools that use a VPN or tools like `spiped` or `stunnel`. External tools like `rsyslog` or syslog-ng support remote logging with an encryption facility.
- The log server. There are many reasons for a centralized log server (and for 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 syslog

The default `syslog` logging mechanism may be used.

Note: This section only applies if `syslogd` is the chosen method for client-side logging. Do not apply this section if other tools are used.

5.1.1.1 Ensure syslog is installed (Manual)

Profile Applicability:

- Level 1

Description:

The `syslogd` software is recommended for FreeBSD and is shipped with the base system.

Rationale:

The `syslogd` utility reads and logs messages to the system console, log files, other machines, and/or users as specified by its configuration file.

Audit:

Run the following command to verify that `syslogd` is enabled at startup.

```
# sysrc syslogd_enable
```

Verify the output matches:

```
syslogd_enable: YES
```

Remediation:

Run the following command to activate and start the `syslogd` service in the highly unlikely case that the service was disabled:

```
# service syslogd start
```

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 syslogd service is enabled (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the `syslogd` service is enabled.

Rationale:

If the `syslogd` service is not enabled to start on boot, the system will not capture logging events.

Audit:

- IF - `syslogd` is being used for logging on the system:
Run the following command to verify `syslogd` is enabled:

```
# sysrc syslogd_enable
```

Verify the output matches:

```
syslogd_enable: YES
```

Remediation:

Run the following command to enable `syslogd`:

```
# service syslogd enable
```

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 syslogd default file permissions are configured (Manual)

Profile Applicability:

- Level 1

Description:

`syslogd` will create log files that do not already exist on the system. This setting controls what permissions will be applied to these newly created files. These settings are handled by a different tool `newsyslog` which also handles the logfile rotation and retention.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Impact:

The system's global mask could be overridden to make the file permissions stricter than what is configured in newsyslog.conf with the mode directive. Thus, it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/newsyslog.conf`, `/etc/newsyslog.conf.d/*conf`, `/use/local/etc/newsyslog.conf.d/*conf` files.

Audit:

Run the following command:

```
# grep -Ei '\s\s[0,2,4,6,7][0,2,4,6,7][0,2,4,6,7]\b' /etc/newsyslog.conf
/etc/newsyslog.conf.d/*
```

Verify the output of the second field is 644 or more restrictive:

```
/etc/newsyslog.conf:/var/log/all.log                  600  7    *     @T00  J
/etc/newsyslog.conf:/var/log/auth.log                 600  7    1000 @0101T JC
/etc/newsyslog.conf:/var/log/console.log                   600  5    1000  *
J
/etc/newsyslog.conf:/var/log/cron                          600  3    1000  *
JC
/etc/newsyslog.conf:/var/log/daemon.log                    644  5    1000
        @0101T JC
/etc/newsyslog.conf:/var/log/daily.log                640  7    *     @T00  JN
/etc/newsyslog.conf:/var/log/debug.log                600  7    1000 *     JC
/etc/newsyslog.conf:/var/log/devd.log                 644  3    1000  *     JC
/etc/newsyslog.conf:/var/log/init.log                 644  3    1000  *     J
/etc/newsyslog.conf:/var/log/kerberos.log                  600  7    1000  *
J
/etc/newsyslog.conf:/var/log/maillog                  640  7    *     @T00  JC
/etc/newsyslog.conf:/var/log/messages                 644  5    1000  @0101T JC
/etc/newsyslog.conf:/var/log/monthly.log                   640  12   *
        $M1D0 JN
/etc/newsyslog.conf:/var/log/security                 600  10   1000  *     JC
/etc/newsyslog.conf:/var/log/utx.log                  644  3    *     @01T05 B
/etc/newsyslog.conf:/var/log/weekly.log                    640  5    *
        $W6D0 JN
/etc/newsyslog.conf.d/ftp.conf:/var/log/xferlog                         600  7
1000    *     JC
/etc/newsyslog.conf.d/lpr.conf:/var/log/lpd-errs                        644  7
1000    *     JC
/etc/newsyslog.conf.d/opensm.conf:/var/log/opensm.log                   600  7
        1000    *       J       /var/run/opensm.pid    30
/etc/newsyslog.conf.d/pf.conf:/var/log/pflog                            600  3
1000    *     JB    /var/run/pflogd.pid
/etc/newsyslog.conf.d/sendmail.conf:/var/log/sendmail.st
        640  10   *     168    BN
```

Remediation:

Edit either `/etc/newsyslog.conf` or a dedicated `.conf` file in `/etc/newsyslog.conf.d/` and set the `mode` of the specific file to `644` or more restrictive.
Restart the service:

```
# service syslogd restart
```

References:

1. See the newsyslog.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	

5.1.1.4 Ensure logging is configured (Manual)

Profile Applicability:

- Level 1

Description:

The `/etc/syslog.conf`, `/etc/syslog.d/*.conf` and `/usr/local/etc/syslog.d/*.conf` files specify logging rules 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 `syslog`, such as successful and failed su attempts, failed login attempts, root login attempts, and more.

Audit:

Review the contents of `/etc/syslog.conf`, `/etc/syslog.d/*.conf` and `/usr/local/etc/syslog.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/syslog.conf` and `/etc/syslog.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 wishes to store log data.

```
*.err;kern.warning;auth.notice;mail.crit                /dev/console
*.notice;authpriv.none;kern.debug;lpr.info;mail.crit;news.err
        /var/log/messages
security.*                                      /var/log/security
auth.info;authpriv.info                                 /var/log/auth.log
mail.info                                       /var/log/maillog
cron.*                                          /var/log/cron
!-devd
*.=debug                                        /var/log/debug.log
*.emerg                                         *
daemon.info                                     /var/log/daemon.log
# uncomment this to log all writes to /dev/console to /var/log/console.log
# touch /var/log/console.log and chmod it to mode 600 before it will work
#console.info                                   /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
# touch /var/log/all.log and chmod it to mode 600 before it will work
#*.*                                            /var/log/all.log
# uncomment this to enable logging to a remote loghost named loghost
#*.*                                            @loghost
# uncomment these if you're running inn
# news.crit                                     /var/log/news/news.crit
# news.err                                      /var/log/news/news.err
# news.notice                                   /var/log/news/news.notice
# Uncomment this if you wish to see messages produced by devd
# !devd
# *.>=notice                                    /var/log/devd.log
!*
include                                         /etc/syslog.d
include                                         /usr/local/etc/syslog.d
```

Run the following command to reload the `syslogd` configuration:

```
# service syslogd restart
```

References:

1. See the syslog.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	

5.1.1.5 Ensure syslog is configured to send logs to a remote log host (Manual)

Profile Applicability:

- Level 1

Description:

Syslog 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/syslog.conf`, `/etc/syslog.d/*.conf` and `/usr/local/etc/syslog.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):

```
# grep "^*.*[^I][^I]*@" /etc/syslog.conf /etc/syslog.d/*.conf
/usr/local/etc/syslog.d/*.conf
```

Output must include `@<FQDN or IP of remote loghost>`, for example

```
*.* @loghost.example.com
```

Remediation:

Edit the `/etc/syslog.conf` and `/etc/syslog.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.

```
*.* @loghost.example.com
```

Run the following command to reload the `syslogd` configuration:

```
# service syslogd restart
```

References:

1. See the rsyslog.conf(5) man page for more information.

Additional Information:

In addition, see the syslogd documentation for implementation details.

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

5.1.1.6 Ensure rsyslog is not configured to receive logs from a remote client (Manual)

Profile Applicability:

- Level 1

Description:

Syslog 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/rc.conf` file and verify that the system is not configured to accept incoming logs.

```
# sysrc syslogd_flags | grep -E '\-.*s'
syslogd_flags: -s
```

`-s` flags denote operation in a secure mode. Do not log messages from remote machines. If specified twice, no network socket will be opened at all, which also disables logging to remote machines.

Remediation:

If the result does not include `-s` flag, then the following commands will fix this:

```
# sysrc syslogd_flags+=" -s"
```

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 Ensure newsyslog is configured (Manual)

Profile Applicability:

- Level 1

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 files `/etc/newsyslog.conf`, `/etc/newsyslog.conf.d/*.conf` and `/usr/local/etc/newsyslog.conf.d/*.conf` is the configuration file used to rotate log files created by `syslog`.

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/newsyslog.conf`, `/etc/newsyslog.conf.d/*.conf` and `/usr/local/etc/newsyslog.conf.d/*.conf` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/newsyslog.conf`, `/etc/newsyslog.conf.d/*.conf` and `/usr/local/etc/newsyslog.conf.d/*.conf` to ensure logs are rotated according to site policy.

