CIS Benchmarks

CIS Apple macOS 10.12 Benchmark

v1.1.0 - 09-06-2018

Terms of Use

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

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

Table of Contents

Overview

This is the archive of the CIS Apple macOS 10.12 Benchmark v1.1.0. CIS encourages you to migrate to a more recent, supported version of this technology.

This document, CIS Apple macOS 10.12 Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple macOS 10.12. This guide was tested against Apple macOS 10.12. To obtain the latest version of this guide, please visit http://benchmarks.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 document 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 Apple macOS 10.12.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

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.

- **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.

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:

Author
Ron Colvin

Contributor
Charles Heizer
William Harrison
Jason Olsen BSCS, ACSP 10.9, ACMT 2015
Greg Stone
Taylor Armstrong
Michael Bur
Rich Trouton

Editor
Rael Daruszka , Center for Internet Security
Eric Pinnell, Center for Internet Security

Recommendations

1 Install Updates, Patches and Additional Security Software

Install Updates, Patches and Additional Security Software

1.1 Verify all Apple provided software is current (Scored)

Profile Applicability:

- Level 1

Description:

Software vendors release security patches and software updates for their products when security vulnerabilities are discovered. There is no simple way to complete this action without a network connection to an Apple software repository. Please ensure appropriate access for this control. This check is only for what Apple provides through software update.

Rationale:

It is important that these updates be applied in a timely manner to prevent unauthorized persons from exploiting the identified vulnerabilities.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Choose Apple menu > App Store
2. Select Updates
3. Verify that all available updates and software patches are installed.

Alternatively:

1. In Terminal, run the following:

```
softwareupdate -l
```

2. Result: `No new software available`

Computers that have installed pre-release software in the past will fail this check if there are pre-release software updates available when audited. In the App Store setting System Preferences the computer may be set to no longer receive pre-release software.
Alternatively

```
defaults read /Library/Preferences/com.apple.SoftwareUpdate | egrep
LastFullSuccessfulDate
```

Response should be in the last 30 days (Example)
LastFullSuccessfulDate = "2018-02-27 00:16:40 +0000";

Remediation:

Perform the following to ensure the system is configured as prescribed:

1. Choose Apple menu > App Store – If prompted, enter an admin name and password.
2. Install all available updates and software patches that are applicable.

Alternatively:

1. In Terminal, run the following:

```
softwareupdate -l
```

2. In Terminal, run the following for any packages that show up in step 1:

```
sudo softwareupdate -i <packagename>
```

Impact:

Missing patches can lead to more exploit opportunities.

1.2 Enable Auto Update (Scored)

Profile Applicability:

- Level 1

Description:

Auto Update verifies that your system has the newest security patches and software updates. If "Automatically check for updates" is not selected background updates for new malware definition files from Apple for XProtect and Gatekeeper will not occur.

http://macops.ca/os-x-admins-your-clients-are-not-getting-background-security-updates/

https://derflounder.wordpress.com/2014/12/17/forcing-xprotect-blacklist-updates-on-mavericks-and-yosemite/

Rationale:

It is important that a system has the newest updates applied so as to prevent unauthorized persons from exploiting identified vulnerabilities.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Open a terminal session and enter the following command:

```
defaults read /Library/Preferences/com.apple.SoftwareUpdate
AutomaticCheckEnabled
```

2. Make sure the result is: `1`

If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Remediation:

Perform the following to implement the prescribed state:
Open a terminal session and enter the following command to enable the auto update feature:

```
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
AutomaticCheckEnabled -int 1
```

Impact:

Without automatic update, updates may not be made in a timely manner and the system will be exposed to additional risk.

1.3 Enable app update installs (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that application updates are installed after they are available from Apple. These updates do not require reboots or admin privileges for end users.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited

Audit:

1. Open *System Preferences*
2. Select App Store
3. Select Install app updates
4. Verify that all available updates and software patches are installed.

Alternatively:
Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.commerce AutoUpdate
```

2. Verify the value returned is 1.

Remediation:

Perform the following to implement the prescribed state:

1. Open a terminal session and enter the following command to enable the auto update feature:

```
sudo defaults write /Library/Preferences/com.apple.commerce AutoUpdate -bool
TRUE
```

The remediation requires a log out and log in to show in the GUI. Please note that.

Impact:

Unpatched software may be exploited

1.4 Enable system data files and security update installs (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that system and security updates are installed after they are available from Apple. This setting enables definition updates for XProtect and Gatekeeper, with this setting in place new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require reboots or end user admin rights.

http://www.thesafemac.com/tag/xprotect/

https://support.apple.com/en-us/HT202491

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited

Audit:

1. Open *System Preferences*
2. Select App Store
3. Select install system data files and security updates
4. Verify that all available updates and software patches are installed.

Alternatively:
Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.SoftwareUpdate | egrep
'(ConfigDataInstall|CriticalUpdateInstall)'
```

2. Make sure the result is: ConfigDataInstall = 1; CriticalUpdateInstall = 1;

If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Remediation:

Perform the following to implement the prescribed state:
Open a terminal session and enter the following command to enable install system data files and security updates:

```
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
ConfigDataInstall -bool true && sudo defaults write
/Library/Preferences/com.apple.SoftwareUpdate CriticalUpdateInstall -bool
true
```

Impact:

Unpatched software may be exploited

1.5 Enable macOS update installs (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that macOS updates are installed after they are available from Apple. This setting enables macOS updates to be automatically installed. Some environments will want to approve and test updates before they are delivered. It is best practice to test first where updates can and have caused disruptions to operations. Automatic updates should be turned off where changes are tightly controlled and there are mature testing and approval processes. Automatic updates should not be turned off so the admin can call the users first to let them know it's ok to install. A dependable repeatable process involving a patch agent or remote management tool should be in place before auto-updates are turned off.

Rationale:

Patches need to be applied in a timely manner to reduce the risk of vulnerabilities being exploited

Audit:

1. Open *System Preferences*
2. Select App Store
3. Select Install macOS updates
4. Verify that all available updates and software patches are installed.

Alternatively:
Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.commerce
AutoUpdateRestartRequired
```

2. Make sure the result is: 1

If automatic updates were selected during system set-up this setting may not have left an auditable artifact. Please turn off the check and re-enable when the GUI does not reflect the audited results.

Remediation:

Perform the following to implement the prescribed state:

1. Open a terminal session and enter the following command to enable install system data files and security updates:

```
sudo defaults write /Library/Preferences/com.apple.commerce
AutoUpdateRestartRequired -bool TRUE
```

Impact:

Unpatched software may be exploited

2 System Preferences

This section contains recommendations related to configurable options in the *System Preferences* panel.

2.1 Bluetooth

Bluetooth is a short-range, low-power wireless technology commonly integrated into portable computing and communication devices and peripherals. Bluetooth is best used in a secure environment where unauthorized users have no physical access near the Mac. If Bluetooth is used, it should be secured properly (see below).

2.1.1 Turn off Bluetooth, if no paired devices exist (Scored)

Profile Applicability:

- Level 1

Description:

Bluetooth devices use a wireless communications system that replaces the cables used by other peripherals to connect to a system. It is by design a peer-to-peer network technology and typically lacks centralized administration and security enforcement infrastructure.

Rationale:

Bluetooth is particularly susceptible to a diverse set of security vulnerabilities involving identity detection, location tracking, denial of service, unintended control and access of data and voice channels, and unauthorized device control and data access.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
defaults read /Library/Preferences/com.apple.Bluetooth ControllerPowerState
```

2. If the value returned is `0` the computer is compliant.
3. If the value returned is `1` that indicates that Bluetooth is enabled; the computer is compliant only if paired devices exist. Use the following step.
4. If the value returned in step 1 is `1` in the Terminal, run the following command:

```
system_profiler SPBluetoothDataType | grep "Bluetooth:" -A 20 | grep
Connectable
```

5. Output should include: Connectable: Yes

Remediation:

Perform the following to implement the prescribed state:

1. In a Terminal, run the following commands:

```
sudo defaults write /Library/Preferences/com.apple.Bluetooth
ControllerPowerState -int 0
```

```
sudo killall -HUP blued
```

Impact:

There have been many Bluetooth exploits, while Bluetooth can be hardened it does create a local wireless network that can be attacked to compromise both devices and information. Apple has emphasized the ease of use in Bluetooth devices so it is generally expected that Bluetooth will be used. Turning off Bluetooth with this control will also disable the Bluetooth sharing capability that is more strongly recommended against in control 2.4.7.

2.1.2 Turn off Bluetooth "Discoverable" mode when not pairing devices (Scored)

Profile Applicability:

- Level 1

Description:

When Bluetooth is set to discoverable mode, the Mac sends a signal indicating that it's available to pair with another Bluetooth device. When a device is "discoverable" it broadcasts information about itself and its location. Starting with OS X 10.9 Discoverable mode is enabled while the Bluetooth System Preference is open and turned off once closed. Systems that have the Bluetooth System Preference open at the time of audit will show as Discoverable.

Rationale:

When in the discoverable state an unauthorized user could gain access to the system by pairing it with a remote device.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
/usr/sbin/system_profiler SPBluetoothDataType | grep -i discoverable
```

2. Verify the value returned is Discoverable: Off

Remediation:

Perform the following to implement the prescribed state:
Starting with OS X (10.9) Bluetooth is only set to Discoverable when the Bluetooth System Preference is selected. To ensure that the computer is not Discoverable do not leave that preference open.

Impact:

The system will need to be made Discoverable in order to easily pair Bluetooth peripherals

2.1.3 Show Bluetooth status in menu bar (Scored)

Profile Applicability:

- Level 1

Description:

By showing the Bluetooth status in the menu bar, a small Bluetooth icon is placed in the menu bar. This icon quickly shows the status of Bluetooth, and can allow the user to quickly turn Bluetooth on or off.

Rationale:

Enabling "Show Bluetooth status in menu bar" is a security awareness method that helps understand the current state of Bluetooth, including whether it is enabled, Discoverable, what paired devices exist and are currently active.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read com.apple.systemuiserver menuExtras | grep Bluetooth.menu
```

2. Verify the value returned is: `/System/Library/CoreServices/Menu Extras/Bluetooth.menu`

Remediation:

In System Preferences: Bluetooth, turn Show Bluetooth Status In Menu Bar on.
Alternatively run the following in the command line:

```
defaults write com.apple.systemuiserver menuExtras -array-add
"/System/Library/CoreServices/Menu Extras/Bluetooth.menu"
```

If the remediation is run multiple times multiple instances of the Bluetooth status will appear after rebooting the system. Command-click and drag the unwanted icons off the menu bar
http://osxdaily.com/2012/01/05/remove-icons-menu-bar-mac-os-x/

Impact:

Bluetooth is a useful wireless tool that has been widely exploited when configured improperly. The user should have insight into the Bluetooth status.

2.2 Date & Time

This section contains recommendations related to the configurable items under the *Date & Time* panel.

2.2.1 Enable "Set time and date automatically" (Scored)

Profile Applicability:

- Level 1

Description:

Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries.

Note: If your organization has internal time servers, enter them here. Enterprise mobile devices may need to use a mix of internal and external time servers. If multiple servers are required use the Date & Time System Preference with each server separated by a space.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features.

Audit:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Date & Time*
3. Select *Set date and time automatically*

Alternatively run the following commands:
Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
sudo systemsetup -getusingnetworktime
```

2. Verify that the results are: `Network Time: On`

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Date & Time*
3. Select *Set date and time automatically*

Alternatively run the following commands:

```
sudo systemsetup -setnetworktimeserver <timeserver>
```

```
sudo systemsetup –setusingnetworktime on
```

Impact:

Apple's automatic time update solution will enable an NTP server that is not controlled by the Application Firewall. Turning on "Set time and date automatically" allows other computers to connect to set their time and allows for exploit attempts against ntpd. It also allows for more accurate network detection and OS fingerprinting

Current testing shows scanners can easily determine the MAC address and the OS vendor. More extensive OS fingerprinting may be possible.

2.2.2 Ensure time set is within appropriate limits (Scored)

Profile Applicability:

- Level 1

Description:

Correct date and time settings are required for authentication protocols, file creation, modification dates and log entries. Ensure that time on the computer is within acceptable limits. Truly accurate time is measured within milliseconds, for this audit a drift under four and a half minutes passes the control check. Since Kerberos is one of the important features of macOS integration into Directory systems the guidance here is to warn you before there could be an impact to operations. From the perspective of accurate time this check is not strict, it may be too great for your organization, adjust to a smaller offset value as needed.

Rationale:

Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes. This in turn can affect Apple's single sign-on feature, Active Directory logons, and other features. Audit check is for more than 4 minutes and 30 seconds ahead or behind.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
sudo systemsetup -getnetworktimeserver
```

2. Use "Network Time Server:" <your.time.server> to capture drift

```
sudo ntpdate -svd <your.time.server> | egrep offset
```

3. Ensure that the offset result(s) are smaller than 270.x or -270.x seconds

Remediation:

Perform the following to implement the prescribed state:

1. In Terminal, run the following command:

```
sudo systemsetup -getnetworktimeserver
```

2. Use "Network Time Server:" <your.time.server> to capture drift

```
sudo ntpdate -sv <your.time.server>
```

Impact:

Accurate time is required for many computer functions.

Notes:

The associated check will fail if no network connection is available.

2.3 Desktop & Screen Saver

This section contains recommendations related to the configurable items under the Desktop & Screen Saver panel.

2.3.1 Set an inactivity interval of 20 minutes or less for the screen saver (Scored)

Profile Applicability:

- Level 1

Description:

A locking screensaver is one of the standard security controls to limit access to a computer and the current user's session when the computer is temporarily unused or unattended. In macOS the screensaver starts after a value selected in a drop down menu, 10 minutes and 20 minutes are both options and either is acceptable. Any value can be selected through the command line or script but a number that is not reflected in the GUI can be problematic. 20 minutes is the default for new accounts.

Rationale:

Setting an inactivity interval for the screensaver prevents unauthorized persons from viewing a system left unattended for an extensive period of time.

Audit:

The preferred audit procedure for this control will evaluate every user account on the box and will report on all users where the value has been set. If the default value of 20 minutes is used and the user has never changed the setting there will not be an audit result on their compliant setting.
Perform the following to ensure the system is configured as prescribed:

```
UUID=`ioreg -rd1 -c IOPlatformExpertDevice | grep "IOPlatformUUID" | sed -e
's/^.* "(.*)"$/1/'`

for i in $(find /Users -type d -maxdepth 1)
do
  PREF=$i/Library/Preferences/ByHost/com.apple.screensaver.$UUID
  if [ -e $PREF.plist ]
  then
    echo -n "Checking User: '$i': "
    defaults read $PREF.plist idleTime 2>&1
  fi
done
```

Verify the setting is not 0 but is adequately low (< 1200)
Perform the following to ensure the system is configured as prescribed for the current logged in user:

1. In Terminal, run the following command:

```
defaults -currentHost read com.apple.screensaver idleTime
```

2. Verify the setting is not but is adequately low (< 1200)

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Desktop & Screen Saver*
3. Select *Screen_Saver*
4. Set *Start after* to 20 minutes or less

Alternatively:

1. In Terminal, run one of the the following commands:

```
defaults -currentHost write com.apple.screensaver idleTime -int 600
defaults -currentHost write com.apple.screensaver idleTime -int 1200
```

There are anomalies if the command line is used to make the setting something other than what is available in the GUI Menu. Choose either 10 minutes or 20 minutes,

Impact:

If the screensaver is not set users may leave the computer available for an unauthorized person to access information.

2.3.2 Secure screen saver corners (Scored)

Profile Applicability:

- Level 2

Description:

Hot Corners can be configured to disable the screen saver by moving the mouse cursor to a corner of the screen.

Rationale:

Setting a hot corner to disable the screen saver poses a potential security risk since an unauthorized person could use this to bypass the login screen and gain access to the system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. For all users, run the following command in Terminal:

```
defaults read ~/Library/Preferences/com.apple.dock | grep -i corner
```

2. Verify that `6` is not returned for any key value for any user.

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Mission Control*
3. Select *Hot Corners*
4. Remove any corners which are set to *Disable Screen Saver*

2.3.3 Set a screen corner to Start Screen Saver (Scored)

Profile Applicability:

- Level 1

Description:

The intent of this control is to resemble control-alt-delete on Windows Systems as a means of quickly locking the screen. If the user of the system is stepping away from the computer the best practice is to lock the screen and setting a hot corner is an appropriate method.

Rationale:

Ensuring the user has a quick method to lock their screen may reduce opportunity for individuals in close physical proximity of the device to see screen contents.