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
T1070, T1070.002	TA0040	M1022

5.1.3 Ensure all logfiles have appropriate access configured (Manual)

Profile Applicability:

- Level 1

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:

Log files must 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:

```
#!/bin/sh

# Define the list of log files, their expected permissions, user, and group
log_files="
/var/log/messages:640:root:wheel
/var/log/cron:640:root:wheel
/var/log/auth.log:640:root:wheel
/var/log/maillog:640:root:wheel
/var/log/xferlog:640:root:wheel
/var/log/debug.log:640:root:wheel
/var/log/console.log:640:root:wheel
/var/log/dmesg:640:root:wheel
/var/log/security:640:root:wheel
/var/log/all.log:640:root:wheel
"

# Iterate over each log file, its expected permissions, user, and group
echo "$log_files" | while IFS=: read -r file expected_perms expected_user
expected_group; do
    if [ -f "$file" ]; then
        # Get current permissions, user, and group of the file
        current_perms=$(stat -f "%Lp" "$file")
        current_user=$(stat -f "%Su" "$file")
        current_group=$(stat -f "%Sg" "$file")

        # Check if permissions are correct
        if [ "$current_perms" -ge "$expected_perms" ]; then
            echo "$file permission is set to $current_perms but should be
$expected_perms"
        fi

        # Check if user ownership is correct
        if [ "$current_user" != "$expected_user" ]; then
            echo "$file ownership is set to $current_user but should be
$expected_user"
        fi

        # Check if group ownership is correct
        if [ "$current_group" != "$expected_group" ]; then
            echo "$file group ownership is set to $current_group but should
be $expected_group"
        fi
    else
        echo "File $file does not exist."
    fi
done

echo "Log file permissions, user, and group ownership check and fix
completed."
```

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 if the remediation causes issues.

```
#!/bin/sh

# Define the list of log files, their expected permissions, user, and group
log_files="
/var/log/messages:640:root:wheel
/var/log/cron:640:root:wheel
/var/log/auth.log:640:root:wheel
/var/log/maillog:640:root:wheel
/var/log/xferlog:640:root:wheel
/var/log/debug.log:640:root:wheel
/var/log/console.log:640:root:wheel
/var/log/dmesg:640:root:wheel
/var/log/security:640:root:wheel
/var/log/all.log:640:root:wheel
"

# Iterate over each log file, its expected permissions, user, and group
echo "$log_files" | while IFS=: read -r file expected_perms expected_user
expected_group; do
    if [ -f "$file" ]; then
        # Get current permissions, user, and group of the file
        current_perms=$(stat -f "%Lp" "$file")
        current_user=$(stat -f "%Su" "$file")
        current_group=$(stat -f "%Sg" "$file")

        # Check if permissions are correct
        if [ "$current_perms" -ne "$expected_perms" ]; then
            echo "Fixing permissions for $file from $current_perms to
$expected_perms"
            chmod "$expected_perms" "$file"
        fi

        # Check if user ownership is correct
        if [ "$current_user" != "$expected_user" ]; then
            echo "Fixing user ownership for $file from $current_user to
$expected_user"
            chown "$expected_user" "$file"
        fi

        # Check if group ownership is correct
        if [ "$current_group" != "$expected_group" ]; then
            echo "Fixing group ownership for $file from $current_group to
$expected_group"
            chgrp "$expected_group" "$file"
        fi
    else
        echo "File $file does not exist."
    fi
done

echo "Log file permissions, user, and group ownership check and fix
completed."
```

Note: You may also need to change the configuration for your logging software or services for any logs that have 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 Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation and detect unauthorized access or modification of data. By default, events will be logged to the `/var/audit/` directory, which can be configured in `/etc/security/audit_control`.

Different audit rules can be specified and defined in the `/etc/security/audit_class` file. More details of each class are mentioned in the Event Selection Expression

Capacity planning

The recommendations in this section implement auditing policies that produce large quantities of logged data and may negatively impact system performance. Capacity planning is critical to ensure production environments are not adversely impacted.

Disk space. If a significantly large set of events is 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 log rotation is implemented; otherwise, 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. In addition to the amount of data collected, also consider the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the system's 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 auditd service is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

Capturing system events provides system administrators with information to determine if unauthorized access to their system has occurred.

Audit:

Run the following command to verify that `auditd` is enabled:

```
# sysrc auditd_enable
auditd_enable: YES
```

Verify result is "YES".

Remediation:

Run the following command to enable `auditd`:

```
# service auditd enable
auditd enabled in /etc/rc.conf
```

Run the following command to start `auditd`:

```
# service auditd start
```

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
T1562, T1562.001	TA0005	

5.2.2 Configure Data Retention

Data Retention rules vary depending on the organization's industry and the compliance frameworks they are required to follow. Ensure adequate storage is allocated to support the data retention requirements for your organization.

5.2.2.1 Ensure audit log storage size is configured (Manual)

Profile Applicability:

- Level 2

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:

An appropriate size must be 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 the output complies with site policy:

```
# grep "^filesz:" /etc/security/audit_control
filesz:2M
```

Remediation:

Set the following parameter in `/etc/security/audit_control` by site policy:

```
filesz:2M
```

References:

1. NIST SP 800-53 Rev. 5: AU-8

Additional Information:

The `filesz` parameter is measured in bytes. For convenience, the trail size may be expressed with suffix letters: B (Bytes), K (Kilobytes), M (Megabytes), or G (Gigabytes). For example, 2M is the same as 2097152.

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 audits 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 (Manual)

Profile Applicability:

- Level 2

Description:

The `expire-after` specifies when audit log files will expire and be removed.

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 "^expire-after:" /etc/security/audit_control
expire-after:10M
```

Remediation:

Based on local site policy either remove the `expire-after` directive or set it to a larger value to retain older logs. The directive can be set in `/etc/security/audit_control`

```
expire-after:10M
```

The expiration specification can be one value or two values with the logical conjunction of AND/OR between them. Values for the audit log file age are numbers with the following suffixes:
s Log file age in seconds.
h Log file age in hours.
d Log file age in days.
y Log file age in years.
Values for the disk space used are numbers with the following suffixes:
(space) or
B Disk space used in Bytes.
K Disk space used in Kilobytes.
M Disk space used in Megabytes.
G Disk space used in Gigabytes.
The suffixes on the values are case-sensitive. If both an age and disk space value are used they are separated by AND or OR and both values are used to determine when audit log files expire. In the case of AND, both the age and disk space conditions must be met before the log file is removed. In the case of OR, either condition may expire the log file. For example:

```
expire-after: 60d AND 1G
```

will expire files that are older than 60 days but only if 1 gigabyte of disk space total is being used by the audit 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	

5.2.3 Configure auditd rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

There are global defaults that cannot be modified but additional directives can be configured for specific users. The entire list of configurable directives is available in the Handbook and is always updated when a new class is added.

User-specific audit rules can be specified in the `/etc/security/audit_user` file.

5.2.3.1 Ensure actions as another user are always logged (Manual)

Profile Applicability:

- Level 2

Description:

`sudo` provides users with temporarily 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 log file to verify if unauthorized commands have been executed.

Audit:

Run the following command to check the global flags:

```
# grep "^flags:.*aa" /etc/security/audit_control
flags:lo,aa
```

Verify the output has `aa` which is the short form of the event class authentication and authorization. `sudo` events are mentioned under `aa` directives.

Remediation:

Create audit rules
Edit the file `/etc/security/audit_event` and add the flag `aa` in the line starting with `flags:`. The file should contain a line similar to:

```
flags:aa
```

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

5.2.3.2 Ensure events that modify the sudo log file are collected (Manual)

Profile Applicability:

- Level 2

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:

Run the following command to check the current global directives for `auditd` events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the following event classes:

- `fa` (file attribute access)
- `fc` (file create)
- `fd` (file delete)
- `fm` (file attribute modify)
- `fr` (file read)
- `fw` (file write)

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events that modify files.
Modify the `flags` directive to match the following:

```
flags:fa,fc,fd,fm,fr,fw
```

These flags should be added if there were other flags previously configured rather than replacing the entire line.

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	

5.2.3.3 Ensure use of privileged commands are collected (Manual)

Profile Applicability:

- Level 2

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.

Audit:

Run the following command to check the current global directives for auditd events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `pc` (process) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events that modify files.
Modify the flags directive to match the following:

```
flags:pc
```

These flags should be added if there were other flags previously configured rather than replacing the entire line.

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

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

5.2.3.4 Ensure discretionary access control permission modification events are collected (Manual)

Profile Applicability:

- Level 2

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 affect 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.

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

Run the following command to check the current global directives for `auditd` events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `fm` (file attribute modify) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events that modify file attributes.
Modify the flags directive to match the following:

```
flags:fm
```

These flags should be added if there were other flags previously configured rather than replacing the entire line.

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

5.2.3.5 Ensure successful file system mounts are collected (Manual)

Profile Applicability:

- Level 2

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 required to 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 are beyond the scope of this document.

Audit:

Run the following command to check the current global directives for auditd events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `ad` (administrative) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events that perform administrative actions as a whole.
Modify the flags directive to match the following:

```
flags:ad
```

This flag should be added if there were other flags previously configured rather than replacing the entire line.

References:

1. NIST SP 800-53 Rev. 5: CM-6

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

5.2.3.6 Ensure login and logout events are collected (Manual)

Profile Applicability:

- Level 2

Description:

Monitor login and logout events.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute-force attacks against user logins.

Audit:

Run the following command to check the current global directives for auditd events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `lo` (login_logout) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events like login/logout.
Modify the flags directive to match the following:

```
flags:lo
```

This flag should be added if there were other flags previously configured rather than replacing the entire line.

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

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	

5.2.3.7 Ensure file deletion events by users are collected (Manual)

Profile Applicability:

- Level 2

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:

Run the following command to check the current global directives for auditd events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `fd` (file delete) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor system calls related to file deletion.
Modify the flags directive to match the following:

```
flags:fd
```

This flag should be added if there were other flags previously configured rather than replacing the entire line.

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	

5.2.3.8 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Manual)

Profile Applicability:

- Level 2

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:

Run the following command to check the current global directives for auditd events that are being monitored:

```
# grep "^flags:" /etc/security/audit_control
flags:lo,aa
```

The flags directive should contain the `ad` (administrative) event class.

Remediation:

Edit the file `/etc/security/audit_control`, with the relevant rules to monitor events like `usermod`.
Modify the flags directive to match the following:

```
flags:ad
```

This flag should be added if there were other flags previously configured rather than replacing the entire line.

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

5.2.4 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 (Manual)

Profile Applicability:

- Level 2

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 -L -f "%N %Lp" "$(awk -F":" '/^dir/ {print $2}'
/etc/security/audit_control)" | grep -Ev -- '^\s*\S+\s+([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 "$(awk -F":" '/^dir/ {print $2}'
/etc/security/audit_control)"
```

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 (Manual)

Profile Applicability:

- Level 2

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/security/audit_control ] && find "$(awk -F ":" '/^dir/ {print
$2}' /etc/security/audit_control | 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 -Lf "%N %Lp" {} +
```

Nothing should be returned.

Remediation:

Run the following command to remove more permissive mode than `0640` from audit log files:

```
# [ -f /etc/security/audit_control ] && find "$(awk -F ":" '/^dir/ {print
$2}' /etc/security/audit_control | 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 (Manual)

Profile Applicability:

- Level 2

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/security/audit_control ] && find "$(awk -F ":" '/^dir/ {print
$2}' /etc/security/audit_control | xargs)" -type f ! -user root -exec stat -
Lf "%N %Su" {} +
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by the `root` user:

```
# [ -f /etc/security/audit_control ] && find "$(awk -F ":" '/^dir/ {print
$2}' /etc/security/audit_control | 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 (Manual)

Profile Applicability:

- Level 2

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:

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 -L -f "%Sg" "$(awk -F":" '/^dir/ {print $2}'
/etc/security/audit_control | xargs)"/* | grep -Ev '^(audit|wheel)'
```

Nothing should be returned

Remediation:

Run the following command to configure the audit log files to be owned by the `audit` group:

```
# chgrp audit /var/audit
```

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 restrictive (Manual)

Profile Applicability:

- Level 2

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:

```
# stat -Lf '%N %Lp' /etc/security/audit_warn | grep -Ev --
'^\s*\S+\s+500\s*$'
# stat -Lf '%N %Lp' /etc/security/audit_event /etc/security/audit_class |
grep -Ev -- '^\s*\S+\s+444\s*$'
# stat -Lf '%N %Lp' /etc/security/audit_control /etc/security/audit_user |
grep -Ev -- '^\s*\S+\s+600\s*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit configuration files:

```
# chmod 444 /etc/security/audit_event /etc/security/audit_class
# chmod 500 /etc/security/audit_warn
# chmod 600 /etc/security/audit_control /etc/security/audit_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
T1070, T1070.002, T1083, T1083.000	TA0007	

5.2.4.6 Ensure audit configuration files are owned by root (Manual)

Profile Applicability:

- Level 2

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 644 or more restrictive and are owned by the root user and root wheel:

```
# find /etc/security -type f -name 'audit*' ! -user root
```

Nothing should be returned

Remediation:

Run the following command to change ownership to `root` user:

```
# find /etc/security -type f -name 'audit*' -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 wheel (Manual)

Profile Applicability:

- Level 2

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/security -type f -name 'audit*' ! -group wheel
```

Nothing should be returned

Remediation:

Run the following command to change group to `wheel`:

```
# find /etc/security -type f -name 'audit*' ! -group wheel chgrp wheel {} +
```

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 555 or more restrictive (Manual)

Profile Applicability:

- Level 2

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 `555` or more restrictive, are owned by the root user and group root:

```
# stat -Lf '%N %Lp' /usr/sbin/*audit* | grep -Ev -- '^\s*\S+\s+([0-
5][0,1,4,5][0,1,4,5])\s*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod 555 /usr/sbin/*audit*
```

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 (Manual)

Profile Applicability:

- Level 2

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 `555` or more restrictive, are owned by the root user and group wheel:

```
# stat -Lf '%N %Su' /usr/sbin/*audit* | grep -Ev -- '^\s*\S+\s+root\s*$'
```

Nothing should be returned

Remediation:

Run the following command to change the owner of the audit tools to the `root` user:

```
# chown root /usr/sbin/*audit*
```

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 wheel (Manual)

Profile Applicability:

- Level 2

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 `555` or more restrictive, are owned by the root user and group wheel:

```
# stat -Lf '%N %Lp %Su %Sg' /usr/sbin/*audit* | grep -Ev -- '^\s*\S+\s+([0-5][0,1,4,5][0,1,4,5])\s+root\s+wheel\s*$'
```

Nothing should be returned

Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod 555 /usr/sbin/*audit*
```

Run the following command to change owner and group of the audit tools to `root` user and `wheel` group:

```
# chown root:wheel /usr/sbin/*audit*
```

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 (Manual)

Profile Applicability:

- Level 1

Description:

Advanced Intrusion Detection Environment (AIDE) is an intrusion detection tool that uses predefined rules to check the integrity of files and directories in the FreeBSD operating system. AIDE has its own database for this purpose.

`aide` takes a snapshot of files and directories, including modification times, permissions, and file hashes. This snapshot can then be used to compare against the current state of the filesystem to detect system modifications.

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 that `aide` is installed:

```
# pkg query -g %n 'aide*'

aide-<version>
```

Remediation:

Run the following command to install `aide`:

```
# pkg 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. https://aide.github.io/
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	

5.3.2 Ensure filesystem integrity is regularly checked (Manual)

Profile Applicability:

- Level 1

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.

```
# crontab -l -u root | grep -Es 'aide\s(--?\S+\s)*(--(check|update))\b'
```

Ensure a cron job in compliance with site policy is returned.

Remediation:

Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
@daily /usr/bin/lockf -s -t 0 /var/run/aide.lock /usr/local/bin/aide --check
```

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 0000 hours. 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 (Manual)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains user account information used by many system utilities, which 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 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 -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)' /etc/passwd

Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ wheel)
```

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: (100644/-rw-r--r--) Uid: (0/ root) Gid: (0/ wheel)

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/group are configured (Manual)

Profile Applicability:

- Level 1

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 also 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/wheel`:

```
# stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)' /etc/group
Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ wheel)
```

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:wheel /etc/group
```

Default Value:

Access: (100644/-rw-r--r--) Uid: (0/ root) Gid: (0/ wheel)

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/master.passwd are configured (Manual)

Profile Applicability:

- Level 1

Description:

The `/etc/master.passwd` 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/master.passwd` file, they can easily run a password cracking program against the hashed password to break it. Other security information stored in the `/etc/master.passwd` file (such as expiration) could also be helpful in subverting user accounts.

Audit:

Run the following command to verify `/etc/master.passwd` is mode 000, `Uid` is `0/root` and `Gid` is `0/wheel`:

```
# stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)'
/etc/master.passwd

Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ wheel)
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/master.passwd`:

```
# chown root:wheel /etc/master.passwd
# chmod 0000 /etc/master.passwd
```

Default Value:

Access: (100644/-rw-r--r--) Uid: (0/ root) Gid: (0/ wheel)

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/shells are configured (Manual)

Profile Applicability:

- Level 1

Description:

`/etc/shells` is a text file that contains the full pathnames of valid login shells. This file is consulted by `chsh` and is available to be queried by other programs.