Audit:

In System Preferences: Desktop & Screen Saver: Screen Saver: Hot Corners, make sure at least one Active Screen Corner is set to Start Screen Saver. Make sure the user knows about this feature.
Alternatively, run the following command for each user:

```
defaults read ~/Library/Preferences/com.apple.dock | grep -i corner
```

For each user, verify at least one of the *-corner keys has a value of `5`. For example, `"wvous-tl-corner" = 5`.

Remediation:

In System Preferences: Desktop & Screen Saver: Screen Saver: Hot Corners, make sure at least one Active Screen Corner is set to Start Screen Saver. Make sure the user knows about this feature.
The screen corners can be set using the defaults command, but the permutations of combinations are many. The plist file to check is `~/Library/Preferences/com.apple.dock` and the keys are

```
wvous-bl-corner
wvous-br-corner
wvous-tl-corner
wvous-tr-corner
```

There are also modifier keys to check and various values for each of these keys. A value of `5` means the corner will start the screen saver. The corresponding wvous-xx-modifier key should be set to `0`.

2.4 Sharing

This section contains recommendations related to the configurable items under the *Sharing* panel.

2.4.1 Disable Remote Apple Events (Scored)

Profile Applicability:

- Level 1

Description:

Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer.

Rationale:

Disabling Remote Apple Events mitigates the risk of an unauthorized program gaining access to the system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo systemsetup -getremoteappleevents
```

2. Verify the value returned is `Remote Apple Events: Off`

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
sudo systemsetup -setremoteappleevents off
```

Impact:

With remote Apple events turned on, an AppleScript program running on another Mac can interact with the local computer.

2.4.2 Disable Internet Sharing (Scored)

Profile Applicability:

- Level 1

Description:

Internet Sharing uses the open source `natd` process to share an internet connection with other computers and devices on a local network. This allows the Mac to function as a router and share the connection to other, possibly unauthorized, devices.

Rationale:

Disabling Internet Sharing reduces the remote attack surface of the system.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
sudo defaults read /Library/Preferences/SystemConfiguration/com.apple.nat |
grep -i Enabled
```

The file should not exist or `Enabled = 0` for all network interfaces.

Remediation:

Perform the following to implement the prescribed state:

1. Open System Preferences
2. Select Sharing
3. Uncheck Internet Sharing

Impact:

Internet sharing allows the computer to function as a router and other computers to use it for access. This can expose both the computer itself and the networks it is accessing to unacceptable access from unapproved devices.

References:

1. STIGID AOSX-12-001270

2.4.3 Disable Screen Sharing (Scored)

Profile Applicability:

- Level 1

Description:

Screen sharing allows a computer to connect to another computer on a network and display the computer's screen. While sharing the computer's screen, the user can control what happens on that computer, such as opening documents or applications, opening, moving, or closing windows, and even shutting down the computer.

Rationale:

Disabling screen sharing mitigates the risk of remote connections being made without the user of the console knowing that they are sharing the computer.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo launchctl load
/System/Library/LaunchDaemons/com.apple.screensharing.plist
```

2. Verify the value returned is Service is disabled

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Sharing*
3. Uncheck *Screen Sharing*

References:

1. http://support.apple.com/kb/ph11151

2.4.4 Disable Printer Sharing (Scored)

Profile Applicability:

- Level 1

Description:

By enabling Printer sharing the computer is set up as a print server to accept print jobs from other computers. Dedicated print servers or direct IP printing should be used instead.

Rationale:

Disabling Printer Sharing mitigates the risk of attackers attempting to exploit the print server to gain access to the system.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
system_profiler SPPrintersDataType | egrep "Shared: Yes"
```

The output should be empty. If "Shared: Yes" is in the output there are still shared printers.

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Sharing*
3. Uncheck *Printer Sharing*

References:

1. http://support.apple.com/kb/PH11450

2.4.5 Disable Remote Login (Scored)

Profile Applicability:

- Level 1

Description:

Remote Login allows an interactive terminal connection to a computer.

Rationale:

Disabling Remote Login mitigates the risk of an unauthorized person gaining access to the system via Secure Shell (SSH). While SSH is an industry standard to connect to posix servers, the scope of the benchmark is for Apple macOS clients, not servers.

macOS does have an IP based firewall available (pf, ipfw has been deprecated) that is not enabled or configured. There are more details and links in section 7.5. macOS no longer has TCP Wrappers support built-in and does not have strong Brute-Force password guessing mitigations, or frequent patching of openssh by Apple. Most macOS computers are mobile workstations, managing IP based firewall rules on mobile devices can be very resource intensive. All of these factors can be parts of running a hardened SSH server.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo systemsetup -getremotelogin
```

2. Verify the value returned is `Remote Login: Off`

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
sudo systemsetup -setremotelogin off
```

Impact:

The SSH server built-in to macOS should not be enabled on a standard user computer, particularly one that changes locations and IP addresses. A standard user that runs local applications including email, web browser and productivity tools should not use the same device as a server. There are Enterprise management tool-sets that do utilize SSH, if they are in use, the computer should be locked down to only respond to known trusted IP addresses and appropriate admin service accounts.

For macOS computers that are being used for specialized functions there are several options to harden the SSH server to protect against unauthorized access including brute force attacks. There are some basic criteria that need to be considered:

- Do not open an SSH server to the internet without controls in place to mitigate SSH brute force attacks, this is particularly important for systems bound to Directory environments. It is great to have controls in place to protect the system but if they trigger after the user is already locked out of their account they are not optimal. If authorization happens after authentication directory accounts for users that don't even use the system can be locked out.
- Do not use SSH key pairs when there is no insight to the security on the client system that will authenticate into the server with a private key. If an attacker gets access to the remote system and can find the key they may not need a password or a key logger to access the SSH server.
- Detailed instructions on hardening an SSH server, if needed, are available in the CIS Linux Benchmarks but it is beyond the scope of this benchmark

Notes:

```
man sshd_config
```

2.4.6 Disable DVD or CD Sharing (Scored)

Profile Applicability:

- Level 1

Description:

DVD or CD Sharing allows users to remotely access the system's optical drive.

Rationale:

Disabling DVD or CD Sharing minimizes the risk of an attacker using the optical drive as a vector for attack and exposure of sensitive data.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
sudo launchctl list | egrep ODSAgent
```

If "com.apple.ODSAgent" appears in the result the control is not in place. No result is compliant.

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Sharing*
3. Uncheck *DVD or CD Sharing*

Impact:

Many Apple devices are now sold without optical drives and drive sharing may be needed for legacy optical media.

2.4.7 Disable Bluetooth Sharing (Scored)

Profile Applicability:

- Level 1

Description:

Bluetooth Sharing allows files to be exchanged with Bluetooth enabled devices.

Rationale:

Disabling Bluetooth Sharing minimizes the risk of an attacker using Bluetooth to remotely attack the system.

Audit:

Perform the following to check the current status:

1. Open System Preferences
2. Bluetooth Sharing should be unchecked

Alternatively:

1. Run the following command in Terminal:

```
system_profiler SPBluetoothDataType | grep State
```

2. Verify that all values are Disabled

Remediation:

Perform the following to implement the prescribed state:

1. Open System Preferences
2. Select Sharing
3. Uncheck Bluetooth Sharing

Impact:

Control 2.1.1 discusses disabling Bluetooth if no paired devices exist. There is a general expectation that Bluetooth peripherals will be used by most users in Apple's ecosystem, it is possible that sharing is required and Bluetooth peripherals are not. Bluetooth must be enabled if sharing is an acceptable use case.

2.4.8 Disable File Sharing (Scored)

Profile Applicability:

- Level 1

Description:

Apple's File Sharing uses a combination of SMB (Windows sharing) and AFP (Mac sharing)

Two common ways to share files using File Sharing are:

1. Apple File Protocol (AFP) AFP automatically uses encrypted logins, so this method of sharing files is fairly secure. The entire hard disk is shared to administrator user accounts. Individual home folders are shared to their respective user accounts. Users' "Public" folders (and the "Drop Box" folder inside) are shared to any user account that has sharing access to the computer (i.e. anyone in the "staff" group, including the guest account if it is enabled).
2. Server Message Block (SMB), Common Internet File System (CIFS) When Windows (or possibly Linux) computers need to access file shared on a Mac, SMB/CIFS file sharing is commonly used. Apple warns that SMB sharing stores passwords is a less secure fashion than AFP sharing and anyone with system access can gain access to the password for that account. When sharing with SMB, each user that will access the Mac must have SMB enabled.

Rationale:

By disabling file sharing, the remote attack surface and risk of unauthorized access to files stored on the system is reduced.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal to check the Apple File Server status:

```
sudo launchctl list | egrep AppleFileServer
```

2. Ensure no output is present
3. Run the following command in terminal to check the Windows File Server status

```
grep -i array
/Library/Preferences/SystemConfiguration/com.apple.smb.server.plist
```

4. Ensure no output is present

Remediation:

Perform the following to implement the prescribed state:

- Run the following command in Terminal to turn off AFP from the command line:

```
sudo launchctl unload -w
/System/Library/LaunchDaemons/com.apple.AppleFileServer.plist
```

- Run the following command in Terminal to turn off SMB sharing from the CLI:

```
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.smbd.plist
```

Impact:

File Sharing can be used to share documents with other users but hardened servers should be used rather than user endpoints. Turning on file sharing increases the visibility and attack surface of a system unnecessarily.

2.4.9 Disable Remote Management (Scored)

Profile Applicability:

- Level 1

Description:

Remote Management is the client portion of Apple Remote Desktop (ARD). Remote Management can be used by remote administrators to view the current Screen, install software, report on, and generally manage client Macs.

The screen sharing options in Remote Management are identical to those in the Screen Sharing section. In fact, only one of the two can be configured. If Remote Management is used, refer to the Screen Sharing section above on issues regard screen sharing.

Remote Management should only be enabled when a Directory is in place to manage the accounts with access. Computers will be available on port 5900 on a macOS System and could accept connections from untrusted hosts depending on the configuration, definitely a concern for mobile systems.

Rationale:

Remote management should only be enabled on trusted networks with strong user controls present in a Directory system. Mobile devices without strict controls are vulnerable to exploit and monitoring.

Audit:

Perform the following check to ensure the remote management process is not running and the system is configured as prescribed:

1. Run the following command in Terminal:

```
ps -ef | egrep ARDAgent
```

2. Ensure `/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent` is not present as a running process.

Remediation:

In System Preferences: Sharing, turn off Remote Management.

Impact:

Many organizations utilize ARD for client management.

Notes:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources
/kickstart -help
```

2.5 Energy Saver

This section contains recommendations related to the configurable items under the *Energy Saver* panel.

2.5.1 Disable "Wake for network access" (Scored)

Profile Applicability:

- Level 1

Description:

This feature allows other users to be able to access your computer's shared resources, such as shared printers or iTunes playlists, even when your computer is in sleep mode. In a closed network when only authorized devices could wake a computer it could be valuable to wake computers in order to do management push activity. Where mobile workstations and agents exist the device will more likely check in to receive updates when already awake. Mobile devices should not be listening for signals on unmanaged network where untrusted devices could send wake signals.

Rationale:

Disabling this feature mitigates the risk of an attacker remotely waking the system and gaining access.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
pmset -g | egrep womp
```

verify the value returned is: " womp 0"

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
sudo pmset -a womp 0
```

Impact:

Management programs like Apple Remote Desktop Administrator use this feature to wake computers. If turned off, such management programs will not be able to wake a computer over the LAN. If the wake-on-LAN feature is needed, do not turn off this feature.

The control to prevent computer sleep has been retired for this version of the Benchmark. Forcing the computer to stay on and use energy in case a management push is needed is contrary to most current management processes. Only keep computers unslept if after hours pushes are required on closed LANs.

Notes:

```
man pmset
```

2.6 Security & Privacy

This section contains recommendations for configurable options under the *Security & Privacy* panel.

2.6.1 Encryption

Apple has created simple easy to use encryption capabilities built-in to macOS. In order to protect data and privacy those tools need to be utilized to protect information processed by macOS computers.

2.6.1.1 Enable FileVault (Scored)

Profile Applicability:

- Level 1

Description:

FileVault secures a system's data by automatically encrypting its boot volume and requiring a password or recovery key to access it.

Rationale:

Encrypting sensitive data minimizes the likelihood of unauthorized users gaining access to it.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
fdesetup status
```

2. A FileVault encrypted system will result in "FileVault is On."

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select *FileVault*
4. Select *Turn on FileVault*

Impact:

Mounting a FileVaulted volume from an alternate boot source will require a valid password to decrypt it.

Notes:

FileVault may not be desirable on a virtual OS. As long as the hypervisor and file storage are encrypted the virtual OS does not need to be. Rather than checking if the OS is virtual and passing the control regardless of the encryption of the host system the normal check will be run. Security officials can evaluate the comprehensive controls outside of the OS being tested.

2.6.1.2 Ensure all user storage CoreStorage volumes are encrypted (Not Scored)

Profile Applicability:

- Level 1

Description:

Apple introduced Core Storage with 10.7. It is used as the default for formatting on macOS volumes prior to 10.13.

All HFS and Core Storage Volumes should be encrypted.

Rationale:

In order to protect user data from loss or tampering volumes carrying data should be encrypted.

Audit:

run diskutil cs list
Ensure all "Logical Volume Family" disks are encrypted
Example:

```
CoreStorage logical volume groups (2 found)
|
+-- Logical Volume Group XXXXX
|   =========================================================
|   Name:         Macintosh HD
|   Status:       Online
|   Size:         250160967680 B (250.2 GB)
|   Free Space:   6516736 B (6.5 MB)
|   |
|   +-< Physical Volume XXXXXY
|   |   ----------------------------------------------------
|   |   Index:    0
|   |   Disk:     disk0s2
|   |   Status:   Online
|   |   Size:     250160967680 B (250.2 GB)
|   |
|   +-> Logical Volume Family XXXXXYY
|       ----------------------------------------------------------
|       Encryption Type:         AES-XTS
|       Encryption Status:       Unlocked
|       Conversion Status:       Complete
|       High Level Queries:      Fully Secure
|       |                        Passphrase Required
|       |                        Accepts New Users
```

```
|       |                       Has Visible Users
|       |                       Has Volume Key
|       |
|       +-> Logical Volume XXXXXYYY
|           ---------------------------------------------------
|           Disk:                   disk2
|           Status:                 Online
|           Size (Total):           249802129408 B (249.8 GB)
|           Revertible:             Yes (unlock and decryption required)
|           LV Name:                Macintosh HD
|           Volume Name:            Macintosh HD
|           Content Hint:           Apple_HFS
|
+-- Logical Volume Group XXXXXYYYY
    =========================================================
    Name:         Passport
    Status:       Online
    Size:         119690149888 B (119.7 GB)
    Free Space:   1486848 B (1.5 MB)
    |
    +-< Physical Volume XXXXXYYY
    |   ----------------------------------------------------
    |   Index:    0
    |   Disk:     disk3s2
    |   Status:   Online
    |   Size:     119690149888 B (119.7 GB)
    |
    +-> Logical Volume Family XXXXXYYYYY
        ----------------------------------------------------------
        Encryption Type:         AES-XTS
        Encryption Status:       Unlocked
        Conversion Status:       Complete
        High Level Queries:      Fully Secure
        |                        Passphrase Required
        |                        Accepts New Users
        |                        Has Visible Users
        |                        Has Volume Key
        |
        +-> Logical Volume XXXXXYYYYYY
            ---------------------------------------------------
            Disk:                   disk4
            Status:                 Online
            Size (Total):           119336337408 B (119.3 GB)
            Revertible:             No
            LV Name:                Passport
            Volume Name:            Passport
            Content Hint:           Apple_HFS
```

Remediation:

Use Disk Utility to erase a disk and format as macOS Extended (Journaled, Encrypted)

Impact:

While FileVault protects the boot volume data may be copied to other attached storage and reduce the protection afforded by FileVault. Ensure all user volumes are encrypted to protect data.

2.6.2 Enable Gatekeeper (Scored)

Profile Applicability:

- Level 1

Description:

Gatekeeper is Apple's application white-listing control that restricts downloaded applications from launching. It functions as a control to limit applications from unverified sources from running without authorization.

Rationale:

Disallowing unsigned software will reduce the risk of unauthorized or malicious applications from running on the system.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
sudo spctl --status
```

Ensure the above command outputs "`assessments enabled`".

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select *General*
4. Select Allow applications downloaded from: Mac App Store and identified developers

Alternatively, perform the following to ensure the system is configured as:
Run the following command in Terminal:

```
sudo spctl --master-enable
```

2.6.3 Enable Firewall (Scored)

Profile Applicability:

- Level 1

Description:

A firewall is a piece of software that blocks unwanted incoming connections to a system. Apple has posted general documentation about the application firewall.

http://support.apple.com/en-us/HT201642

Rationale:

A firewall minimizes the threat of unauthorized users from gaining access to your system while connected to a network or the Internet.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.alf globalstate
```

2. Verify the value returned is `1` or `2`

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select *Firewall*
4. Select *Turn On Firewall*

Alternatively:

1. Run the following command in Terminal:

```
defaults write /Library/Preferences/com.apple.alf globalstate - int <value>
```

2. Where `<value>` is:

- `1` = on for specific services
- `2` = on for essential services

Impact:

The firewall may block legitimate traffic. Applications that are unsigned will require special handling.

Notes:

http://docs.info.apple.com/article.html?artnum=306938

2.6.4 Enable Firewall Stealth Mode (Scored)

Profile Applicability:

- Level 1

Description:

While in Stealth mode the computer will not respond to unsolicited probes, dropping that traffic.

http://support.apple.com/en-us/HT201642

Rationale:

Stealth mode on the firewall minimizes the threat of system discovery tools while connected to a network or the Internet.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
/usr/libexec/ApplicationFirewall/socketfilterfw --getstealthmode
```

2. Verify the value returned is Stealth mode enabled

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select *Firewall Options*
4. Select *Enable stealth mode*

Alternatively:
Run the following command in Terminal:

```
sudo /usr/libexec/ApplicationFirewall/socketfilterfw --setstealthmode on
```

Impact:

Traditional network discovery tools like ping will not succeed. Other network tools that measure activity and approved applications will work as expected.

This control aligns with the primary macOS use case of a laptop that is often connected to untrusted networks where host segregation may be non-existent. In that use case hiding from the other inmates is likely more than desirable. In use cases where use is only on trusted LANs with static IP addresses stealth mode may not be desirable.

Notes:

http://docs.info.apple.com/article.html?artnum=306938

2.6.5 Review Application Firewall Rules (Scored)

Profile Applicability:

- Level 1

Description:

A firewall is a piece of software that blocks unwanted incoming connections to a system. Apple has posted general documentation about the application firewall.

http://support.apple.com/en-us/HT201642

A computer should have a limited number of applications open to incoming connectivity. This rule will check for whether there are more than 10 rules for inbound connections.

Rationale:

A firewall minimizes the threat of unauthorized users from gaining access to your system while connected to a network or the Internet. Which applications are allowed access to accept incoming connections through the firewall is important to understand.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
/usr/libexec/ApplicationFirewall/socketfilterfw --listapps
```

2. Verify that the number of rules returned is lower than 10

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select *Firewall Options*
4. Select unneeded rules
5. Select the minus sign below to delete them

Alternatively:

1. Edit and run the following command in Terminal to remove specific applications:

```
/usr/libexec/ApplicationFirewall/socketfilterfw --remove
</Applications/badapp.app>
```

2. Where `</Applications/badapp.app>` is the one to be removed

2.6.6 Enable Location Services (Not Scored)

Profile Applicability:

- Level 2

Description:

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. Users do not need to change the time or the time zone, the computer will do it for them. They do not need to specify their location for weather or travel times and even get alerts on travel times to meetings and appointment where location information is supplied.

For the purpose of asset management and time and log management with mobile computers location services simplify some processes.

There are some use cases where it is important that the computer not be able to report it's exact location. While the general use case is to enable Location Services, it should not be allowed if the physical location of the computer and the user should not be public knowledge.

https://support.apple.com/en-us/HT204690

Rationale:

Location services are helpful in most use cases and can simplify log and time management where computers change time zones.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
sudo launchctl load /System/Library/LaunchDaemons/com.apple.locationd.plist
```

2. Verify that the results include: "Operation already in progress" or "service already loaded"

Remediation:

Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
sudo launchctl load /System/Library/LaunchDaemons/com.apple.locationd.plist
```

2. There should be no response

In some use cases organizations may not want Location Services running in those cases "unload" rather than "load" is the appropriate command
Perform the following to ensure the system is configured as prescribed:

1. In Terminal, run the following command:

```
sudo launchctl unload /System/Library/LaunchDaemons/com.apple.locationd.plist
```

2. Verify that the results include: Could not find specified service

2.6.7 Monitor Location Services Access (Not Scored)

Profile Applicability:

- Level 2

Description:

macOS uses location information gathered through local Wi-Fi networks to enable applications to supply relevant information to users. While location services may be very useful it may not be desirable to allow all applications that can use location services to use your location for Internet queries to provide tailored content based on your current location.

Ensure that the applications that can use Location Services are authorized to use that information and provide that information where the application interacts with external systems. Apple provides feedback within System Preferences and may be enabled to provide information on the menu bar when Location Services are used.

Safari can deny access from websites or prompt for access.

Applications that support Location Services can be individually controlled in the Privacy tab in Security & Privacy under System Preferences.

Access should be evaluated to ensure that privacy controls are as expected.

Rationale:

Privacy controls should be monitored for appropriate settings

Audit:

Perform the following to ensure the system is configured as prescribed for the current user
Evaluate Applications that are enabled to use Location Services

```
sudo defaults read /var/db/locationd/clients.plist
```

Ensure applications should be authorized to access Location information

Remediation:

Safari Configuration
Perform the following to implement the prescribed state:

```
1. Open Safari
2. Select Safari from the menu bar
3. Select Websites
4. Select Location
5. When visiting other websites should be set to Ask or Deny
```

Perform the following to review applications in System Preferences:

```
1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Location Services
5. Uncheck applications that are not approved for access to location service
information
```

Impact:

Many macOS services rely on location services for tailored services. Users expect their time zone and weather to be relevant to where they are without manual intervention. Find my Mac does need to know where your Mac actually is. Where possible the tolerance between location privacy and convenience may be best left to the user when the location itself is not sensitive. If facility locations are not public location information should be tightly controlled

2.6.8 Disable sending diagnostic and usage data to Apple (Scored)

Profile Applicability:

- Level 2

Description:

Apple provides a mechanism to send diagnostic and usage data back to Apple to help them improve the platform. Diagnostics and usage information may contain internal organizational information that should be controlled and not available for processing by Apple. Turn off Share Mac Analytics.

Rationale:

Organizations should have knowledge of what is shared with the vendor and the setting automatically forwards information to Apple.

Audit:

Perform the following to review the current state:

```
1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Analytics
5. Ensure that "Share Mac Analytics" is not selected
```

Remediation:

Perform the following to implement the prescribed state:

```
1. Open System Preferences
2. Select Security & Privacy
3. Select Privacy
4. Select Analytics
5. Deselect "Share Mac Analytics"
```

2.7 iCloud

iCloud is Apple's service for synchronizing, storing and backing up data from Apple applications in both macOS and iOS

2.7.1 iCloud configuration (Not Scored)

Profile Applicability:

- Level 2

Description:

Apple's iCloud is a consumer oriented service that allows a user to store data as well as find, control and backup devices that are associated with their Apple ID (Apple account.) The use of iCloud on Enterprise devices should align with the acceptable use policy for devices that are managed as well as confidentiality requirements for data handled by the user. If iCloud is allowed the data that is copied to Apple servers will likely be duplicated on both personal as well as Enterprise devices.

For many users the Enterprise email system may replace many of the available features in iCloud. If using either an Exchange or Google environment email, calendars, notes and contacts can sync to the official Enterprise repository and be available through multiple devices.

Depending on workplace requirements it may not be appropriate to intermingle Enterprise and personal bookmarks, photos and documents. Since the service allows every device associated with the users ID to synchronize and have access to the cloud storage the concern is not just about having sensitive data on Apple's servers but having that same data on the phone of the teenage son or daughter of an employee. The use of family sharing options can reduce the risk.

The remote connectivity of "Back to My Mac" relies on screen sharing that should already be turned off, if available the users Apple ID (personal?) can be used for remote access to the Enterprise computer rather than through Enterprise managed accounts.

Apple's iCloud is just one of many cloud based solutions being used for data synchronization across multiple platforms and it should be controlled consistently with other cloud services in your environment. Work with your employees and configure the access to best enable data protection for your mission.

Rationale:

Organizations must make a risk decision on how their computers will interact with public cloud services.

Audit:

Review enabled and connected iCloud services.

```
defaults read ~/Library/Preferences/MobileMeAccounts.plist
```

Remediation:

Disable unapproved services in System Preferences > iCloud.
Use a profile to disable services where organizationally required.

Impact:

iCloud services are integrated deeply into macOS and in many cases are expected to be used by Mac users. iCloud is a public cloud and is not covered by organizational security plans. In many cases synchronizing user data from an organizational computers to an uncontrolled location, no matter who is the data owner, is unacceptable.

2.7.2 iCloud keychain (Not Scored)

Profile Applicability:

- Level 2

Description:

The iCloud keychain is Apple's password manager that works with macOS and iOS. The capability allows users to store passwords in either iOS or macOS for use in Safari on both platforms and other iOS integrated applications. The most pervasive use is driven by iOS use rather than macOS. The passwords stored in an macOS keychain on an Enterprise managed computer could be stored in Apple's cloud and then be available on a personal computer using the same account. The stored passwords could be for organizational as well as for personal accounts.

If passwords are no longer being used as organizational tokens they are not in scope for iCloud keychain storage.

Rationale:

Ensure that the iCloud keychain is used consistently with organizational requirements

Audit:

Review KEYCHAIN_SYNC in

```
defaults read ~/Library/Preferences/MobileMeAccounts.plist
```

Remediation:

Open System Preferences: iCloud and deselect Keychain if it is not approved in your organization.

2.7.3 iCloud Drive (Not Scored)

Profile Applicability:

- Level 2

Description:

iCloud Drive is Apple's storage solution for applications on both macOS and iOS to use the same files that are resident in Apple's cloud storage. The iCloud Drive folder is available much like Dropbox, Microsoft OneDrive or Google Drive.

One of the concerns in public cloud storage is that proprietary data may be inappropriately stored in an end user's personal repository. Organizations that need specific controls on information should ensure that this service is turned off or the user knows what information must be stored on services that are approved for storage of controlled information.

Rationale:

Organizations should review third party storage solutions pertaining to existing data confidentiality and integrity requirements.

Audit:

Review

```
defaults read ~/Library/Preferences/MobileMeAccounts.plist
```

Specific settings to review include

- CLOUDDESKTOP
- MOBILE_DOCUMENTS

Remediation:

If cloud storage is not allowed in your organization in System Preferences: iCloud uncheck iCloud Drive.

Impact:

Users will not be able to use continuity on macOS to resume the use of newly composed but unsaved files

2.7.4 iCloud Drive Document sync (Scored)

Profile Applicability:

- Level 2

Description:

With macOS 10.12 Apple introduced the capability to have a user's Documents folder automatically synchronize to the user's iCloud Drive, providing they have enough room purchased through Apple on their iCloud drive. This capability mirrors what Microsoft is doing with the use of OneDrive and Office 365. There are concerns with using this capability.

The storage space that Apple provides for free is used by users with iCloud mail, all of a user's Photo Library created with the ever larger Multi-Pixel iPhone cameras and all of the iOS Backups. Adding a synchronization capability for users who have files going back a decade or more and storage may be tight without much larger Apple charges than the free 5GB. Users with multiple computers running 10.12 and above with unique content on each will have issues as well.

Enterprise users may not be allowed to store Enterprise information in a third party public cloud. In previous implementations iCloud Drive or even DropBox the user selected what files were synchronized even if there were no other controls. The new feature synchronizes all files in a folder widely used to put working files.

The automatic synchronization of all files in a user's Documents folder should be disabled.

https://derflounder.wordpress.com/2016/09/23/icloud-desktop-and-documents-in-macos-sierra-the-good-the-bad-and-the-ugly/

Rationale:

Automated Document synchronization should be planned and controlled to approved storage.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
ls -l ~/Library/Mobile?/Documents/com~apple~CloudDocs/Documents/ | grep total
```

2. There should be no result

Remediation:

Perform the following to implement the prescribed state:

1. Open System Preferences
2. Select iCloud
3. Select iCloud Drive
4. Select Options next to iCloud Drive
5. Uncheck Desktop & Documents Folders

Impact:

Users will not be able to use iCloud for automatic Documents sync.

2.7.5 iCloud Drive Desktop sync (Scored)

Profile Applicability:

- Level 2

Description:

With macOS 10.12 Apple introduced the capability to have a user's Desktop folder automatically synchronize to the user's iCloud Drive, providing they have enough room purchased through Apple on their iCloud drive. This capability mirrors what Microsoft is doing with the use of OneDrive and Office 365. There are concerns with using this capability.

The storage space that Apple provides for free is used by users with iCloud mail, all of a user's Photo Library created with the ever larger Multi-Pixel iPhone cameras and all of the iOS Backups. Adding a synchronization capability for users who have files going back a decade or more and storage may be tight without much larger Apple charges than the free 5GB. Users with multiple computers running 10.12 and above with unique content on each will have issues as well.

Enterprise Users may not be allowed to store Enterprise information in a third party public cloud. In previous implementations iCloud Drive or even DropBox the user selected what files were synchronized even if there were no other controls. The new features synchronize all files in a folder widely used to put working files.

The automatic synchronization of all files in a user's Desktop folder should be disabled

https://derflounder.wordpress.com/2016/09/23/icloud-desktop-and-documents-in-macos-sierra-the-good-the-bad-and-the-ugly/

Rationale:

Automated Desktop synchronization should be planned and controlled to approved storage.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
ls -l ~/Library/Mobile?/Documents/com~apple~CloudDocs/Desktop/ | grep total
```

2. There should be no result

Remediation:

Perform the following to implement the prescribed state:

1. Open System Preferences
2. Select iCloud
3. Select iCloud Drive
4. Select Options next to iCloud Drive
5. Uncheck Desktop & Documents Folders

Impact:

Users will not be able to use iCloud for automatic Desktop sync.

2.8 Time Machine

One of the most important IT Operational concerns is to ensure that information is protected against loss or tampering. The purpose of the IT devices is to process the data after all. At one time the cost of IT equipment and the volume of the data might make the protection of the equipment itself more important, at this point the vast size of data archives and the lower cost of end user equipment makes data protection central to operational planning. Backup strategies are generally focused on ensuring that there are multiple copies of relevant versions of user files. The plan is that no single hardware or software loss or failure will result in major data loss.

Apple introduced Time Machine in 2007 as a simple to use built-in mechanism for users to ensure that their machine was backed up and if there was a mistake or loss information could be easily recovered. There are other solutions to ensure information is protected including several Enterprise solutions and simple drive or directory cloning.

The controls in this section are specifically about FileVault. The general ideas are applicable to any data backup solution.

2.8.1 Time Machine Auto-Backup (Scored)

Profile Applicability:

- Level 2

Description:

Backup solutions are only effective if the backups run on a regular basis. The time to check for backups is before the hard drive fails or the computer goes missing. In order to simplify the user experience so that backups are more likely to occur Time Machine should be on and set to Back Up Automatically whenever the target volume is available.

Operational staff should ensure that backups complete on a regular basis and the backups are tested to ensure that file restoration from backup is possible when needed.

Backup dates are available even when the target volume is not available in the Time Machine plist.