Rationale:

It is critical to protect the `/etc/shells` file from unauthorized access. Although it is protected by default, the file permissions could be changed 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/wheel`:

```
# stat -L -f 'Access: (%p/%Sp)  Uid: ( %u/ %Su) Gid: ( %g/ %Sg)' /etc/shells

Access: (100644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ wheel)
```

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:wheel /etc/shells
```

Default Value:

Access: (100644/-rw-r--r--) Uid: (0/ root) Gid: (0/ wheel)

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 world writable files and directories are secured (Automated)

Profile Applicability:

- Level 1

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

```
#!/bin/sh

a_path_exclusions="! -path '/tmp/*' ! -path '/proc/*'"

eval "find / \( $a_path_exclusions \) -type f -perm -o=w -print"

# Evaluate and execute the find command for directories
eval "find / \( $a_path_exclusions \) -type d -perm -o=w ! -perm -1000 -
print"
```

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

```
#!/bin/sh

# Define paths to exclude (space-separated)
a_path_exclusions="! -path '/tmp/*' ! -path '/proc/*'"

# Fix world-writable files by removing the write permission for "others"
find / \( $a_path_exclusions \) -type f -perm -o=w -print -exec chmod o-w {}
\;

# Fix world-writable directories without the sticky bit
find / \( $a_path_exclusions \) -type d -perm -o=w ! -perm -1000 -print -exec
chmod +t,o-w {} \;
```

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

6.1.6 Ensure no unowned or ungrouped files or directories exist (Automated)

Profile Applicability:

- Level 1

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 command to verify no unowned or ungrouped files or directories exist:

```
# find / -xdev \( -nouser -o -nogroup \) -print
```

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

6.1.7 Ensure SUID and SGID files are reviewed (Manual)

Profile Applicability:

- Level 1

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:

```
#!/bin/sh
echo "Generating a list of SUID and SGID files..."

# Find SUID files
echo "SUID Files:"
find / -xdev -type f -perm -4000 -print

# Find SGID files
echo "SGID Files:"
find / -xdev -type f -perm -2000 -print
```

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

6.2 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/master.passwd use shadowed passwords (Manual)

Profile Applicability:

- Level 1

Description:

Local accounts can use shadowed passwords. These passwords are saved in a shadow password file, `/etc/master.passwd`, 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. Despite 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/master.passwd`. The `/etc/master.passwd` file is set, so only the root can read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords 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 == "*" ) { print $1 " is not set to shadowed passwords "}'
/etc/master.passwd
```

Remediation:

Investigate to determine if the account is logged in, what it is being used for, and whether 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	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/master.passwd password fields are not empty (Manual)

Profile Applicability:

- Level 1

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/master.passwd
```

Remediation:

If any accounts in the `/etc/master.passwd` 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:

```
# pw lock <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 (Manual)

Profile Applicability:

- Level 1

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:

```
#!/bin/sh

# Extract all unique group IDs (GID) from /etc/passwd
awk -F: '{print $4}' /etc/passwd | sort -u | while read gid; do
  # Check if the GID exists in /etc/group
  if ! grep -q -E "^.*:.*:$gid:" /etc/group; then
    echo "Group $gid 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 (Manual)

Profile Applicability:

- Level 1

Description:

Although the `adduser` or `pw` program will not let you create a duplicate User ID (UID), an administrator can 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:

```
#!/bin/sh
PASSWD_FILE="/etc/passwd"

awk -F: '{print $3}' "$PASSWD_FILE" | sort | uniq -c | awk '$1 > 1 {print
$2}' | while read -r uid; do
    echo "Duplicate UID: $uid"
    grep -F ":$uid:" "$PASSWD_FILE"
done
```

Remediation:

Based on the audit script's results, 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

Additional Information:

FreeBSD ships with a `toor` user with the UID `0`. The purpose of this is to provide an interactive shell if the administrator prefers third-party shells like bash, zsh, or ksh, which are available as pkg but do not ship with the base system.

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078, T1078.001, T1078.003	TA0005	M1027

6.2.5 Ensure no duplicate GIDs exist (Manual)

Profile Applicability:

- Level 1

Description:

Although the `pw` 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:

```
#!/bin/sh

# Define the path to the group file
GROUP_FILE="/etc/group"

# Extract GIDs and count occurrences
awk -F: '{print $3}' "$GROUP_FILE" | sort | uniq -c | awk '$1 > 1 {print $2}'
| while read -r gid; do
    echo "Duplicate GID: $gid"
    grep -F ":$gid:" "$GROUP_FILE"
done
```

Remediation:

Based on the audit script's results, 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

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 (Manual)

Profile Applicability:

- Level 1

Description:

Although the `adduser` or `pw` 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:

```
#!/bin/sh
PASSWD_FILE="/etc/passwd"

awk -F: '{print $1}' "$PASSWD_FILE" | sort | uniq -c | awk '$1 > 1 {print
$2}' | while read -r username; do
    echo "Duplicate username: $username"
    grep -F "^$username:" "$PASSWD_FILE"
done
```

Remediation:

Establish unique user names for the users based on the audit script's results. As long as the users have unique UIDs, file ownership will automatically reflect the change.

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 (Manual)

Profile Applicability:

- Level 1

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:

```
#!/bin/sh

dup_groups=""
dup_gids=""

group_names=$(cut -d: -f1 /etc/group)
group_gids=$(cut -d: -f3 /etc/group)

find_duplicates() {
    list="$1"
    echo "$list" | awk '
    {
        count[$0]++
    }
    END {
        for (i in count) {
            if (count[i] > 1) {
                print i
            }
        }
    }'
}

dup_groups=$(find_duplicates "$group_names")

dup_gids=$(find_duplicates "$group_gids")

if [ -n "$dup_groups" ]; then
    echo "Duplicate group names found:"
    echo "$dup_groups"
else
    echo "No duplicate group names found."
fi

if [ -n "$dup_gids" ]; then
    echo "Duplicate GIDs found:"
    echo "$dup_gids"
else
    echo "No duplicate GIDs found."
fi
```

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 (Manual)

Profile Applicability:

- Level 1

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`

```
#!/bin/sh

# Function to check if a path is valid
check_path() {
  path=$1

  # Check if path is empty (i.e., "::" in the PATH variable)
  if [ -z "$path" ]; then
    echo "Warning: PATH contains an empty directory (::)"
    return 1
  fi

  # Check if path exists and is a directory
  if [ ! -d "$path" ]; then
    echo "Warning: $path is not a directory"
    return 1
  fi

  # Check if path is the current working directory (.)
  if [ "$path" = "." ]; then
    echo "Warning: PATH contains the current working directory (.)"
    return 1
  fi

  # Check if the directory is owned by root
  #if [ "$(stat -c '%U' "$path")" != "root" ]; then
  if [ "$(stat -L -f '%Su' "$path")" != "root" ]; then
    echo "Warning: $path is not owned by root"
    return 1
  fi

  # Check if the directory has permissions more permissive than 0755
  if [ "$(stat -L -f '%Lp' "$path")" -gt 755 ]; then
    echo "Warning: $path has permissions more permissive than 0755"
    return 1
  fi

  return 0
}

# Ensure the script is being run as root
if [ "$(id -u)" -ne 0 ]; then
  echo "This script must be run as root."
  exit 1
fi

# Check if the PATH ends with a trailing colon
if [ "${PATH%:}" != "$PATH" ]; then
  echo "Warning: PATH has a trailing colon (:)"
fi

# Split PATH by colon and check each entry
IFS=: # Set Internal Field Separator to colon
for dir in $PATH; do
  check_path "$dir"
done
```

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 (Manual)

Profile Applicability:

- Level 1

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 4.3.7 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

Additional Information:

Note that FreeBSD ships with a `toor` user with a UID of `0`. This is mainly used by administrators who prefer a third party shell like bash, zsh, ksh which are available in pkg but not shipped with base system.

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

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 755 or more restrictive