SnapshotDates = (

"2012-08-20 12:10:22 +0000",

"2013-02-03 23:43:22 +0000",

"2014-02-19 21:37:21 +0000",

"2015-02-22 13:07:25 +0000",

"2016-08-20 14:07:14 +0000"

When the backup volume is connected to the computer more extensive information is available through tmutil. See man tmutil

Rationale:

Backups should automatically run whenever the backup drive is available.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.TimeMachine.plist AutoBackup
```

The output should not be `0`
If Time Machine has never been used, and is not configured there will not be an AutoBackup flag to check. After it has been set-up it should be configured correctly

2. Check Snapshot Dates for approved backup frequency

```
defaults read /Library/Preferences/com.apple.TimeMachine.plist AutoBackup
```

"SnapshotDates= (" contains the five most recent dates

Remediation:

Perform the following to configure the system as prescribed:
Run the following command in Terminal:

```
defaults write /Library/Preferences/com.apple.TimeMachine.plist AutoBackup 1
```

Impact:

The backup will run periodically in the background and could have user impact while running.

2.8.2 Time Machine Volumes Are Encrypted (Scored)

Profile Applicability:

- Level 1

Description:

One of the most important security tools for data protection on macOS is FileVault. With encryption in place it makes it difficult for an outside party to access your data if they get physical possession of the computer. One very large weakness in data protection with FileVault is the level of protection on backup volumes. If the internal drive is encrypted but the external backup volume that goes home in the same laptop bag is not it is self-defeating. Apple tries to make this mistake easily avoided by providing a checkbox to enable encryption when setting-up a time machine backup. Using this option does require some password management, particularly if a large drive is used with multiple computers. A unique complex password to unlock the drive can be stored in keychains on multiple systems for ease of use.

While some portable drives may contain non-sensitive data and encryption may make interoperability with other systems difficult backup volumes should be protected just like boot volumes.

Rationale:

Backup volumes need to be encrypted

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
tmutil destinationinfo | grep -i NAME
```

Result should be formatted as

```
Name          : TMbackup
```

All "Local" drives should be encrypted
Perform the following to ensure the system is configured as prescribed:

2. Run the following command in Terminal:

```
diskutil info TMbackup | grep -i Encrypted
```

Results should be:

```
Encrypted:                Yes
```

All Time Machine targets identified in Step 1 should show an encrypted status in step 2

Remediation:

Ensure that backup volumes are encrypted using the Time Machine control or using Disk Utility

2.9 Pair the remote control infrared receiver if enabled (Scored)

Profile Applicability:

- Level 1

Description:

An infrared receiver is a piece of hardware that sends information from an infrared remote control to another device by receiving and decoding signals. If a remote is used with a computer, a specific remote, or "pair", can be set-up to work with the computer. This will allow only the paired remote to work on that computer. If a remote is needed the receiver should only be accessible by a paired device. Many models do not have infrared hardware. The audit check looks for the hardware first.

Rationale:

An infrared remote can be used from a distance to circumvent physical security controls. A remote could also be used to page through a document or presentation, thus revealing sensitive information.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
system_profiler 2>/dev/null | egrep "IR Receiver"
```

2. If "IR Receiver" information is returned run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.driver.AppleIRController
```

3. Verify the value returned for `DeviceEnabled = 0`; If the value returned is `DeviceEnabled = 1`, then verify the value returned for the `UIDFilter` does not equal `none`

Remediation:

Perform one of the following to implement the prescribed state:
Disable the remote control infrared receiver:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select the *General* tab
4. Select *Advanced*
5. Check *Disable remote control infrared receiver*

Pair a remote control infrared receiver:

1. Holding the remote close to the computer, point the remote at the front of the computer.
2. Pair the Apple Remote.

- If you have an Apple Remote with seven buttons, press and hold both the Right and Menu buttons on the remote until the paired-remote icon appears on your screen
- If you have an Apple Remote with six buttons, press and hold both the Next and Menu buttons on the remote until the paired-remote icon appears on your screen

References:

1. http://support.apple.com/kb/PH11060

2.10 Enable Secure Keyboard Entry in terminal.app (Scored)

Profile Applicability:

- Level 1

Description:

Secure Keyboard Entry prevents other applications on the system and/or network from detecting and recording what is typed into Terminal.

Rationale:

Enabling Secure Keyboard Entry minimizes the risk of a key logger from detecting what is entered in Terminal.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read -app Terminal SecureKeyboardEntry
```

2. Verify the value returned is `1`.

Remediation:

Perform the following to implement the prescribed state:

1. Open *Terminal*
2. Select *Terminal*
3. Select *Secure Keyboard Entry*

Notes:

http://docs.info.apple.com/article.html?path=Terminal/2.1/en/5386.html

2.11 Java 6 is not the default Java runtime (Scored)

Profile Applicability:

- Level 2

Description:

Apple had made Java part of the core Operating System for macOS. Apple is no longer providing Java updates for macOS and updated JREs and JDK are made available by Oracle. The latest version of Java 6 made available by Apple has many unpatched vulnerabilities and should not be the default runtime for Java applets that request one from the Operating System

Rationale:

Java has been one of the most exploited environments and Java 6, which was provided as an OS component by Apple, is no longer maintained by Apple or Oracle. The old versions provided by Apple are both unsupported and missing the more modern security controls that have limited current exploits. The EOL version may still be installed and should be removed from the computer or not be in the default path.

Audit:

Old Java versions may still be installed and should be removed from the computer or not be in the default path.

```
java -version
```

The output of the above command should not return a result with Java 6:

- Java version "1.6.0_x"
- Java(TM) SE Runtime Environment (build 1.6.0_x)

Note: If Java is required the latest JDK or JRE can be downloaded from Oracle.

Remediation:

Java 6 can be removed completely or, if required Java applications will only work with Java 6, a custom path can be used. Apple is likely to finally pull the plug on Java 6 in upcoming macOS versions so any applications that still require Java 6 will likely soon be unavailable.

Impact:

Old applications may rely on either an Apple supplied version of Java 6 or an updated JDK.

2.12 Securely delete files as needed (Not Scored)

Profile Applicability:

- Level 2

Description:

In previous versions of macOS Apple included a capability to securely empty the trash that included overwrites of the existing data. With the wider use of FileVault and other encryption methods and the growing use of Solid State Drives the requirements have changed and the "Secure Empty Trash" capability has been removed from the GUI. For systems that are not using encryption and continue to use platter-based hard drives there is residual risk that deleted files can still be recovered from the file system.

In previous versions of the Benchmark srm was mentioned as an alternative to the removal of "Secure Empty Trash." With the release of macOS 10.12 srm has been removed. There is still an option to erase free space from the command line but Apple has warned that encryption is a better solution

From manual entry for diskutil

NOTE: This kind of secure erase is no longer considered safe

because modern devices have wear-leveling, block-sparing, and

possibly-persistent cache hardware. The modern solution for

quickly and securely erasing your data is strong encryption,

with which mere destruction of the key more or less instantly

renders your data irretrievable in practical terms.

To erase free space on the boot volume

```
diskutil secureErase freespace 0 /
```

Rationale:

Securely removing files mitigates the risk of an admin user on the system recovering sensitive files that the user has deleted. It is possible for anyone with physical access to the device to get access if FileVault is not used, or to recover deleted data if the FileVault volume is already mounted. Users and admins of computers containing sensitive information should be screened appropriately or additional security controls should be in place to prevent unauthorized access to sensitive information.

Impact:

Securely deleting files can take a long time, with FileVault in place the protection is erasing data within an already encrypted volume.

3 Logging and Auditing

This section provide guidance on configuring the logging and auditing facilities available in macOS

3.1 Enable security auditing (Scored)

Profile Applicability:

- Level 1

Description:

macOS's audit facility, `auditd`, receives notifications from the kernel when certain system calls, such as `open`, `fork`, and `exit`, are made. These notifications are captured and written to an audit log.

Rationale:

Logs generated by `auditd` may be useful when investigating a security incident as they may help reveal the vulnerable application and the actions taken by a malicious actor.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo launchctl list | grep -i auditd
```

2. Verify "`com.apple.auditd`" appears.

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
```

3.2 Configure Security Auditing Flags (Scored)

Profile Applicability:

- Level 2

Description:

Auditing is the capture and maintenance of information about security-related events.

Rationale:

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises or attacks that have occurred, have begun, or are about to begin. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo egrep "^flags:" /etc/security/audit_control
```

2. Ensure at least the following flags are present:

- `lo` - audit successful/failed login/logout events
- `ad` - audit successful/failed administrative events
- `fd` - audit successful/failed file deletion events
- `fm` - audit successful/failed file attribute modification events
- `-all` - audit all failed events across all audit classes

Note: excluding potentially noisy audit events may be ideal, depending on your use-case.

Remediation:

Perform the following to implement the prescribed state:

1. Open a terminal session and edit the `/etc/security/audit_control file`
2. Find the line beginning with "`flags`"
3. Add the following flags: `lo`, `ad`, `fd`, `fm`, `-all`.
4. Save the file.

3.3 Ensure security auditing retention (Scored)

Profile Applicability:

- Level 1

Description:

The macOS audit capability contains important information to investigate security or operational issues. This resource is only completely useful if it is retained long enough to allow technical staff to find the root cause of anomalies in the records.

Retention can be set to respect both size and longevity. To retain as much as possible under a certain size the recommendation is to use:

expire-after:60D OR 1G

More info in the man page man audit_control

Rationale:

The audit records need to be retained long enough to be reviewed as necessary.

Audit:

Run from the command line

```
sudo cat /etc/security/audit_control | egrep expire-after
```

Results should be the following or larger/higher

```
expire-after:60D OR 1G
```

Remediation:

Edit the /etc/security/audit_control file so that:
expire-after is at least 60D OR 1G

Impact:

The recommendation is that at least 60 days or 1 gigabyte of audit records are retained. Systems that very little remaining disk space may have issues retaining sufficient data.

3.4 Control access to audit records (Scored)

Profile Applicability:

- Level 1

Description:

The audit system on macOS writes important operational and security information that can be both useful for an attacker and a place for an attacker to attempt to obfuscate unwanted changes that were recorded. As part of defense-in-depth the /etc/security/audit_control configuration and the files in /var/audit should be owned only by root with group wheel with read only rights and no other access allowed. macOS ACLs should not be used for these files.

Rationale:

Audit records should never be changed except by the system daemon posting events. Records may be viewed or extracts manipulated but the authoritative files should be protected from unauthorized changes.

Audit:

Use ls -le to check file access rights.

```
ls -le /etc/security/audit_control
ls -le /var/audit/
```

All entries should be owned by root with group wheel with read access and no other access, including no ACLs
Example

```
-r--------  1 root  wheel  364 Jun 29 18:50 /etc/security/audit_control
and
-r--r-----  1 root  wheel    51240 Jun  4 05:34 20180604092609.crash_recovery
-r--r-----  1 root  wheel   900686 Jul  4 09:29 20180604094343.not_terminated
lrwxr-xr-x  1 root  wheel       40 Jun  4 05:43 current ->
/var/audit/20180604094343.not_terminated
```

The current symbolic link will have different Access Control

Remediation:

If the system has different access controls on the audit logs and the changes cannot be traced a new install may be prudent. Check for signs of file tampering as well as unapproved OS changes.

Impact:

This control is only checking the default configuration to ensure that unwanted access to audit records is not available.

Notes:

From ls man page

```
-e      Print the Access Control List (ACL) associated with the file, if
            present, in long (-l) output.
```

More info:

https://www.techrepublic.com/blog/apple-in-the-enterprise/introduction-to-os-x-access-control-lists-acls

http://ahaack.net/technology/OS-X-Access-Control-Lists-ACL.html

3.5 Retain install.log for 365 or more days (Scored)

Profile Applicability:

- Level 1

Description:

macOS writes information pertaining to system-related events to the file `/var/log/install.log` and has a configurable retention policy for this file. The default logging setting limits the file size of the logs and the maximum size for all logs. The default allows for an errant application to fill the log files and does not enforce sufficient log retention. The Benchmark recommends a value based on standard use cases. The value should align with local requirements within the organization.

The default value has an "all_max" file limitation, no reference to a minimum retention and a less precise rotation argument.

- The maximum file size limitation string should be removed "all_max="
- An organization appropriate retention should be added "ttl="
- The rotation should be set with time stamps "rotate=utc" or "rotate=local"

Rationale:

Archiving and retaining `install.log` for at least a year is beneficial in the event of an incident as it will allow the user to view the various changes to the system along with the date and time they occurred.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
grep -i ttl /etc/asl/com.apple.install
```

2. Verify that `ttl` is `365` or higher for install.log

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo vim /etc/asl/com.apple.install
```

2. Replace or edit the current setting with a compliant setting

```
* file /var/log/install.log mode=0640 format=bsd rotate=utc compress
file_max=5M ttl=365
```

Impact:

Without log files system maintenance and security forensics cannot be properly performed.

3.6 Ensure Firewall is configured to log (Scored)

Profile Applicability:

- Level 1

Description:

The socketfilter firewall is what is used when the firewall is turned on in the Security PreferencePane. In order to appropriately monitor what access is allowed and denied logging must be enabled.

Rationale:

In order to troubleshoot the successes and failures of a firewall logging should be enabled.

Audit:

Run

```
/usr/libexec/ApplicationFirewall/socketfilterfw --getloggingmode
```

Response is

```
Log mode is on
```

Remediation:

Run

```
/usr/libexec/ApplicationFirewall/socketfilterfw --setloggingmode on
```

Impact:

Detailed logging may result in excessive storage.

Notes:

More info:

http://krypted.com/tag/socketfilterfw/

4 Network Configurations

This section contains guidance on configuring the networking related aspects of macOS.

4.1 Disable Bonjour advertising service (Scored)

Profile Applicability:

- Level 2

Description:

Bonjour is an auto-discovery mechanism for TCP/IP devices which enumerate devices and services within a local subnet. DNS on macOS is integrated with Bonjour and should not be turned off, but the Bonjour advertising service can be disabled.

Rationale:

Bonjour can simplify device discovery from an internal rogue or compromised host. An attacker could use Bonjour's multicast DNS feature to discover a vulnerable or poorly-configured service or additional information to aid a targeted attack. Implementing this control disables the continuous broadcasting of "I'm here!" messages. Typical end-user endpoints should not have to advertise services to other computers. This setting does not stop the computer from sending out service discovery messages when looking for services on an internal subnet, if the computer is looking for a printer or server and using service discovery. To block all Bonjour traffic except to approved devices the pf or other firewall would be needed.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.mDNSResponder.plist
NoMulticastAdvertisements
```

2. Verify the value returned is `1`

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
defaults write /Library/Preferences/com.apple.mDNSResponder.plist
NoMulticastAdvertisements
```

Impact:

Some applications, like Final Cut Studio and AirPort Base Station management, may not operate properly if the `mDNSResponder` is turned off.

Notes:

Anything Bonjour discovers is already available on the network and probably discoverable with network scanning tools. The security benefit of disabling Bonjour for that reason is minimal.

4.2 Enable "Show Wi-Fi status in menu bar" (Scored)

Profile Applicability:

- Level 1

Description:

The Wi-Fi status in the menu bar indicates if the system's wireless internet capabilities are enabled. If so, the system will scan for available wireless networks to connect to. At the time of this revision all computers Apple builds have wireless network capability, which has not always been the case. This control only pertains to systems that have a wireless NIC available. Operating systems running in a virtual environment may not score as expected either.

Rationale:

Enabling "Show Wi-Fi status in menu bar" is a security awareness method that helps mitigate public area wireless exploits by making the user aware of their wireless connectivity status.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read com.apple.systemuiserver menuExtras | grep AirPort.menu
```

2. Verify the value returned is: `/System/Library/CoreServices/Menu Extras/AirPort.menu`

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select Network
3. Check *Show Wi-Fi status in menu bar*

Alternatively run the following in the command line:

```
Open /System/Library/CoreServices/Menu/Extras/AirPort.menu/
```

Impact:

The user of the system should have a quick check on their wireless network status available

Notes:

AirPort is Apple's marketing name for its 802.11b, g, and n wireless interfaces.

4.3 Create network specific locations (Not Scored)

Profile Applicability:

- Level 2

Description:

The network location feature of the Mac is very powerful tool to manage network security. By creating different network locations, a user can easily (and without administrative privileges) change the network settings on the Mac. By only using the network interfaces needed at any specific time, exposure to network attacks is limited.

A little understanding of how the Network System Preferences pane works is required.

Rationale:

Network locations allow the computer to have specific configurations ready for network access when required. Locations can be used to manage which network interfaces are available for specialized network access

Audit:

Open System Preferences: Network
Verify each network location is set up properly.

Remediation:

Create multiple network locations as needed.
Delete the Automatic location for any device that does not use multiple network services set for DHCP or dynamic addressing. If network services like FireWire, VPN, AirPort or Ethernet are not used by a specific device class those services should be deleted:

1. Select Edit Locations from the Locations popup menu.
2. Select the Automatic location.
3. Click the minus button for any unneeded service.

Impact:

Unneeded network interfaces increases the attack surface and could lead to a successful exploit.

Notes:

Deleting the Automatic location cannot be undone.

4.4 Ensure http server is not running (Scored)

Profile Applicability:

- Level 1

Description:

macOS used to have a graphical front-end to the embedded Apache web server in the Operating System. Personal web sharing could be enabled to allow someone on another computer to download files or information from the user's computer. Personal web sharing from a user endpoint has long been considered questionable and Apple has removed that capability from the GUI. Apache however is still part of the Operating System and can be easily turned on to share files and provide remote connectivity to an end user computer. Web sharing should only be done through hardened web servers and appropriate cloud services.

Rationale:

Web serving should not be done from a user desktop. Dedicated webservers or appropriate cloud storage should be used. Open ports make it easier to exploit the computer.

Audit:

Run the following in the terminal

```
ps -ef | grep -i httpd
```

There should be no results for /usr/sbin/httpd

Remediation:

Ensure that the Web Server is not running and is not set to start at boot
Stop the Web Server

```
sudo apachectl stop
```

Ensure that the web server will not auto-start at boot

```
sudo defaults write /System/Library/LaunchDaemons/org.apache.httpd Disabled -
bool true
```

Impact:

The web server is both a point of attack for the system and a means for unauthorized file transfers.

References:

1. STIGID AOSX-12-001275

4.5 Ensure FTP server is not running (Scored)

Profile Applicability:

- Level 1

Description:

macOS used to have a graphical front-end to the embedded FTP server in the Operating System. FTP sharing could be enabled to allow someone on another computer to download files or information from the user's computer. Running an FTP server from a user endpoint has long been considered questionable and Apple has removed that capability from the GUI. The FTP server however is still part of the Operating System and can be easily turned on to share files and provide remote connectivity to an end user computer. FTP servers meet a specialized need to distribute files without strong authentication and should only be done through hardened servers. Cloud services or other distribution methods should be considered

Rationale:

FTP servers should not be run on an end user desktop. Dedicated servers or appropriate cloud storage should be used. Open ports make it easier to exploit the computer.

Audit:

Run the following in the terminal

```
sudo launchctl list | egrep ftp
```

There should be no results for com.apple.ftpd

Remediation:

Ensure that the FTP Server is not running and is not set to start at boot
Stop the ftp Server

```
sudo -s launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
```

Impact:

The FTP server is both a point of attack for the system and a means for unauthorized file transfers. The FTP server is another avenue to attempt brute forcing password for existing valid users.

4.6 Ensure nfs server is not running (Scored)

Profile Applicability:

- Level 1

Description:

macOS can act as an NFS fileserver. NFS sharing could be enabled to allow someone on another computer to mount shares and gain access to information from the user's computer. File sharing from a user endpoint has long been considered questionable and Apple has removed that capability from the GUI. NFSD is still part of the Operating System and can be easily turned on to export shares and provide remote connectivity to an end user computer.

Rationale:

File serving should not be done from a user desktop, dedicated servers should be used. Open ports make it easier to exploit the computer.

Audit:

Run the following commands in the terminal

```
ps -ef | grep -i nfsd
```

There should be no results for /sbin/nfsd

```
cat /etc/exports
```

Should return "No such file or directory"

Remediation:

Ensure that the NFS Server is not running and is not set to start at boot
Stop the NFS Server

```
sudo nfsd disable
```

Remove the exported Directory listing

```
rm /etc/export
```

Impact:

The nfs server is both a point of attack for the system and a means for unauthorized file transfers.

5 System Access, Authentication and Authorization

System Access, Authentication and Authorization

5.1 File System Permissions and Access Controls

File system permissions have always been part of computer security. There are several principles that are part of best practices for a posix based system that are contained in this section, This section does not contain a complete list of every permission on a macOS System that might be problematic. Developers and use cases differ and what some admins long in the profession might consider a travesty a risk assessor steeped in BYOD trends may not give a second glance at. We are documenting here controls that should point out truly bad practices or anomalies that should be looked at and considered closely. Many of the controls are to mitigate the risk of privilege escalation attacks and data exposure to unauthorized parties.

5.1.1 Secure Home Folders (Scored)

Profile Applicability:

- Level 1

Description:

By default macOS allows all valid users into the top level of every other users home folder, and restricts access to the Apple default folders within. Another user on the same system can see you have a "Documents" folder but cannot see inside it. This configuration does work for personal file sharing but can expose user files to standard accounts on the system.

The best parallel for Enterprise environments is that everyone who has a Dropbox account can see everything that is at the top level but can't see your pictures, in the parallel with macOS they can see into every new Directory that is created because of the default permissions.

Home folders should be restricted to access only by the user. Sharing should be used on dedicated servers or cloud instances that are managing access controls. Some environments may encounter problems if execute rights are removed as well as read and write. Either no access or execute only for group or others is acceptable

Rationale:

Allowing all users to view the top level of all networked user's home folder may not be desirable since it may lead to the revelation of sensitive information.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
ls -l /Users/
```

2. Verify the value returned is either:

```
drwx------
```

```
drwx--x--x
```

Remediation:

Perform the following to implement the prescribed state:

1. Run one of the following commands in Terminal:

```
sudo chmod -R og-rwx /Users/<username>
```

```
sudo chmod -R og-rw /Users/<username>
```

2. Substitute user name in `<username>`.
3. This command has to be run for each user account with a local home folder.

Impact:

If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.

5.1.2 Check System Wide Applications for appropriate permissions (Scored)

Profile Applicability:

- Level 1

Description:

Applications in the System Applications Directory (/Applications) should be world executable since that is their reason to be on the system. They should not be world writable and allow any process or user to alter them for other processes or users to then execute modified versions

Rationale:

Unauthorized modifications of applications could lead to the execution of malicious code.

Audit:

Run the following from the command line

```
sudo find /Applications -iname "*.app" -type d -perm -2 -ls
```

Any applications discovered should be removed or changed. If changed the results should look like this:

```
drwxr-xr-x
```

Remediation:

Change permissions so that "Others" can only execute. (Example Below)

```
sudo chmod -R o-w /Applications/BadPermissions.app/
```

Impact:

Applications changed will no longer be world writable

5.1.3 Check System folder for world writable files (Scored)

Profile Applicability:

- Level 1

Description:

Software sometimes insists on being installed in the `/System` Directory and have inappropriate world writable permissions.

Rationale:

Folders in `/System` should not be world writable. The audit check excludes the "Drop Box" folder that is part of Apple's default user template.

Audit:

Check for Directories in `/System` that are world writable

```
sudo find /System -type d -perm -2 -ls | grep -v "Public/Drop Box"
```

Remediation:

Change permissions so that "Others" can only execute. (Example Below)

```
sudo chmod -R o-w /Bad/Directory
```

5.1.4 Check Library folder for world writable files (Scored)

Profile Applicability:

- Level 2

Description:

Software sometimes insists on being installed in the `/Library` Directory and have inappropriate world writable permissions.

Rationale:

Folders in `/Library` should not be world writable. The audit check excludes the `/Library/Caches` folder where the sticky bit is set.

Audit:

Check for Directories in `/Library` that are world writable

```
sudo find /Library -type d -perm -2 -ls | grep -v Caches
```

Remediation:

Change permissions so that "Others" can only execute. (Example Below)

```
sudo chmod -R o-w /Bad/Directory
```

5.2 Password Management

Password security is an important part of general IT security where passwords are in use. For macOS passwords are still much more widely used than other methods for account access. While there are other authentication and authorization methods for access from an macOS computer to organizational services, console access to the Mac is probably done using a password. This section contains password controls.

Recent updates based on research by NIST in SP800-63 call in to question traditional password complexity and rotation requirements. Sticky notes are not a password management program and password vault APIs are under increasing attack and ideally the user will remember their important passwords. The new understanding has informed changes to the previous password recommendations.

Length, Threshold and a yearly rotation requirement are the only scored controls below. Other controls will remain as unscored options. Passwords used for macOS are likely to also function as encryption keys for FileVault and depending on the information confidentiality on FileVault volumes stronger passwords may be required than are necessary to pass the controls in this Benchmark.

Apple supported solutions for managing local passwords on macOS are to use either an XML file that contains password rules that are imported with pwpolicy or through the use of a profile. In either case the controls in this section can be implemented with organizationally approved password policy.

Content is available where security hardening content is available and is native to Management suites and MDM tools.

Content also available here: https://github.com/ronc-LAemigre/macos-sec-config

NIST guidance on passwords starting at 5.1.1.1

https://pages.nist.gov/800-63-3/sp800-63b.html

5.2.1 Configure account lockout threshold (Scored)

Profile Applicability:

- Level 1

Description:

The account lockout threshold specifies the amount of times a user can enter an incorrect password before a lockout will occur.

Ensure that a lockout threshold is part of the password policy on the computer

Rationale:

The account lockout feature mitigates brute-force password attacks on the system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | grep -A 1
'policyAttributeMaximumFailedAuthentications' | tail -1 | cut -d'>' -f2 | cut
-d '<' -f1
```

2. Verify the value returned is 5 or lower

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

The number of incorrect log on attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user log on.

References:

1. STIGID AOSX-12-001324

5.2.2 Set a minimum password length (Scored)

Profile Applicability:

- Level 1

Description:

A minimum password length is the fewest number of characters a password can contain to meet a system's requirements.

Ensure that a minimum of a 15 character password is part of the password policy on the computer.

Where the confidentiality of encrypted information in FileVault is more of a concern requiring a longer password or passphrase may be sufficient rather than imposing additional complexity requirements that may be self-defeating.

Rationale:

Information systems that are not protected with strong password schemes including passwords of minimum length provide a greater opportunity for attackers to crack the password and gain access to the system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep "15 characters"
```

2. Verify the value returned

Password must be a minimum of 15 characters in length

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Short passwords can be easily attacked.

5.2.3 Complex passwords must contain an Alphabetic Character (Not Scored)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that an Alphabetic character is part of the password policy on the computer

Rationale:

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

Audit:

Perform one of the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep Alpha
```

2. Verify the value returned

RequiresAlpha
minimumAlphaCharacters

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep "1 letter"
```

2. Verify the value returned

Password must have at least 1 letter

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

5.2.4 Complex passwords must contain a Numeric Character (Not Scored)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that a number or numeric value is part of the password policy on the computer.

Rationale:

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

Audit:

Perform one of the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep Numeric
```

2. Verify the value returned has

RequiresNumeric
minimumNumericCharacters
Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep "1 number"
```

2. Verify the value returned has

Password must have at least 1 number

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

5.2.5 Complex passwords must contain a Special Character (Not Scored)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Ensure that a special character is part of the password policy on the computer

Rationale:

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep "1 special"
```

2. Verify the value returned

Password must have at least 1 special character

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

5.2.6 Complex passwords must uppercase and lowercase letters (Not Scored)

Profile Applicability:

- Level 2

Description:

Complex passwords contain one character from each of the following classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters.

Ensure that both uppercase and lowercase letters are part of the password policy on the computer

Rationale:

The more complex a password the more resistant it will be against persons seeking unauthorized access to a system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep com.apple.uppercaseAndLowercase
```

2. Verify the value returned

com.apple.uppercaseAndLowercase

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Password policy should be in effect to reduce the risk of exposed services being compromised easily through dictionary attacks or other social engineering attempts.

5.2.7 Password Age (Scored)

Profile Applicability:

- Level 1

Description:

Over time passwords can be captured by third parties through mistakes, phishing attacks, third party breaches or merely brute force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed) users should reset passwords periodically. This control uses 365 days as the acceptable value, some organizations may be more or less restrictive. This control mainly exists to mitigate against password reuse of the macOS account password in other realms that may be more prone to compromise. Attackers take advantage of exposed information to attack other accounts.

Rationale:

Passwords should be changed periodically to reduce exposure

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep policyAttributeExpiresEveryNDays
```

2. Verify the value returned

policyAttributeCurrentTime > policyAttributeLastPasswordChangeTime +
policyAttributeExpiresEveryNDays * 24 * 60 * 60
policyAttributeExpiresEveryNDays
Should contain `365` or less

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Required password changes will lead to some locked computers requiring admin assistance

5.2.8 Password History (Scored)

Profile Applicability:

- Level 1

Description:

Over time passwords can be captured by third parties through mistakes, phishing attacks, third party breaches or merely brute force attacks. To reduce the risk of exposure and to decrease the incentives of password reuse (passwords that are not forced to be changed periodically generally are not ever changed) users must reset passwords periodically. This control ensures that previous passwords are not reused immediately by keeping a history of previous passwords hashes. Ensure that password history checks are part of the password policy on the computer. This control checks whether a new password is different than the previous 15.

The latest NIST guidance based on exploit research referenced in this section details how one of the greatest risks is password exposure rather than password cracking. Passwords should be changed to a new unique value whenever a password might have been exposed to anyone other than the account holder. Attackers have maintained persistent control based on predictable password change patterns and substantially different patterns should be used in case of a leak.

Rationale:

Old passwords should not be reused

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
pwpolicy -getaccountpolicies | egrep "differ from past"
```

2. Verify the value returned

Password must differ from past 15 passwords

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls
Run the following command in Terminal:

```
pwpolicy -setaccountpolicies
```

Examples in pwpolicy man page

Impact:

Required password changes will lead to some locked computers requiring admin assistance

5.3 Reduce the sudo timeout period (Scored)

Profile Applicability:

- Level 1

Description:

The `sudo` command allows the user to run programs as the root user. Working as the root user allows the user an extremely high level of configurability within the system.

Rationale:

The `sudo` command stays logged in as the root user for five minutes before timing out and re-requesting a password. This five minute window should be eliminated since it leaves the system extremely vulnerable. This is especially true if an exploit were to gain access to the system, since they would be able to make changes as a root user.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo cat /etc/sudoers | grep timestamp
```

2. Verify the value returned is:

```
Defaults timestamp_timeout=0
```

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo visudo
```

2. In the "`# Override built-in defaults`" section, add the line:

```
Defaults timestamp_timeout=0
```

Impact:

Users with sudo rights will have to enter their password after every sudo command with no grace period allowed.

Notes:

sudoers file.

#

This file MUST be edited with the 'visudo' command as root.

Failure to use 'visudo' may result in syntax or file permission errors

that prevent sudo from running.

#

See the sudoers man page for the details on how to write a sudoers file.

#

Host alias specification

User alias specification

Cmnd alias specification

Defaults specification

Defaults env_reset

Defaults timestamp_timeout=0

Defaults env_keep += "BLOCKSIZE"

Defaults env_keep += "COLORFGBG COLORTERM"

Defaults env_keep += "__CF_USER_TEXT_ENCODING"

Defaults env_keep += "CHARSET LANG LANGUAGE LC_ALL LC_COLLATE LC_CTYPE"

Defaults env_keep += "LC_MESSAGES LC_MONETARY LC_NUMERIC LC_TIME"

Defaults env_keep += "LINES COLUMNS"

Defaults env_keep += "LSCOLORS"

```
Defaults env_keep += "SSH_AUTH_SOCK"

Defaults env_keep += "TZ"

Defaults env_keep += "DISPLAY XAUTHORIZATION XAUTHORITY"

Defaults env_keep += "EDITOR VISUAL"

Defaults env_keep += "HOME MAIL"

# Runas alias specification

# User privilege specification

root ALL=(ALL) ALL

%admin ALL=(ALL) ALL

# Uncomment to allow people in group wheel to run all commands

# %wheel ALL=(ALL) ALL

# Same thing without a password

# %wheel ALL=(ALL) NOPASSWD: ALL

# Samples

# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom

# %users localhost=/sbin/shutdown -h now
```

5.4 Use a separate timestamp for each user/tty combo (Scored)

Profile Applicability:

- Level 1

Description:

In combination with removing the sudo timeout grace period a further mitigation should be in place to reduce the possibility of a a background process using elevated rights when a user elevates to root in an explicit context or tty. With the included sudo 1.8 introduced in 10.12 the default value is to have tty tickets for each interface so that root access is limited to a specific terminal. The default configuration can be overwritten or not configured correctly on earlier versions of macOS.

Rationale:

Additional mitigation should be in place to reduce the risk of privilege escalation of background processes.

Audit:

Ensure that the default sudoers controls are in place with explicit tickets per tty

```
cat /etc/sudoers | egrep tty_tickets
```

There should be no results

Remediation:

Remove "Defaults !tty_tickets" from the /etc/sudoers file using visudo

Notes:

https://github.com/jorangreef/sudo-prompt/issues/33

https://derflounder.wordpress.com/2016/09/21/tty_tickets-option-now-on-by-default-for-macos-sierras-sudo-tool

http://rixstep.com/2/20050521,00.shtml

5.5 Automatically lock the login keychain for inactivity (Scored)

Profile Applicability:

- Level 2

Description:

The login keychain is a secure database store for passwords and certificates and is created for each user account on macOS. The system software itself uses keychains for secure storage. Anyone with physical access to an unlocked keychain where the screen is also unlocked can copy all passwords in that keychain. Application access to the login keychain does not keep it unlocked. If you set Apple Mail to check for email every 10 minutes using the keychain for credentials and the keychain to lock every 15 minutes if inactive it will still cause the keychain to lock. The approach recommended here is that the login keychain be set to periodically lock when inactive to reduce the risk of password exposure or unauthorized use of credentials by a third party. The time period that an organization uses will depend on how great the use is of keychain aware applications. Organizations that use Firefox and Thunderbird will have a much different tolerance than those organization using keychain aware applications extensively.