```
#!/bin/sh

# Check if a user's home directory exists
check_home_directory() {
  local username=$1
  local homedir=$2

  if [ ! -d "$homedir" ]; then
    echo "Warning: Home directory $homedir does not exist for user $username"
    return 1
  fi
  return 0
}

# Check if the user owns their home directory
check_home_ownership() {
  local username=$1
  local homedir=$2

  if [ "$(stat -L -f '%Su' "$homedir")" != "$username" ]; then
    echo "Warning: User $username does not own their home directory $homedir"
    return 1
  fi
  return 0
}

# Check if the user's primary GID owns their home directory
check_home_group_ownership() {
  local gid=$1
  local homedir=$2

  if [ "$(stat -L -f '%Sg' "$homedir")" != "$(getent group "$gid" | cut -d: -f1)" ]; then
    echo "Warning: The primary group ID $gid does not own the home directory $homedir"
    return 1
  fi
  return 0
}

# Check if the home directory permissions are 0755 or more restrictive
check_home_permissions() {
  local homedir=$1

  if [ "$(stat -L -f '%Lp' "$homedir")" -gt 755 ]; then
    echo "Warning: Home directory $homedir has permissions more permissive than 0755"
    return 1
  fi
  return 0
}

# Get a list of all local interactive users
get_local_interactive_users() {
  awk -F: '($3 >= 1000 && $3 < 65534) && $7 != "/sbin/nologin" && $7 != "/bin/false" {print
$1":"$6":"$4}' /etc/passwd
}

# Main script execution
for user_info in $(get_local_interactive_users); do
  username=$(echo "$user_info" | cut -d: -f1)
  homedir=$(echo "$user_info" | cut -d: -f2)
  gid=$(echo "$user_info" | cut -d: -f3)

  check_home_directory "$username" "$homedir"
  check_home_ownership "$username" "$homedir"
  check_home_group_ownership "$gid" "$homedir"
  check_home_permissions "$homedir"
done
```

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.

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

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.
- `.sh_history` or `.history` file keeps track of the user's last 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
- `.sh_history` or `.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.

```
#!/bin/sh

# Function to check file permissions
check_file_permissions() {
  local filepath=$1
  local required_mode=$2
  local current_mode

  current_mode=$(stat -f '%Lp' "$filepath")
  if [ "$current_mode" -gt "$required_mode" ]; then
    echo "Warning: $filepath has permissions more permissive than
$required_mode"
  fi
}

# Function to check file ownership
check_file_ownership() {
  local filepath=$1
  local username=$2
  local gid=$3

  if [ "$(stat -f '%Su' "$filepath")" != "$username" ]; then
    echo "Warning: $filepath is not owned by $username"
  fi

  if [ "$(stat -f '%Sg' "$filepath")" != "$(getent group "$gid" | cut -d: -
f1)" ]; then
    echo "Warning: The primary group ID $gid does not own $filepath"
  fi
}

# Function to verify dot files for a user
verify_dot_files() {
  local username=$1
  local homedir=$2
  local gid=$3

  for file in "$homedir"/.[!.]*; do
    [ -e "$file" ] || continue # Skip if the file does not exist

    # Exclude .forward, .rhost, .netrc
    case "$(basename "$file")" in
      .forward|.rhost|.netrc)
        echo "Warning: $file should not exist"
        ;;
      .sh_history)
        check_file_permissions "$file" 600
        ;;
      .history)
        check_file_permissions "$file" 600
        ;;
      *)
        check_file_permissions "$file" 644
        ;;
    esac

    # Check ownership for all other files
```

```
    check_file_ownership "$file" "$username" "$gid"
  done
}

# Get a list of all local interactive users
get_local_interactive_users() {
  awk -F: '($3 >= 1000 && $3 < 65534) && $7 != "/sbin/nologin" && $7 !=
"/bin/false" {print $1":"$6":"$4}' /etc/passwd
}

# Main script execution
for user_info in $(get_local_interactive_users); do
  username=$(echo "$user_info" | cut -d: -f1)
  homedir=$(echo "$user_info" | cut -d: -f2)
  gid=$(echo "$user_info" | cut -d: -f3)

  [ -d "$homedir" ] && verify_dot_files "$username" "$homedir" "$gid"
done
```

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 following site policy.

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 ext2fs kernel module is not available (Manual)	☐	☐
1.1.1.2	Ensure msdosfs kernel module is not available (Manual)	☐	☐
1.1.1.3	Ensure zfs kernel module is not available (Manual)	☐	☐
1.1.2	**Configure Filesystem Partitions**		
1.1.2.1	**Configure /tmp**		
1.1.2.1.1	Ensure /tmp is a separate partition (Manual)	☐	☐
1.1.2.1.2	Ensure nosuid option set on /tmp partition (Manual)	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition (Manual)	☐	☐
1.1.2.2	**Configure /home**		
1.1.2.2.1	Ensure separate partition exists for /home (Manual)	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition (Manual)	☐	☐
1.1.2.3	**Configure /var**		
1.1.2.3.1	Ensure separate partition exists for /var (Manual)	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition (Manual)	☐	☐
1.1.2.4	**Configure /var/tmp**		
1.1.2.4.1	Ensure separate partition exists for /var/tmp (Manual)	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.2.4.3	Ensure noexec option set on /var/tmp partition (Manual)	☐	☐
1.1.2.5	**Configure /var/log**		
1.1.2.5.1	Ensure separate partition exists for /var/log (Manual)	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition (Manual)	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition (Manual)	☐	☐
1.1.2.6	**Configure /var/audit**		
1.1.2.6.1	Ensure separate partition exists for /var/audit (Manual)	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition (Manual)	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition (Manual)	☐	☐
1.2	**Configure Software and Patch Management**		
1.2.1	Ensure update server certificate key fingerprints are configured (Manual)	☐	☐
1.2.2	Ensure package manager repositories are configured (Manual)	☐	☐
1.2.3	Ensure updates, patches, and additional security software are installed (Manual)	☐	☐
1.3	**Configure Secure Boot Settings**		
1.3.1	Ensure bootloader password is set (Automated)	☐	☐
1.3.2	Ensure permissions on bootloader config are configured (Manual)	☐	☐
1.4	**Configure Additional Process Hardening**		
1.4.1	Ensure address space layout randomization (ASLR) is enabled (Manual)	☐	☐
1.4.2	Ensure core dump backtraces are disabled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.4.3	Ensure core dump storage is disabled (Manual)	☐	☐
1.5	**Mandatory Access Control**		
1.6	**Configure Command Line Warning Banners**		
1.6.1	Ensure message of the day is configured properly (Manual)	☐	☐
1.6.2	Ensure local login warning banner is configured properly (Manual)	☐	☐
1.6.3	Ensure remote login warning banner is configured properly (Manual)	☐	☐
1.6.4	Ensure access to /etc/motd is configured (Manual)	☐	☐
1.6.5	Ensure access to /etc/issue is configured (Manual)	☐	☐
2	**Services**		
2.1	**Configure Time Synchronization**		
2.1.1	Ensure time synchronization is in use (Manual)	☐	☐
2.2	**Configure Special Purpose Services**		
2.2.1	Ensure autofs services are not in use (Manual)	☐	☐
2.2.2	Ensure ftp server services are not in use (Manual)	☐	☐
2.2.3	Ensure message access server services are not in use (Manual)	☐	☐
2.2.4	Ensure network file system services are not in use (Manual)	☐	☐
2.2.5	Ensure nis server services are not in use (Manual)	☐	☐
2.2.6	Ensure rpcbind services are not in use (Manual)	☐	☐
2.2.7	Ensure snmp services are not in use (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.8	Ensure telnet server services are not in use (Manual)	☐	☐
2.2.9	Ensure tftp server services are not in use (Manual)	☐	☐
2.2.10	Ensure web proxy server services are not in use (Manual)	☐	☐
2.2.11	Ensure mail transfer agents are configured for local-only mode (Automated)	☐	☐
2.2.12	Ensure only approved services are listening on a network interface (Manual)	☐	☐
3	**Network**		
3.1	**Configure Network Devices**		
3.1.1	Ensure IPv6 status is identified (Manual)	☐	☐
3.2	**Configure Network Kernel Modules**		
3.2.1	Ensure sctp kernel module is not available (Manual)	☐	☐
3.3	**Configure Network Kernel Parameters**		
3.3.1	Ensure ip forwarding is disabled (Manual)	☐	☐
3.3.2	Ensure packet redirect sending is disabled (Manual)	☐	☐
3.3.3	Ensure broadcast & multicast icmp requests are ignored (Manual)	☐	☐
3.3.4	Ensure icmp redirects are not accepted (Manual)	☐	☐
3.3.5	Ensure source routed packets are not accepted (Manual)	☐	☐
3.3.6	Ensure tcp syn cookies is enabled (Manual)	☐	☐
3.3.7	Ensure ipv6 router advertisements are not accepted (Manual)	☐	☐
3.4	**Configure Host Based Firewall**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4.1	**Configure a firewall utility**		
3.4.1.1	Ensure ipfw is enabled and configured (Manual)	☐	☐
3.4.1.2	Ensure a single firewall utility is in use (Manual)	☐	☐
4	**Access, Authentication and Authorization**		
4.1	**Configure job schedulers**		
4.1.1	**Configure cron**		
4.1.1.1	Ensure permissions on /etc/crontab are configured (Automated)	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured (Automated)	☐	☐
4.1.1.3	Ensure crontab is restricted to authorized users (Manual)	☐	☐
4.1.2	**Configure at**		
4.1.2.1	Ensure at is restricted to authorized users (Manual)	☐	☐
4.2	**Configure SSH Server**		
4.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Manual)	☐	☐
4.2.2	Ensure permissions on SSH private host key files are configured (Manual)	☐	☐
4.2.3	Ensure permissions on SSH public host key files are configured (Manual)	☐	☐
4.2.4	Ensure sshd access is configured (Manual)	☐	☐
4.2.5	Ensure sshd Banner is configured (Manual)	☐	☐
4.2.6	Ensure sshd Ciphers are configured (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Manual)	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled (Manual)	☐	☐
4.2.9	Ensure sshd HostbasedAuthentication is disabled (Manual)	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled (Manual)	☐	☐
4.2.11	Ensure sshd KexAlgorithms is configured (Manual)	☐	☐
4.2.12	Ensure sshd LoginGraceTime is configured (Manual)	☐	☐
4.2.13	Ensure sshd LogLevel is configured (Manual)	☐	☐
4.2.14	Ensure sshd MACs are configured (Manual)	☐	☐
4.2.15	Ensure sshd MaxAuthTries is configured (Manual)	☐	☐
4.2.16	Ensure sshd MaxSessions is configured (Manual)	☐	☐
4.2.17	Ensure sshd MaxStartups is configured (Manual)	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled (Manual)	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled (Manual)	☐	☐
4.2.20	Ensure sshd PermitUserEnvironment is disabled (Automated)	☐	☐
4.2.21	Ensure sshd UsePAM is enabled (Automated)	☐	☐
4.3	**Configure privilege escalation**		
4.3.1	Ensure sudo is installed (Manual)	☐	☐
4.3.2	Ensure sudo commands use pty (Automated)	☐	☐
4.3.3	Ensure sudo log file exists (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.4	Ensure users must provide password for escalation (Manual)	☐	☐
4.3.5	Ensure re-authentication for privilege escalation is not disabled globally (Manual)	☐	☐
4.3.6	Ensure sudo authentication timeout is configured correctly (Manual)	☐	☐
4.3.7	Ensure access to the su command is restricted (Manual)	☐	☐
4.4	**Configure Pluggable Authentication Modules**		
4.4.1	**Configure pluggable module arguments**		
4.4.1.1	**Configure pam_passwdqc module**		
4.4.1.1.1	Ensure password length is configured (Manual)	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user (Manual)	☐	☐
4.4.1.2	**Configure pam_unix module**		
4.4.1.2.1	Ensure pam_unix does not include nullok (Manual)	☐	☐
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 (Manual)	☐	☐
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 (Manual)	☐	☐
4.5.2	**Configure root and system accounts and environment**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.2.1	Ensure default group for the root account is GID 0 (Manual)	☐	☐
4.5.2.2	Ensure root user umask is configured (Manual)	☐	☐
4.5.2.3	Ensure system accounts are secured (Manual)	☐	☐
4.5.3	**Configure user default environment**		
4.5.3.1	Ensure nologin is not listed in /etc/shells (Manual)	☐	☐
4.5.3.2	Ensure default user umask is configured (Manual)	☐	☐
5	**Logging and Auditing**		
5.1	**Configure Logging**		
5.1.1	**Configure syslog**		
5.1.1.1	Ensure syslog is installed (Manual)	☐	☐
5.1.1.2	Ensure syslogd service is enabled (Manual)	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured (Manual)	☐	☐
5.1.1.4	Ensure logging is configured (Manual)	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host (Manual)	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client (Manual)	☐	☐
5.1.2	Ensure newsyslog is configured (Manual)	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured (Manual)	☐	☐
5.2	**Configure System Accounting (auditd)**		
5.2.1	**Ensure auditing is enabled**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.1.1	Ensure auditd service is enabled (Manual)	☐	☐
5.2.2	**Configure Data Retention**		
5.2.2.1	Ensure audit log storage size is configured (Manual)	☐	☐
5.2.2.2	Ensure audit logs are not automatically deleted (Manual)	☐	☐
5.2.3	**Configure auditd rules**		
5.2.3.1	Ensure actions as another user are always logged (Manual)	☐	☐
5.2.3.2	Ensure events that modify the sudo log file are collected (Manual)	☐	☐
5.2.3.3	Ensure use of privileged commands are collected (Manual)	☐	☐
5.2.3.4	Ensure discretionary access control permission modification events are collected (Manual)	☐	☐
5.2.3.5	Ensure successful file system mounts are collected (Manual)	☐	☐
5.2.3.6	Ensure login and logout events are collected (Manual)	☐	☐
5.2.3.7	Ensure file deletion events by users are collected (Manual)	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Manual)	☐	☐
5.2.4	**Configure auditd file access**		
5.2.4.1	Ensure the audit log directory is 0750 or more restrictive (Manual)	☐	☐
5.2.4.2	Ensure audit log files are mode 0640 or less permissive (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.4.3	Ensure only authorized users own audit log files (Manual)	☐	☐
5.2.4.4	Ensure only authorized groups are assigned ownership of audit log files (Manual)	☐	☐
5.2.4.5	Ensure audit configuration files are restrictive (Manual)	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root (Manual)	☐	☐
5.2.4.7	Ensure audit configuration files belong to group wheel (Manual)	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive (Manual)	☐	☐
5.2.4.9	Ensure audit tools are owned by root (Manual)	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel (Manual)	☐	☐
5.3	**Configure Integrity Checking**		
5.3.1	Ensure AIDE is installed (Manual)	☐	☐
5.3.2	Ensure filesystem integrity is regularly checked (Manual)	☐	☐
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Ensure permissions on /etc/passwd are configured (Manual)	☐	☐
6.1.2	Ensure permissions on /etc/group are configured (Manual)	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured (Manual)	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1.5	Ensure world writable files and directories are secured (Automated)	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist (Automated)	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed (Manual)	☐	☐