Rationale:

While logged in, the keychain does not prompt the user for passwords for various systems and/or programs. This can be exploited by unauthorized users to gain access to password protected programs and/or systems in the absence of the user. Timing out the keychain can reduce the exploitation window.

Audit:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
security show-keychain-info
```

2. Verify that a value is returned below 6 hours: `Keychain "<NULL>" timeout=21600s`

Remediation:

Perform the following to implement the prescribed state:

1. Open *Utilities*
2. Select *Keychain Access*
3. Select a keychain
4. Select *Edit*
5. Select *Change Settings for keychain <keychain_name>*
6. Authenticate, if requested.
7. Change the *Lock after # minutes of inactivity* setting for the Login Keychain to an approved value that should be longer than 6 hours or 3600 minutes or based on the access frequency of the security credentials included in the keychain for other keychains.

Impact:

If the timeout is set too low on heavily used items the user will be annoyed and may use workarounds.

5.6 Ensure login keychain is locked when the computer sleeps (Scored)

Profile Applicability:

- Level 2

Description:

The login keychain is a secure database store for passwords and certificates and is created for each user account on macOS. The system software itself uses keychains for secure storage. Anyone with physical access to an unlocked keychain where the screen is also unlocked can copy all passwords in that keychain. The approach recommended here is that the login keychain be set to lock when when the computer sleeps to reduce the risk of password exposure. Organizations that use Firefox and Thunderbird will have a much different tolerance than those organization using keychain aware applications extensively.

Rationale:

While logged in, the keychain does not prompt the user for passwords for various systems and/or programs. This can be exploited by unauthorized users to gain access to password protected programs and/or systems in the absence of the user.

Audit:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
security show-keychain-info
```

2. Verify that the value returned contains: `Keychain "<NULL>" lock-on-sleep`

Remediation:

Perform the following to implement the prescribed state:

1. Open *Utilities*
2. Select *Keychain Access*
3. Select a keychain
4. Select *Edit*
5. Select *Change Settings for keychain <keychain_name>*
6. Authenticate, if requested.
7. Select *Lock when sleeping* setting

Impact:

The user may experience multiple prompts to unlock the keychain when waking from sleep.

5.7 Enable OCSP and CRL certificate checking (Scored)

Profile Applicability:

- Level 2

Description:

Certificates should only be trusted if they have both a satisfactory trust chain and they have not been revoked. macOS check whether the certificate is still valid based on issued parameters within the certificate.

Rationale:

A rogue or compromised certificate should not be trusted

Audit:

Run the following commands

```
defaults read com.apple.security.revocation CRLStyle
```

```
defaults read com.apple.security.revocation OCSPStyle
```

This audit check may fail while running as root, which is recommended. On systems running 10.12 and above initial testing has shown that the even if the configurations are in place in the GUI the artifact is not found using root. Run the remediation steps as root to overcome the false positive.

Remediation:

Run the following commands to enforce the compliant state
To set the CRL settings:

```
defaults write com.apple.security.revocation CRLStyle -string
RequireIfPresent
```

To set the OCSP settings:

```
defaults write com.apple.security.revocation OCSPStyle -string
RequireIfPresent
```

Impact:

Network or connectivity issues could interfere with certificate checks for valid certificates

5.8 Do not enable the "root" account (Scored)

Profile Applicability:

- Level 1

Description:

The root account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. With some Linux distros the system administrator may commonly uses the root account to perform administrative functions.

Rationale:

Enabling and using the root account puts the system at risk since any successful exploit or mistake while the root account is in use could have unlimited access privileges within the system. Using the `sudo` command allows users to perform functions as a root user while limiting and password protecting the access privileges. By default the root account is not enabled on a macOS computer. An administrator can escalate privileges using the `sudo` command (use `-s` or `-i` to get a root shell).

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
dscl . -read /Users/root AuthenticationAuthority
```

2. Verify the value returned is:

```
No such key: AuthenticationAuthority
```

Remediation:

Open System Preferences, Uses & Groups. Click the lock icon to unlock it. In the Network Account Server section, click Join or Edit. Click Open Directory Utility. Click the lock icon to unlock it. Select the Edit menu > Disable Root User.

Impact:

Some legacy posix software might expect an available root account.

5.9 Disable automatic login (Scored)

Profile Applicability:

- Level 1

Description:

The automatic login feature saves a user's system access credentials and bypasses the login screen, instead the system automatically loads to the user's desktop screen.

Rationale:

Disabling automatic login decreases the likelihood of an unauthorized person gaining access to a system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.loginwindow | grep autoLoginUser
```

2. Verify that no value is returned

Remediation:

Perform the following to implement the prescribed state:
Run the following command in Terminal:

```
sudo defaults delete /Library/Preferences/com.apple.loginwindow autoLoginUser
```

Impact:

If Automatic login is not disabled an unauthorized user could login without supplying a user password or credential.

5.10 Require a password to wake the computer from sleep or screen saver (Scored)

Profile Applicability:

- Level 1

Description:

Sleep and screensaver modes are low power modes that reduces electrical consumption while the system is not in use.

Rationale:

Prompting for a password when waking from sleep or screensaver mode mitigates the threat of an unauthorized person gaining access to a system in the user's absence.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read com.apple.screensaver askForPassword
```

2. Verify the value returned is 1.

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal: The current user will need to log off and on for changes to take effect.

```
defaults write com.apple.screensaver askForPassword -int 1
```

2. The current user will need to log off and on for changes to take effect.

Impact:

Without a screenlock in place anyone with physical access to the computer would be logged in and able to use the active users session.

Notes:

This only protects the system when the screen saver is running.

5.11 Ensure system is set to hibernate (Scored)

Profile Applicability:

- Level 2

Description:

In order to use a computer with Full Disk Encryption (FDE) macOS must keep encryption keys in memory to allow the use of the disk that has been FileVault protected. The storage volume has been unlocked and acts as if it was not encrypted. When the system is not in use the volume is protected through encryption. When the system is sleeping and available to quickly resume the encryption keys remain in memory.

If an unauthorized party has possession of the computer and the computer is only slept there are known attack vectors that can be attempted against the RAM that has the encryption keys or the running operating system that is protected by a login screen. Network attacks if network interfaces are on as well as USB or other open device ports are possible. Most of these attacks require knowledge of unpatched vulnerabilities or a high level of sophistication if all the other controls function as intended.

There is little impact on hibernating the system rather than sleeping after an appropriate time period to remediate the risk of OS level attacks. Hibernation writes the keys to desk and requires FileVault to be unlocked prior to the OS being available. In the case of unauthorized personnel with access to the computer encryption would have to be broken prior to attacking the operating system in order to recover data from the system.

https://www.helpnetsecurity.com/2018/08/20/laptop-sleep-security/

Mac systems should be set to hibernate after sleeping for a risk acceptable time period. The default value for "standbydelay" is three hours (10800 seconds). This value is likely appropriate for most Desktops. If Mac desktops are deployed in unmonitored less physically secure areas with confidential data this value might be adjusted. The desktop or would have to retain power so that the running OS or physical RAM could be attacked however.

MacBooks should be set so that the standbydelay is 15 minutes (900 seconds) or less. This setting should allow laptop users in most cases to stay within physically secured areas while going to a conference room, auditorium or other internal location without having to unlock the encryption. When the user goes home at night the laptop will auto-hibernate after 15 minutes and require the FileVault password to unlock prior to logging back in to system when it resumes.

Rationale:

To mitigate the risk of data loss the system should power down and lock the encrypted drive after a specified time. Laptops should hibernate 15 minutes or less after sleeping.

Audit:

Perform the following to ensure laptops are configured as prescribed:

1. Run the following command in Terminal:

```
system_profiler SPHardwareDataType | egrep MacBook
```

2. If there are any results the system is in scope for a non-default hibernation value

```
pmset -g | egrep standbydelay
```

3. The results should be 900 or less

```
 standbydelay         900
```

Remediation:

Perform the following to configure laptops as prescribed:

1. Run the following command in Terminal:

```
sudo pmset -a standbydelay 900
```

Impact:

The laptop will take additional time to resume normal operation then if only sleeping rather than hibernating

Notes:

There are several good references to the concerns about ensuring hibernation rather than sleep is in place. A selection below:

http://mattwashchuk.com/articles/2016/01/08/maximizing-filevault-security

https://www.zdziarski.com/blog/?p=6705

https://www.howtogeek.com/260478/how-to-choose-when-your-mac-hibernates-or-enters-standby/

https://www.lifewire.com/change-mac-sleep-settings-2260804

5.12 Require an administrator password to access system-wide preferences (Scored)

Profile Applicability:

- Level 1

Description:

System Preferences controls system and user settings on a macOS Computer. System Preferences allows the user to tailor their experience on the computer as well as allowing the System Administrator to configure global security settings. Some of the settings should only be altered by the person responsible for the computer.

Rationale:

By requiring a password to unlock System-wide System Preferences the risk is mitigated of a user changing configurations that affect the entire system and requires an admin user to re-authenticate to make changes

Audit:

In System Preferences: Security, General tab under Advanced, verify "Require an administrator password to access system-wide preferences" is checked.
Alternatively, Use the following command:

```
security authorizationdb read system.preferences 2> /dev/null | grep -A1
shared | grep -E '(true|false)'
```

The response returned should be ""

Remediation:

In System Preferences: Security, General tab under Advanced, check "Require an administrator password to access system-wide preferences"

Impact:

If Automatic login is not disabled an unauthorized user could login without supplying a user password or credential.

5.13 Disable ability to login to another user's active and locked session (Scored)

Profile Applicability:

- Level 1

Description:

macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions.

Rationale:

Disabling the admins and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
/usr/bin/security authorizationdb read system.login.screensaver 2>/dev/null |
/usr/bin/grep -A 1 "<array>" | /usr/bin/awk -F "<|>" 'END{ print $3 }'
```

2. Returned value should be "use-login-window-ui" if the system is configured as recommended.

Remediation:

Edit the Authorization Database "authorizationdb" by replacing "authenticate-session-owner-or-admin" with "use-login-window-ui"
References
https://derflounder.wordpress.com/2014/02/16/managing-the-authorization-database-in-os-x-mavericks/
https://www.jamf.com/jamf-nation/discussions/18195/system-login-screensaver

Impact:

While Fast user switching is a workaround for some lab environments especially where there is even less of an expectation of privacy this setting change may impact some maintenance workflows

5.14 Create a custom message for the Login Screen (Scored)

Profile Applicability:

- Level 1

Description:

An access warning informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored.

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command to see the login window text:

```
defaults read /Library/Preferences/com.apple.loginwindow.plist
LoginwindowText
```

Remediation:

Perform the following to implement the prescribed state:

1. To add text with elevated privileges:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow
LoginwindowText "your text here"
```

2. To remove the text with elevated privileges:

```
sudo defaults delete /Library/Preferences/com.apple.loginwindow
LoginwindowText
```

Impact:

If users are not informed of their responsibilities there may be unapproved activity. Users that are not approved for access may take the lack of a warning banner as implied consent to access.

5.15 Create a Login window banner (Scored)

Profile Applicability:

- Level 2

Description:

A Login window banner warning informs the user that the system is reserved for authorized use only. It enforces an acknowledgment by the user that they have been informed of the use policy in the banner if required

Rationale:

An access warning may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command to see the login window text:

```
cat /Library/Security/PolicyBanner.txt
```

Remediation:

Place a file named `PolicyBanner.txt` in `/Library/Security/`

Impact:

Users will have to click on the window with the Login text before logging into the computer

5.16 Do not enter a password-related hint (Not Scored)

Profile Applicability:

- Level 1

Description:

Password hints help the user recall their passwords for various systems and/or accounts. In most cases, password hints are simple and closely related to the user's password.

Rationale:

Password hints that are closely related to the user's password are a security vulnerability, especially in the social media age. Unauthorized users are more likely to guess a user's password if there is a password hint. The password hint is very susceptible to social engineering attacks and information exposure on social media networks

Audit:

1. Open `System Preferences`
2. Select `Users & Groups`
3. Highlight the user
4. Select `Change Password`
5. Verify that no text is entered in the `Password hint` box

Remediation:

1. Open `System Preferences`
2. Select `Users & Groups`
3. Highlight the user
4. Select `Change Password`
5. Verify that no text is entered in the `Password hint` box

Notes:

Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

5.17 Disable Fast User Switching (Not Scored)

Profile Applicability:

- Level 2

Description:

Fast user switching allows a person to quickly log in to the computer with a different account. While only a minimal security risk, when a second user is logged in, that user might be able to see what processes the first user is using, or possibly gain other information about the first user. In a large directory environment where it is difficult to limit login access many valid users can login to other user's assigned computers.

Rationale:

Fast user switching allows multiple users to run applications simultaneously at console. There can be information disclosed about processes running under a different user. Without a specific configuration to save data and log out users can have unsaved data running in a background session that is not obvious.

Audit:

In System Preferences: Accounts, Login Options, make sure the "Enable fast user switching" checkbox is off.

Remediation:

In System Preferences: Accounts, Login Options, make sure the "Enable fast user switching" checkbox is off.

Impact:

Where support staff visit users computers consoles they will not be able to log in to their own session if there is an active and locked session.

Notes:

macOS is a multi-user operating system, and there are other similar methods that might provide the same kind of risk. The Remote Login service that can be turned on in the Sharing System Preferences pane is another.

5.18 Secure individual keychains and items (Not Scored)

Profile Applicability:

- Level 2

Description:

By default, the keychain for an account, especially a local account, have the same password as the account's logon password. It is possible to change the passwords on keychains to something different than the login password, and doing so would keep that keychain locked until needed after login. This is especially important when a smartcard is being used for console login. Keychains need to be protected by more than a pin in order to be secured and the default behavior with a smartcard will result in a pin for the login password. Individual keychain entries can have special ACLs to increase security as well.

Rationale:

Each keychain entry can have different access controls. It's possible to set the keychain item to require a keychain password every time an item is accessed, even if the keychain is unlocked. This level of security could be useful for bank passwords or other passwords that need extra security.

Audit:

1. Open `Utilities`
2. Select `Keychain Access`
3. Double-click keychain
4. Select `Access Control`
5. Verify if the box next to "Ask for Keychain Password" is checked

Remediation:

1. Open `Utilities`
2. Select `Keychain Access`
3. Double-click keychain
4. Select `Access Control`
5. Check box next to "Ask for Keychain Password"

Impact:

Having to enter the keychain password for each access could become inconvenient and/or tedious for users.

5.19 Create specialized keychains for different purposes (Not Scored)

Profile Applicability:

- Level 2

Description:

The keychain is a secure database store for passwords and certificates and is created for each user account on macOS. The system software itself uses keychains for secure storage. Users can create more than one keychain to protect various passwords separately.

Rationale:

If the user can logically split password and other entries into different keychains with different passwords, a compromise of one password will have limited effect.

Audit:

1. Open `Utilities`
2. Select `Keychain Access`
3. Verify there are multiple keychains listed under `Keychains` on the upper lefthand side of the window

Remediation:

1. Open `Utilities`
2. Select `Keychain Access`
3. Select `File`
4. Select `New Keychain`
5. Input name of new keychain next to `Save As`
6. Select `Create`
7. Drag and drop desired keychain items into new keychain from login keychain

Impact:

Using multiple keychains can be inconvenient. It is also not necessarily possible for all kinds of data, such as Safari auto-fill information, to be stored in secondary keychains. Not all keychain-aware applications may provide an interface to choose secondary keychains.

Notes:

One useful separation of keychains might be in a business environment. Personal information might be stored in one keychain and business information in a different keychain.

5.20 System Integrity Protection status (Scored)

Profile Applicability:

- Level 1

Description:

System Integrity Protection is a security feature introduced in OS X 10.11 El Capitan. System Integrity Protection restricts access to System domain locations and restricts runtime attachment to system processes. Any attempt to attempt to inspect or attach to a system process will fail. Kernel Extensions are now restricted to /Library/Extensions and are required to be signed with a Developer ID.

Rationale:

Running without System Integrity Protection on a production system runs the risk of the modification of system binaries or code injection of system processes that would otherwise be protected by SIP.

Audit:

Perform the following to determine the System Integrity Protection status.

1. Run the following command in Terminal:

```
/usr/bin/csrutil status
```

2. The output should be:

```
System Integrity Protection status: enabled.
```

Remediation:

Perform the following while booted in macOS Recovery Partition.

1. Select Terminal from the Utilities menu
2. Run the following command in Terminal:

```
/usr/bin/csrutil enable
```

3. The output should be:

```
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
```

4. Reboot.

If a change is to the status is attempted from the booted Operating System rather than the recovery partition an error will be generated.
csrutil: failed to modify system integrity configuration. This tool needs to be executed from the Recovery OS.

Impact:

System binaries and processes could become compromised

6 User Accounts and Environment

Account management is a central part of security for any computer system including macOS. General practices should be followed to ensure that all accounts on a system are still needed and that default accounts have been removed. Users with admin roles should have distinct accounts for Admin functions as well as day to day work where the passwords are different and known only by the user assigned to the account. Accounts with Elevated privileges should not be easily discerned from the account name from standard accounts.

When any computer system is added to a Directory System there are additional controls available including user account management that are not available in a standalone computer. One of the drawbacks is the local computer is no longer in control of the accounts that can access or manage it if given permission. For macOS if the computer is connected to a Directory any standard user can now login to the computer at console which by default may be desirable or not depending on the use case. If an admin group is allowed to administer the local computer the membership of that group is controlled completely in the Directory.

macOS computers connected to a Directory should be configured so that the risk is appropriate for the mission use of the computer. Only those accounts that require local authentication should be allowed, only required administrator accounts should be in the local administrator group. Authenticated Users for console access and Domain Admins for Administration may be too broad or too limited

6.1 Accounts Preferences Action Items

Proper account management is critical to computer security. Many options and settings in the Account System Preference Pane can be used to increase the security of the Mac.

6.1.1 Display login window as name and password (Scored)

Profile Applicability:

- Level 1

Description:

The login window prompts a user for his/her credentials, verifies their authorization level and then allows or denies the user access to the system.

Rationale:

Prompting the user to enter both their username and password makes it twice as hard for unauthorized users to gain access to the system since they must discover two attributes.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.loginwindow SHOWFULLNAME
```

2. Make sure the value returned is `1`.

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Users and Groups*
3. Select *Login Options*
4. Select *Name and Password*

Alternatively:
Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow SHOWFULLNAME -
bool yes
```

6.1.2 Disable "Show password hints" (Scored)

Profile Applicability:

- Level 1

Description:

Password hints are user created text displayed when an incorrect password is used for an account.

Rationale:

Password hints make it easier for unauthorized persons to gain access to systems by providing information to anyone that the user provided to assist remembering the password. This info could include the password itself or other information that might be readily discerned with basic knowledge of the end user.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.loginwindow RetriesUntilHint
```

2. Make sure the value returned is `0`
3. If the "The domain/default pair... does not exist" the computer is compliant

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Users & Groups*
3. Select *Login Options*
4. Uncheck *Show password hints*

Alternatively:
Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow
RetriesUntilHint -int 0
```

Impact:

The user can set the hint to any value including the password itself or clues that allow trivial social engineering attacks.

6.1.3 Disable guest account login (Scored)

Profile Applicability:

- Level 1

Description:

The guest account allows users access to the system without having to create an account or password. Guest users are unable to make setting changes, cannot remotely login to the system and all created files, caches, and passwords are deleted upon logging out.

Rationale:

Disabling the guest account mitigates the risk of an untrusted user doing basic reconnaissance and possibly using privilege escalation attacks to take control of the system.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
sudo defaults read /Library/Preferences/com.apple.loginwindow.plist
GuestEnabled
```

2. Make sure the value returned is 0.

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Users & Groups*
3. Select *Guest User*
4. Uncheck *Allow guests to log in to this computer*

Alternatively:
Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow GuestEnabled -
bool NO
```

Impact:

A guest user can use that access to find out additional information about the system and might be able to use privilege escalation vulnerabilities to establish greater access.

Notes:

By default, the guest account is enabled for access to sharing services, but is not allowed to log in to the computer.

The guest account does not need a password when it is enabled to log in to the computer.

6.1.4 Disable "Allow guests to connect to shared folders" (Scored)

Profile Applicability:

- Level 1

Description:

Allowing guests to connect to shared folders enables users to access selected shared folders and their contents from different computers on a network.

Rationale:

Not allowing guests to connect to shared folders mitigates the risk of an untrusted user doing basic reconnaissance and possibly use privilege escalation attacks to take control of the system.

Audit:

Perform the following to ensure the system is configured as prescribed:
For AFP sharing:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.AppleFileServer | grep -i guest
```

2. Make sure the value returned contains `guestAccess = 0;`
3. If the "The domain/default pair... does not exist" the computer is compliant

For SMB sharing:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/SystemConfiguration/com.apple.smb.server |
grep -i guest
```

2. Make sure the value returned contains `AllowGuestAccess = 0;`
3. If the "The domain/default pair... does not exist" the computer is compliant

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Users & Groups*
3. Select *Guest User*
4. Uncheck *Allow guests to connect to shared folders*

Alternatively:
For AFP sharing:
Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/com.apple.AppleFileServer
guestAccess -bool no
```

For SMB sharing:
Run the following command in Terminal:

```
sudo defaults write
/Library/Preferences/SystemConfiguration/com.apple.smb.server
AllowGuestAccess -bool no
```

Impact:

Unauthorized users could access shared files on the system.

6.1.5 Remove Guest home folder (Scored)

Profile Applicability:

- Level 1

Description:

In the previous two controls the guest account login has been disabled and sharing to guests has been disabled as well. There is no need for the legacy Guest home folder to remain in the file system. When normal user accounts are removed you have the option to archive it, leave it in place or delete. In the case of the guest folder the folder remains in place without a GUI option to remove it. If at some point in the future a Guest account is needed it will be re-created. The presence of the Guest home folder can cause automated audits to fail when looking for compliant settings within all User folders as well. Rather than ignoring the folders continued existence it is best removed.

Rationale:

The Guest home folders are unneeded after the Guest account is disabled and could be used inappropriately.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
ls /Users/ | grep Guest
```

2. Make sure there is no ouput

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
rm -R /Users/Guest
```

2. Make sure there is no ouput

Impact:

The Guest account should not be necessary after it is disabled and it will be automatically re-created if the Guest account is re-eanbled

6.2 Turn on filename extensions (Scored)

Profile Applicability:

- Level 1

Description:

A filename extension is a suffix added to a base filename that indicates the base filename's file format.

Rationale:

Visible filename extensions allows the user to identify the file type and the application it is associated with which leads to quick identification of misrepresented malicious files.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read NSGlobalDomain AppleShowAllExtensions
```

2. The output should be `1`

Be aware that this is a user level configuration item and it should be configured correctly for every user of the computer. The control check in CIS-CAT will check for the correct configuration for every active user.

Remediation:

Perform the following to implement the prescribed state:

1. Select *Finder*
2. Select *Preferences*
3. Check *Show all filename extensions*

Alternatively, use the following command:

```
defaults write NSGlobalDomain AppleShowAllExtensions -bool true
```

Impact:

The user of the system can open files of unknown or unexpected filetypes if the extension is not visible.

6.3 Disable the automatic run of safe files in Safari (Scored)

Profile Applicability:

- Level 1

Description:

Safari will automatically run or execute what it considers safe files. This can include installers and other files that execute on the operating system. Safari bases file safety by using a list of filetypes maintained by Apple. The list of files include text, image, video and archive formats that would be run in the context of the OS rather than the browser.

Rationale:

Hackers have taken advantage of this setting via drive-by attacks. These attacks occur when a user visits a legitimate website that has been corrupted. The user unknowingly downloads a malicious file either by closing an infected pop-up or hovering over a malicious banner. An attacker can create a malicious file that will fall within Safari's safe file list that will download and execute without user input.

Audit:

Perform the following to ensure the system is configured as prescribed:

1. Run the following command in Terminal:

```
defaults read com.apple.Safari AutoOpenSafeDownloads
```

2. The result should be `0`

Remediation:

Perform the following to implement the prescribed state:

1. Open *Safari*
2. Select *Safari* from the menu bar
3. Select *Preferences*
4. Select *General*
5. Uncheck *Open "safe" files after downloading*

Alternatively run the following command in Terminal:

```
defaults write com.apple.Safari AutoOpenSafeDownloads -boolean no
```

Impact:

Apple considers many files that the operating system itself auto-executes as "safe files." Many of these files could be malicious and could execute locally without the user even knowing that a file of a specific type had been download.

6.4 Safari disable Internet Plugins for global use (Not Scored)

Profile Applicability:

- Level 2

Description:

Starting with Safari 10 and continuing with 11 Apple changed the model on how the built-in web browser handles Internet Plug-Ins. Instead of using a global approach where the Plug-in is either on or off for all sites the default decision is about allowing, not allowing, or allowing permanently for a specific site that is visited. Other browsers are moving to stop using Plug-ins altogether and insist on the use of HTML 5 for rich content. Only allowing Plug-in content from specific sites is a viable security option. In the Security Preferences, Plug-in settings it is possible to override the security feature and enable Plug-in content globally by Plug-in. With the controls planned in other macOS browsers allowing content globally is likely to put Safari users more at risk than other browser users.

There are three options for Internet Plug-ins with Safari 10 "When visiting other websites" Ask, Off or On. The on setting should not be used.

https://support.apple.com/en-us/HT202819

Rationale:

Allow Internet Plugins only on required sites

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
defaults read ~/Library/Preferences/com.apple.safari.plist | grep -i
"PlugInFirstVisitPolicy = *"
```

Results should not be:

```
PlugInFirstVisitPolicy = PlugInPolicyAllowWithSecurityRestrictions;
```

Remediation:

Select either ask to use or block

Impact:

Users will have to approve Internet Plugin use by site.

6.5 Use parental controls for systems that are not centrally managed (Not Scored)

Profile Applicability:

- Level 2

Description:

Many aspects and features of macOS can be restricted on a user-by-user basis via the Parental Controls feature. This includes computer usage time limits, application accessibility limitations, and website restrictions. Although this feature is called Parental Controls, these restrictions may be appropriate for corporate, government, or educational use.

Rationale:

Limiting usage and restricting features for managed users reduces the risk of the user and/or system being exposed to malicious and/or inappropriate content.

Audit:

1. Open `System Preferences`
2. Select `Users & Groups`
3. Highlight managed user
4. Verify that the box next to `Enable parental controls` is checked
5. Select `Open Parental Controls`
6. Verify restricted items are selected within `Parental Controls` feature

Remediation:

1. Open `System Preferences`
2. Select `Users & Groups`
3. Highlight managed user
4. Check box next to `Enable parental controls`
5. Select `Open Parental Controls`
6. Select items within the `Parental Controls`feature that should be restricted.

Impact:

The extensive use of parental controls adds to the configuration management burden and can limit legitimate user activity.

7 Appendix: Additional Considerations

This section is for guidance on topics for which the Benchmark does not include a prescribed state, and for security controls that were previously represented in macOS security guides.

7.1 Wireless technology on macOS (Not Scored)

Profile Applicability:

- Level 2

Description:

Some organizations have comprehensive rules that cover the use of wireless technologies in order to implement operational security. There are specific policies governing the use of both Bluetooth and Wi-Fi (802.11) that often include disabling the wireless capability in either software or hardware or both.

Wireless access is part of the feature set required for mobile computers and is considered essential for most users. The general use case for macOS is to use wireless connectivity, Apple provides a wireless network card and Bluetooth capability in almost every product they make. Bluetooth keyboards are now the default selection where a keyboard is not already integrated into the device.

There are instructions on how to remove parts of the operating system in order to remediate wireless connectivity but they are not recommended within the scope of this Benchmark.

https://apple.stackexchange.com/questions/99686/how-to-easily-and-completely-disable-enable-wlan-so-it-cannot-be-turned-on-agai

https://apple.stackexchange.com/questions/123326/disable-bluetooth-permanently

macOS computers will not allow this if System Integrity Protection is enabled.

7.2 iSight Camera Privacy and Confidentiality Concerns (Not Scored)

Profile Applicability:

- Level 2

Description:

If the computer is present in an area where there are privacy concerns or sensitive images or actions are taking place the camera should be covered at those times. A permanent cover or alteration may be required when the computer is always located in a confidential area.

Malware is continuously discovered that circumvents the privacy controls of the built-in camera. No computer has perfect security and it seems likely that even if all the drivers are disabled or removed that working drivers can be re-introduced by a determined attacker.

At this point video chatting and other uses of the built-in camera are standard uses for a computer. It is contrary to a standard use case to permanently remove the camera. In cases where the camera is not allowed to be used at all or when the computer is located in private areas additional precautions are warranted. The General rule should be that if the camera can capture images that could cause embarrassment or an adverse impact the camera should be covered until it is appropriate to use.

7.3 Computer Name Considerations (Not Scored)

Profile Applicability:

- Level 2

Description:

If the computer is used in an organization that assigns host names, it is a good idea to change the computer name to the host name. This is more of a best practice than a security measure. If the host name and the computer name are the same, computer support may be able to track problems down more easily.

With mobile devices using DHCP IP tracking has serious drawbacks, hostname or computer name tracking makes much more sense for those organizations that can implement it. If the computer is using different names for the "Computer Name" DNS and Directory environments it can be difficult to manage Macs in an Enterprise asset inventory.

7.4 Software Inventory Considerations (Not Scored)

Profile Applicability:

- Level 2

Description:

With the introduction of Mac OS X 10.6.6, Apple added a new application, App Store, which resides in the Applications directory. This application allows a user with admin privileges and an Apple ID to browse Apple's online App Store, purchase (including no cost purchases), and install new applications, bypassing Enterprise software inventory controls. Any admin user can install software in the /Applications directory whether from internet downloads, thumb drives, optical media, cloud storage or even binaries through email. Even standard users can run executables if permitted. The source of the software is not nearly as important as a consistent audit of all installed software for patch compliance and appropriateness.

A single user desktop where the user, administrator and the person approving software are all the same person probably does not need to audit software inventory to this extent. It is helpful in the case of stability problems or malware however.

Scan systems on a monthly basis and determine the number of unauthorized pieces of software that are installed. Verify that if an unauthorized piece of software is found one month, it is removed from the system the next.

Export Apple System Profiler information through the built-in or other third party tools on an organizationally defined timetable.

Notes:

https://www.sans.org/critical-security-controls/control.php?id=2

7.5 Firewall Consideration (Not Scored)

Profile Applicability:

- Level 2

Description:

In addition to the Application Layer Firewall (`alf`) mentioned in the benchmark, macOS also ships with packet filter, or `pf`. Leveraging `pf` is beyond the scope of this Benchmark. For more information, please see:

- https://support.apple.com/kb/ht5519
- http://blog.scottlowe.org/2013/05/15/using-pf-on-os-x-mountain-lion/

7.6 Automatic Actions for Optical Media (Not Scored)

Profile Applicability:

- Level 1

Description:

Managing automatic actions, while useful in very few situations, is unlikely to increase security on the computer and does complicate the users experience and add additional complexity to the configuration. These settings are user controlled and can be changed without Administrator privileges unless controlled through MCX settings or Parental Controls. Unlike Windows Auto-run the optical media is accessed through Operating System applications, those same applications can open and access the media directly. If optical media is not allowed in the environment the optical media drive should be disabled in hardware and software

7.7 App Store Automatically download apps purchased on other Macs Considerations (Not Scored)

Profile Applicability:

- Level 2

Description:

With 10.9 Apple expanded the capability of the App Store to automatically download macOS applications that were purchased in the App Store on another Mac. This feature can be very desirable for personal Macs or in a small business setting so that all purchased software through Apple's App Store is provisioned on all macOS Computers, just like iOS. This feature may not be desirable in Enterprise environments where the expectations of handling software licenses, tracking software inventory and personal software are different.

Please evaluate your organizations expectations about the use of personal software and software license tracking to align with this setting.

For those organizations that are using Enterprise Apple IDs for their employees the reverse is true. If the user has the username and password for their Apple ID and software is being purchased on that account the user could download the software on other computers they have access to.

7.8 Extensible Firmware Interface (EFI) password (Not Scored)

Profile Applicability:

- Level 2

Description:

EFI is the software link between the motherboard hardware and the software operating system. EFI determines which partition or disk to load macOS from, it also determines whether the user can enter single-user mode. The main reasons to set a firmware password have been protections against an alternative boot disk, protection against a passwordless root shell through single user mode and protection against firewire DMA attacks. In the past it was not difficult to reset the firmware password by removing RAM but it did make tampering slightly harder and having to remove RAM remediated memory scraping attacks through DMA. It has always been difficult to Manage the firmware password on macOS computers, though some tools did make it much easier.

Apple patched OS X in 10.7 to mitigate the DMA attacks and the use of FileVault 2 Full-Disk Encryption mitigates the risk of damage to the boot volume if an unauthorized user uses a different boot volume or uses Single User Mode. Apple's reliance on the recovery partition and the additional features it provides make controls that do not allow the user to boot into the recovery partition less attractive.