6.2	**Local User and Group Settings**		
6.2.1	Ensure accounts in /etc/master.passwd use shadowed passwords (Manual)	☐	☐
6.2.2	Ensure /etc/master.passwd password fields are not empty (Manual)	☐	☐
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Manual)	☐	☐
6.2.4	Ensure no duplicate UIDs exist (Manual)	☐	☐
6.2.5	Ensure no duplicate GIDs exist (Manual)	☐	☐
6.2.6	Ensure no duplicate user names exist (Manual)	☐	☐
6.2.7	Ensure no duplicate group names exist (Manual)	☐	☐
6.2.8	Ensure root path integrity (Manual)	☐	☐
6.2.9	Ensure root is the only UID 0 account (Manual)	☐	☐
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
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.8	Ensure telnet server services are not in use	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.19	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	☐	☐
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	Ensure auditd service is enabled	☐	☐
5.2.3.3	Ensure use of privileged commands are collected	☐	☐
5.2.3.6	Ensure login and logout events are collected	☐	☐
5.2.3.7	Ensure file deletion events by users are collected	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group wheel	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
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 ext2fs kernel module is not available	☐	☐
1.1.1.2	Ensure msdosfs kernel module is not available	☐	☐
1.1.1.3	Ensure zfs kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/audit	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure ftp server services are not in use	☐	☐
2.2.3	Ensure message access server services are not in use	☐	☐
2.2.4	Ensure network file system services are not in use	☐	☐
2.2.5	Ensure nis server services are not in use	☐	☐
2.2.6	Ensure rpcbind services are not in use	☐	☐
2.2.7	Ensure snmp services are not in use	☐	☐
2.2.8	Ensure telnet server services are not in use	☐	☐
2.2.9	Ensure tftp server services are not in use	☐	☐
2.2.10	Ensure web proxy server services are not in use	☐	☐
2.2.11	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.12	Ensure only approved services are listening on a network interface	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.2.1	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 broadcast & multicast icmp requests are ignored	☐	☐
3.3.4	Ensure icmp redirects are not accepted	☐	☐
3.3.5	Ensure source routed packets are not accepted	☐	☐
3.3.6	Ensure tcp syn cookies is enabled	☐	☐
3.3.7	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐

Recommendation		Set Correctly	
		Yes	No
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	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.11	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.14	Ensure sshd MACs are configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.21	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	☐	☐
4.4.1.1.1	Ensure password length is configured	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user	☐	☐
4.4.1.2.1	Ensure pam_unix does not include nullok	☐	☐
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	☐	☐
4.5.2.1	Ensure default group for the root account is GID 0	☐	☐
4.5.2.2	Ensure root user umask is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.5.2.3	Ensure system accounts are secured	☐	☐
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2	Ensure newsyslog is configured	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	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 actions as another user are always logged	☐	☐
5.2.3.2	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.3	Ensure use of privileged commands are collected	☐	☐
5.2.3.4	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.5	Ensure successful file system mounts are collected	☐	☐
5.2.3.6	Ensure login and logout events are collected	☐	☐
5.2.3.7	Ensure file deletion events by users are collected	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group wheel	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
6.2.1	Ensure accounts in /etc/master.passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/master.passwd 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 ext2fs kernel module is not available	☐	☐
1.1.1.2	Ensure msdosfs kernel module is not available	☐	☐
1.1.1.3	Ensure zfs kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/audit	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure ftp server services are not in use	☐	☐
2.2.3	Ensure message access server services are not in use	☐	☐
2.2.4	Ensure network file system services are not in use	☐	☐
2.2.5	Ensure nis server services are not in use	☐	☐
2.2.6	Ensure rpcbind services are not in use	☐	☐
2.2.7	Ensure snmp services are not in use	☐	☐
2.2.8	Ensure telnet server services are not in use	☐	☐
2.2.9	Ensure tftp server services are not in use	☐	☐
2.2.10	Ensure web proxy server services are not in use	☐	☐
2.2.11	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.12	Ensure only approved services are listening on a network interface	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.2.1	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 broadcast & multicast icmp requests are ignored	☐	☐
3.3.4	Ensure icmp redirects are not accepted	☐	☐
3.3.5	Ensure source routed packets are not accepted	☐	☐
3.3.6	Ensure tcp syn cookies is enabled	☐	☐
3.3.7	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.11	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.14	Ensure sshd MACs are configured	☐	☐
4.2.15	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.21	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	☐	☐
4.4.1.1.1	Ensure password length is configured	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user	☐	☐
4.4.1.2.1	Ensure pam_unix does not include nullok	☐	☐
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	☐	☐

Recommendation		Set Correctly	
		Yes	No
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	☐	☐
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2	Ensure newsyslog is configured	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	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 actions as another user are always logged	☐	☐
5.2.3.2	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.3	Ensure use of privileged commands are collected	☐	☐
5.2.3.4	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.5	Ensure successful file system mounts are collected	☐	☐
5.2.3.6	Ensure login and logout events are collected	☐	☐
5.2.3.7	Ensure file deletion events by users are collected	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 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 wheel	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
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/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
6.2.1	Ensure accounts in /etc/master.passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/master.passwd 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
1.4.2	Ensure core dump backtraces are disabled	☐	☐
1.4.3	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	☐	☐
4.2.5	Ensure sshd Banner is configured	☐	☐
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	☐	☐
4.2.9	Ensure sshd HostbasedAuthentication is disabled	☐	☐
4.2.12	Ensure sshd LoginGraceTime is configured	☐	☐
4.2.16	Ensure sshd MaxSessions is configured	☐	☐
4.2.20	Ensure sshd PermitUserEnvironment is disabled	☐	☐
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	☐	☐
6.2.9	Ensure root is the only UID 0 account	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/audit	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.21	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	☐	☐
4.4.1.1.1	Ensure password length is configured	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user	☐	☐
4.4.1.2.1	Ensure pam_unix does not include nullok	☐	☐
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	☐	☐
4.5.2.1	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	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2	Ensure newsyslog is configured	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	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	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 restrictive	☐	☐
5.2.4.6	Ensure audit configuration files are owned by root	☐	☐
5.2.4.7	Ensure audit configuration files belong to group wheel	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
6.2.2	Ensure /etc/master.passwd 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 ext2fs kernel module is not available	☐	☐
1.1.1.2	Ensure msdosfs kernel module is not available	☐	☐
1.1.1.3	Ensure zfs kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/audit	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure ftp server services are not in use	☐	☐
2.2.3	Ensure message access server services are not in use	☐	☐
2.2.4	Ensure network file system services are not in use	☐	☐
2.2.5	Ensure nis server services are not in use	☐	☐
2.2.6	Ensure rpcbind services are not in use	☐	☐
2.2.7	Ensure snmp services are not in use	☐	☐
2.2.8	Ensure telnet server services are not in use	☐	☐
2.2.9	Ensure tftp server services are not in use	☐	☐
2.2.10	Ensure web proxy server services are not in use	☐	☐
2.2.11	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.12	Ensure only approved services are listening on a network interface	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.2.1	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 broadcast & multicast icmp requests are ignored	☐	☐
3.3.4	Ensure icmp redirects are not accepted	☐	☐
3.3.5	Ensure source routed packets are not accepted	☐	☐
3.3.6	Ensure tcp syn cookies is enabled	☐	☐
3.3.7	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.11	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.14	Ensure sshd MACs are configured	☐	☐
4.2.15	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.21	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	☐	☐
4.4.1.1.1	Ensure password length is configured	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user	☐	☐
4.4.1.2.1	Ensure pam_unix does not include nullok	☐	☐
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	☐	☐

Recommendation		Set Correctly	
		Yes	No
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	☐	☐
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2	Ensure newsyslog is configured	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	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 actions as another user are always logged	☐	☐
5.2.3.2	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.3	Ensure use of privileged commands are collected	☐	☐
5.2.3.4	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.5	Ensure successful file system mounts are collected	☐	☐
5.2.3.6	Ensure login and logout events are collected	☐	☐
5.2.3.7	Ensure file deletion events by users are collected	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 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 wheel	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
6.2.1	Ensure accounts in /etc/master.passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/master.passwd 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 ext2fs kernel module is not available	☐	☐
1.1.1.2	Ensure msdosfs kernel module is not available	☐	☐
1.1.1.3	Ensure zfs kernel module is not available	☐	☐
1.1.2.1.1	Ensure /tmp is a separate partition	☐	☐
1.1.2.1.2	Ensure nosuid option set on /tmp partition	☐	☐
1.1.2.1.3	Ensure noexec option set on /tmp partition	☐	☐
1.1.2.2.1	Ensure separate partition exists for /home	☐	☐
1.1.2.2.2	Ensure nosuid option set on /home partition	☐	☐
1.1.2.3.1	Ensure separate partition exists for /var	☐	☐
1.1.2.3.2	Ensure nosuid option set on /var partition	☐	☐
1.1.2.4.1	Ensure separate partition exists for /var/tmp	☐	☐
1.1.2.4.2	Ensure nosuid option set on /var/tmp partition	☐	☐
1.1.2.4.3	Ensure noexec option set on /var/tmp partition	☐	☐
1.1.2.5.1	Ensure separate partition exists for /var/log	☐	☐
1.1.2.5.2	Ensure nosuid option set on /var/log partition	☐	☐
1.1.2.5.3	Ensure noexec option set on /var/log partition	☐	☐
1.1.2.6.1	Ensure separate partition exists for /var/audit	☐	☐
1.1.2.6.2	Ensure nosuid option set on /var/audit partition	☐	☐
1.1.2.6.3	Ensure noexec option set on /var/audit partition	☐	☐
1.2.1	Ensure update server certificate key fingerprints are configured	☐	☐
1.2.2	Ensure package manager repositories are configured	☐	☐
1.2.3	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	☐	☐
1.4.1	Ensure address space layout randomization (ASLR) is enabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.6.4	Ensure access to /etc/motd is configured	☐	☐
1.6.5	Ensure access to /etc/issue is configured	☐	☐
2.1.1	Ensure time synchronization is in use	☐	☐
2.2.1	Ensure autofs services are not in use	☐	☐
2.2.2	Ensure ftp server services are not in use	☐	☐
2.2.3	Ensure message access server services are not in use	☐	☐
2.2.4	Ensure network file system services are not in use	☐	☐
2.2.5	Ensure nis server services are not in use	☐	☐
2.2.6	Ensure rpcbind services are not in use	☐	☐
2.2.7	Ensure snmp services are not in use	☐	☐
2.2.8	Ensure telnet server services are not in use	☐	☐
2.2.9	Ensure tftp server services are not in use	☐	☐
2.2.10	Ensure web proxy server services are not in use	☐	☐
2.2.11	Ensure mail transfer agents are configured for local-only mode	☐	☐
2.2.12	Ensure only approved services are listening on a network interface	☐	☐
3.1.1	Ensure IPv6 status is identified	☐	☐
3.2.1	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 broadcast & multicast icmp requests are ignored	☐	☐
3.3.4	Ensure icmp redirects are not accepted	☐	☐
3.3.5	Ensure source routed packets are not accepted	☐	☐
3.3.6	Ensure tcp syn cookies is enabled	☐	☐
3.3.7	Ensure ipv6 router advertisements are not accepted	☐	☐
3.4.1.1	Ensure ipfw is enabled and configured	☐	☐
3.4.1.2	Ensure a single firewall utility is in use	☐	☐
4.1.1.1	Ensure permissions on /etc/crontab are configured	☐	☐
4.1.1.2	Ensure permissions on /etc/cron.d are configured	☐	☐
4.1.1.3	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	☐	☐
4.2.6	Ensure sshd Ciphers are configured	☐	☐
4.2.8	Ensure sshd DisableForwarding is enabled	☐	☐
4.2.10	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.2.11	Ensure sshd KexAlgorithms is configured	☐	☐
4.2.13	Ensure sshd LogLevel is configured	☐	☐
4.2.14	Ensure sshd MACs are configured	☐	☐
4.2.15	Ensure sshd MaxAuthTries is configured	☐	☐
4.2.17	Ensure sshd MaxStartups is configured	☐	☐
4.2.18	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.2.19	Ensure sshd PermitRootLogin is disabled	☐	☐
4.2.21	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	☐	☐
4.4.1.1.1	Ensure password length is configured	☐	☐
4.4.1.1.2	Ensure password quality is enforced for the root user	☐	☐
4.4.1.2.1	Ensure pam_unix does not include nullok	☐	☐
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	☐	☐

Recommendation		Set Correctly	
		Yes	No
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	☐	☐
4.5.3.2	Ensure default user umask is configured	☐	☐
5.1.1.1	Ensure syslog is installed	☐	☐
5.1.1.2	Ensure syslogd service is enabled	☐	☐
5.1.1.3	Ensure syslogd default file permissions are configured	☐	☐
5.1.1.4	Ensure logging is configured	☐	☐
5.1.1.5	Ensure syslog is configured to send logs to a remote log host	☐	☐
5.1.1.6	Ensure rsyslog is not configured to receive logs from a remote client	☐	☐
5.1.2	Ensure newsyslog is configured	☐	☐
5.1.3	Ensure all logfiles have appropriate access configured	☐	☐
5.2.1.1	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 actions as another user are always logged	☐	☐
5.2.3.2	Ensure events that modify the sudo log file are collected	☐	☐
5.2.3.3	Ensure use of privileged commands are collected	☐	☐
5.2.3.4	Ensure discretionary access control permission modification events are collected	☐	☐
5.2.3.5	Ensure successful file system mounts are collected	☐	☐
5.2.3.6	Ensure login and logout events are collected	☐	☐
5.2.3.7	Ensure file deletion events by users are collected	☐	☐
5.2.3.8	Ensure successful and unsuccessful attempts to use the usermod command are recorded	☐	☐
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 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 wheel	☐	☐
5.2.4.8	Ensure audit tools are 555 or more restrictive	☐	☐
5.2.4.9	Ensure audit tools are owned by root	☐	☐
5.2.4.10	Ensure audit tools belong to group wheel	☐	☐
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/group are configured	☐	☐
6.1.3	Ensure permissions on /etc/master.passwd are configured	☐	☐
6.1.4	Ensure permissions on /etc/shells are configured	☐	☐
6.1.5	Ensure world writable files and directories are secured	☐	☐
6.1.6	Ensure no unowned or ungrouped files or directories exist	☐	☐
6.1.7	Ensure SUID and SGID files are reviewed	☐	☐
6.2.1	Ensure accounts in /etc/master.passwd use shadowed passwords	☐	☐
6.2.2	Ensure /etc/master.passwd 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
1.4.2	Ensure core dump backtraces are disabled	☐	☐
1.4.3	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	☐	☐
4.2.5	Ensure sshd Banner is configured	☐	☐
4.2.7	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	☐	☐
4.2.9	Ensure sshd HostbasedAuthentication is disabled	☐	☐
4.2.12	Ensure sshd LoginGraceTime is configured	☐	☐
4.2.16	Ensure sshd MaxSessions is configured	☐	☐
4.2.20	Ensure sshd PermitUserEnvironment is disabled	☐	☐
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	☐	☐
6.2.9	Ensure root is the only UID 0 account	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08/15/2024	1.0.0	Published
ADDED ITEMS:		
11/18/2024	1.0.1	ADDED RECOMMENDATION: 5.2.4.5 - Ensure audit configuration files are restrictive
11/18/2024	1.0.1	ADDED RECOMMENDATION: 5.2.4.7 - Ensure audit configuration files belong to group wheel
11/18/2024	1.0.1	ADDED RECOMMENDATION: 5.2.4.8 - Ensure audit tools are 555 or more restrictive
11/18/2024	1.0.1	ADDED RECOMMENDATION: 5.2.4.10 - Ensure audit tools belong to group wheel
DROPPED ITEMS:		
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 1.6.6 - Ensure access to /etc/issue.net is configured (LATER)
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 5.2.4.5 - Ensure audit configuration files are 640 or more restrictive
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 5.2.4.7 - Ensure audit configuration files belong to group root
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 5.2.4.8 - Ensure audit tools are 755 or more restrictive
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 5.2.4.10 - Ensure audit tools belong to group root
11/18/2024	1.0.1	DROPPED RECOMMENDATION: 5.3.3 - Ensure cryptographic mechanisms are used to protect the integrity of audit tools
UPDATED ITEMS:		

Date	Version	Changes for this version
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 1.3.2 - Ensure permissions on bootloader config are configured - Sections Modified: Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 1.4.2 - Ensure core dump backtraces are disabled - Sections Modified: Remediation Procedure
11/18/2024	1.0.1	UPDATED SECTION: 1.6 - Configure Command Line Warning Banners - Sections Modified: Description
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 1.6.1 - Ensure message of the day is configured properly - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 1.6.2 - Ensure local login warning banner is configured properly - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 1.6.3 - Ensure remote login warning banner is configured properly - Sections Modified: Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 2.2.2 - Ensure ftp server services are not in use - Sections Modified: Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 3.3.1 - Ensure ip forwarding is disabled - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 3.4.1.2 - Ensure a single firewall utility is in use - Sections Modified: Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 4.4.1.1.1 - Ensure password length is configured - Sections Modified: Remediation Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 4.4.1.1.2 - Ensure password quality is enforced for the root user - Sections Modified: Description; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.1.3 - Ensure all logfiles have appropriate access configured - Sections Modified: Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.1 - Ensure the audit log directory is 0750 or more restrictive - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.2 - Ensure audit log files are mode 0640 or less permissive - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.3 - Ensure only authorized users own audit log files - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.4 - Ensure only authorized groups are assigned ownership of audit log files - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.6 - Ensure audit configuration files are owned by root - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.2.4.9 - Ensure audit tools are owned by root - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 5.3.2 - Ensure filesystem integrity is regularly checked - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 6.1.5 - Ensure world writable files and directories are secured - Sections Modified: Remediation Procedure; Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 6.1.6 - Ensure no unowned or ungrouped files or directories exist - Sections Modified: Audit Procedure
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 6.1.7 - Ensure SUID and SGID files are reviewed - Sections Modified: Audit Procedure

Date	Version	Changes for this version
11/18/2024	1.0.1	UPDATED RECOMMENDATION: 6.2.7 - Ensure no duplicate group names exist - Sections Modified: Assessment Status; Audit Procedure
11/19/2024	1.0.1	Published