Starting in Late 2010 with the MacBook Air Apple has slowly updated the requirements to recover from a lost firmware password. Apple only supports taking the computer to an Apple authorized service provider. This change makes managing the firmware password effectively more critical if it is used.

Setting the firmware password may be good practice in some environments. We cannot recommend it as a standard security practice at this time.

http://support.apple.com/kb/ts3554

https://jamfnation.jamfsoftware.com/article.html?id=58

http://derflounder.wordpress.com/2012/02/05/protecting-yourself-against-firewire-dma-attacks-on-10-7-x/

http://derflounder.wordpress.com/2013/04/26/booting-into-single-user-mode-on-a-filevault-2-encrypted-mac/

7.9 FileVault and Local Account Password Reset using AppleID (Not Scored)

Profile Applicability:

- Level 2

Description:

Apple has provided services for several years that allowed a user to reset a local account password on a computer using their Apple ID and a service to store the FileVault Master Password with Apple that would be controlled by access to an Apple ID. These distinct services have been more cleanly integrated starting in 10.12.

This integrated service for password and decryption is a concern in Enterprise environments. Normal Enterprise management controls mitigate the risk of external control of organizational systems. The user of the system already has the ability to unlock the disk in order to login and use it and some form of password recovery function is likely already in place for any approved accounts. In addition:

- You cannot reset anything but a local account
- You need physical access to the computer on a network that can phone home to Apple
- Enterprise FileVault management precludes the use of Apple's personal encryption recovery tied to a User's Apple ID
- The current login keychain will have to be discarded unless the user remembers the old password

This service allows for organizational computer users to utilize AppleIDs for encryption key escrow and user account management. The use of Apple's services rather than Enterprise services may be considered inappropriate.

https://support.apple.com/en-us/HT204837

7.10 Repairing permissions is no longer needed (Not Scored)

Profile Applicability:

- Level 1

Description:

With the introduction of System Integrity Protection (SIP) Apple has removed the necessity of repairing permissions. In earlier versions of the Operating System repair permissions checked the receipt files of installed software and ensured that the existing permissions in the file system matched what the receipts said it should. System integrity protection manages and blocks permission to certain directories continuously.

http://www.macissues.com/2015/10/02/about-os-x-10-11-el-capitan-and-permissions-fixes/

https://en.wikipedia.org/wiki/System_Integrity_Protection

http://www.infoworld.com/article/2988096/mac-os-x/sorry-unix-fans-os-x-el-capitan-kills-root.html

7.11 App Store Password Settings (Not Scored)

Profile Applicability:

- Level 2

Description:

With OS X 10.11 Apple added settings for password storage for the App Store in macOS. These settings parallel the settings in iOS. As with iOS the choices are a requirement to provide a password after every purchase or to have a 15 minute grace period, and whether to require a password for free purchases. The response to this setting is stored in a cookie and processed by iCloud.

There is plenty of risk information on the wisdom of this setting for parents with children buying games on iPhones and iPads. the most relevant information here is the likelihood that users that are not authorized to download software may have physical access to an unlocked computer where someone who is authorized recently made a purchase. If that is a concern a password should be required at all times for App Store access in the Password Settings controls

7.12 Siri on macOS (Not Scored)

Profile Applicability:

- Level 1

Description:

With macOS 10.12 Sierra Apple has introduced Siri from iOS to macOS. While there are data spillage concerns with use of software data gathering personal assistants the risk here does not seem greater in sending queries to Apple through Siri than in sending search terms in a browser to Google or Microsoft. While it is possible that Siri will be used for local actions rather than Internet searches which could, in theory, tell Apple about confidential Programs and Projects that should not be revealed this appears be an edge use case.

In cases where sensitive and protected data is processed and Siri could help a user navigate their machine and expose that information it should be disabled. Siri does need to phone home to Apple so it should not be available from air-gapped networks as part of it's requirements.

Most of the use case data published has shown that Siri is a tremendous time saver on iOS where multiple screens and menus need to be navigated through. Information like sports scores, weather, movie times and simple to-do items on existing calendars can be easily found with Siri. None of the standard use cases should be more risky than already approved activity. Where "normal" user activity is already limited Siri use should be controlled as well.

7.13 Apple Watch features with macOS (Not Scored)

Profile Applicability:

- Level 1

Description:

With the release of macOS 10.12 Apple introduced a feature where the owner of an Apple Watch can lock and unlock their screen simply by being within range of a 10.12 computer when both devices are using the same AppleID with iCloud active. The benefit of not leaving the computer unlocked while the user is out of sight and readying the computer to resume work when the user returns without having to type in a password or insert a smartcard does seem attractive to people who have the Apple Watch. It is a continuation of other features like hand-off and continuity for the multiple Apple products users who have grown to expect their devices to work together.

For the screen unlock capability in particular it may not be attractive to organizations that are managing Apple devices and credentials. The capability allows a user to unlock their computer tied to an Enterprise account with a personal token that is not managed or controlled by the Enterprise. If the user loses their watch revoking the credential that can unlock the screen might be problematic.

Unless Enterprise control of the watch as a token tied to a user identity can be achieved Apple Watches should not be used for screen unlocks. The risk of an auto-lock based on the user being out of proximity may still be acceptable if possible to do lock only.

This functionality does require the computer to be logged in to iCloud. If iCloud is disabled the Apple watch lock and unlock will not be possible.

A profile may be used to control unlock functionality.

7.14 Apple File System (APFS) (Not Scored)

Profile Applicability:

- Level 1

Description:

With the release of macOS 10.12 Apple has included a developer preview of a new file system called APFS. Many features desired in a modern file system are ready for use and some will be available when the release version is available in 2017. At this time the file system cannot be used for boot volumes or with FileVault. Filesystem formatting and manipulation is only available in the command line and not the GUI and there are some reported gaps with the encryption capabilities. Until the filesystem supports boot volumes, FileVault, OS integrated encryption and key management as well as GUI management it should not be used with production systems.

APFS is part of macOS 10.13 and is expected to be used there. It is still recommended not to use on 10.12 systems.

For more information on APFS

https://developer.apple.com/library/prerelease/content/documentation/FileManagement/Conceptual/APFS_Guide/Introduction/Introduction.html#//apple_ref/doc/uid/TP40016999-CH1-DontLinkElementID_18

http://arstechnica.com/apple/2016/09/macos-10-12-sierra-the-ars-technica-review/8/

Rationale:

APFS in macOS 10.12 has limitations that were resolved in macOS 10.13. The unfinished feature set argue agains the use of APFS in production systems that are not running 10.13 or higher.

Audit:

Perform the following to ensure the system is configured as prescribed:
Run the following command in Terminal:

```
diskutil list | grep -i apfs
```

Remediation:

Ensure that if found the use of a the filesystem is not in contradiction of organizational policies. If required ensure information is backed up and reformat the drive to Journaled HFS+.

7.15 System information backup to remote computers (Not Scored)

Profile Applicability:

- Level 2

Description:

It is best practice to ensure that local computers are not a single point of failure for logging and auditing records about activity on the computer itself. Whether end user activity or system process information a mechanism should be in place to transfer the logs to another system that is hardened to receive them. A hardened log host reduces the risk of failure or compromise, particularly with user end points. From an enterprise management standpoint those records should be reviewed to ensure that there is not a common exploitable vulnerability, system bug or even hardware issue that can effect other devices in the environment.

With changes in Apple's logging methods in the last few years third party tools appear to be preferred to ensure logs and records are obtained appropriately. Aggressive retention likely requires more space than available on built-in SSDs even if offline Time Machine backups are large and pristine.

Please ensure that solutions to capture and retain log and audit records are in place.

7.16 Unified logging (Not Scored)

Profile Applicability:

- Level 1

Description:

Starting with macOS 10.12 Apple introduced unified logging. This capability replaces the previous logging methodology with centralized system wide common controls. A full explanation of macOS logging behavior is beyond the scope of this Benchmark. These changes impact previous logging controls from macOS Benchmarks. At this point many of the syslog controls have been or are being removed since the old logging methods have been deprecated. Controls that still appear useful will be retained. Some legacy controls have been removed for this release.

More info

https://developer.apple.com/documentation/os/logging

https://eclecticlight.co/2018/03/19/macos-unified-log-1-why-what-and-how/

7.17 AirDrop security considerations (Not Scored)

Profile Applicability:

- Level 1

Description:

AirDrop is Apple's built-in on demand ad hoc file exchange system that is compatible with both macOS and iOS. It uses Bluetooth LE for discovery that limits connectivity to macOS or iOS users that are in close proximity. Depending on the setting it allows everyone or only Contacts to share files when they are nearby to each other.

In many ways this technology is far superior to the alternatives. The file transfer is done over a TLS encrypted session, does not require any open ports that are required for file sharing, does not leave file copies on email servers or within cloud storage, and allows for the service to be mitigated so that only people already trusted and added to contacts can interact with you.

Even with all of these positives some environments may wish to disable AirDrop. Organizations where Bluetooth and Wireless are not used will disable AirDrop by blocking it's necessary interfaces. Organizations that have disabled USB and other pluggable storage mechanisms and have blocked all unmanaged cloud and transfer solutions for DLP may want to disable AirDrop as well.

AirDrop should be used with Contacts only to limit attacks.

More info:

https://www.imore.com/how-apple-keeps-your-airdrop-files-private-and-secure

https://en.wikipedia.org/wiki/AirDrop

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Install Updates, Patches and Additional Security Software**		
1.1	Verify all Apple provided software is current (Scored)	☐	☐
1.2	Enable Auto Update (Scored)	☐	☐
1.3	Enable app update installs (Scored)	☐	☐
1.4	Enable system data files and security update installs (Scored)	☐	☐
1.5	Enable macOS update installs (Scored)	☐	☐
2	**System Preferences**		
2.1	**Bluetooth**		
2.1.1	Turn off Bluetooth, if no paired devices exist (Scored)	☐	☐
2.1.2	Turn off Bluetooth "Discoverable" mode when not pairing devices (Scored)	☐	☐
2.1.3	Show Bluetooth status in menu bar (Scored)	☐	☐
2.2	**Date & Time**		
2.2.1	Enable "Set time and date automatically" (Scored)	☐	☐
2.2.2	Ensure time set is within appropriate limits (Scored)	☐	☐
2.3	**Desktop & Screen Saver**		
2.3.1	Set an inactivity interval of 20 minutes or less for the screen saver (Scored)	☐	☐
2.3.2	Secure screen saver corners (Scored)	☐	☐
2.3.3	Set a screen corner to Start Screen Saver (Scored)	☐	☐
2.4	**Sharing**		
2.4.1	Disable Remote Apple Events (Scored)	☐	☐
2.4.2	Disable Internet Sharing (Scored)	☐	☐
2.4.3	Disable Screen Sharing (Scored)	☐	☐
2.4.4	Disable Printer Sharing (Scored)	☐	☐
2.4.5	Disable Remote Login (Scored)	☐	☐
2.4.6	Disable DVD or CD Sharing (Scored)	☐	☐
2.4.7	Disable Bluetooth Sharing (Scored)	☐	☐
2.4.8	Disable File Sharing (Scored)	☐	☐
2.4.9	Disable Remote Management (Scored)	☐	☐
2.5	**Energy Saver**		
2.5.1	Disable "Wake for network access" (Scored)	☐	☐
2.6	**Security & Privacy**		
2.6.1	**Encryption**		
2.6.1.1	Enable FileVault (Scored)	☐	☐

2.6.1.2	Ensure all user storage CoreStorage volumes are encrypted (Not Scored)	☐	☐
2.6.2	Enable Gatekeeper (Scored)	☐	☐
2.6.3	Enable Firewall (Scored)	☐	☐
2.6.4	Enable Firewall Stealth Mode (Scored)	☐	☐
2.6.5	Review Application Firewall Rules (Scored)	☐	☐
2.6.6	Enable Location Services (Not Scored)	☐	☐
2.6.7	Monitor Location Services Access (Not Scored)	☐	☐
2.6.8	Disable sending diagnostic and usage data to Apple (Scored)	☐	☐
2.7	**iCloud**		
2.7.1	iCloud configuration (Not Scored)	☐	☐
2.7.2	iCloud keychain (Not Scored)	☐	☐
2.7.3	iCloud Drive (Not Scored)	☐	☐
2.7.4	iCloud Drive Document sync (Scored)	☐	☐
2.7.5	iCloud Drive Desktop sync (Scored)	☐	☐
2.8	**Time Machine**		
2.8.1	Time Machine Auto-Backup (Scored)	☐	☐
2.8.2	Time Machine Volumes Are Encrypted (Scored)	☐	☐
2.9	Pair the remote control infrared receiver if enabled (Scored)	☐	☐
2.10	Enable Secure Keyboard Entry in terminal.app (Scored)	☐	☐
2.11	Java 6 is not the default Java runtime (Scored)	☐	☐
2.12	Securely delete files as needed (Not Scored)	☐	☐
3	**Logging and Auditing**		
3.1	Enable security auditing (Scored)	☐	☐
3.2	Configure Security Auditing Flags (Scored)	☐	☐
3.3	Ensure security auditing retention (Scored)	☐	☐
3.4	Control access to audit records (Scored)	☐	☐
3.5	Retain install.log for 365 or more days (Scored)	☐	☐
3.6	Ensure Firewall is configured to log (Scored)	☐	☐
4	**Network Configurations**		
4.1	Disable Bonjour advertising service (Scored)	☐	☐
4.2	Enable "Show Wi-Fi status in menu bar" (Scored)	☐	☐
4.3	Create network specific locations (Not Scored)	☐	☐
4.4	Ensure http server is not running (Scored)	☐	☐
4.5	Ensure FTP server is not running (Scored)	☐	☐
4.6	Ensure nfs server is not running (Scored)	☐	☐
5	**System Access, Authentication and Authorization**		
5.1	**File System Permissions and Access Controls**		
5.1.1	Secure Home Folders (Scored)	☐	☐
5.1.2	Check System Wide Applications for appropriate permissions (Scored)	☐	☐
5.1.3	Check System folder for world writable files (Scored)	☐	☐
5.1.4	Check Library folder for world writable files (Scored)	☐	☐

5.2	**Password Management**		
5.2.1	Configure account lockout threshold (Scored)	☐	☐
5.2.2	Set a minimum password length (Scored)	☐	☐
5.2.3	Complex passwords must contain an Alphabetic Character (Not Scored)	☐	☐
5.2.4	Complex passwords must contain a Numeric Character (Not Scored)	☐	☐
5.2.5	Complex passwords must contain a Special Character (Not Scored)	☐	☐
5.2.6	Complex passwords must uppercase and lowercase letters (Not Scored)	☐	☐
5.2.7	Password Age (Scored)	☐	☐
5.2.8	Password History (Scored)	☐	☐
5.3	Reduce the sudo timeout period (Scored)	☐	☐
5.4	Use a separate timestamp for each user/tty combo (Scored)	☐	☐
5.5	Automatically lock the login keychain for inactivity (Scored)	☐	☐
5.6	Ensure login keychain is locked when the computer sleeps (Scored)	☐	☐
5.7	Enable OCSP and CRL certificate checking (Scored)	☐	☐
5.8	Do not enable the "root" account (Scored)	☐	☐
5.9	Disable automatic login (Scored)	☐	☐
5.10	Require a password to wake the computer from sleep or screen saver (Scored)	☐	☐
5.11	Ensure system is set to hibernate (Scored)	☐	☐
5.12	Require an administrator password to access system-wide preferences (Scored)	☐	☐
5.13	Disable ability to login to another user's active and locked session (Scored)	☐	☐
5.14	Create a custom message for the Login Screen (Scored)	☐	☐
5.15	Create a Login window banner (Scored)	☐	☐
5.16	Do not enter a password-related hint (Not Scored)	☐	☐
5.17	Disable Fast User Switching (Not Scored)	☐	☐
5.18	Secure individual keychains and items (Not Scored)	☐	☐
5.19	Create specialized keychains for different purposes (Not Scored)	☐	☐
5.20	System Integrity Protection status (Scored)	☐	☐
6	**User Accounts and Environment**		
6.1	**Accounts Preferences Action Items**		
6.1.1	Display login window as name and password (Scored)	☐	☐
6.1.2	Disable "Show password hints" (Scored)	☐	☐
6.1.3	Disable guest account login (Scored)	☐	☐
6.1.4	Disable "Allow guests to connect to shared folders" (Scored)	☐	☐
6.1.5	Remove Guest home folder (Scored)	☐	☐

6.2	Turn on filename extensions (Scored)	☐	☐
6.3	Disable the automatic run of safe files in Safari (Scored)	☐	☐
6.4	Safari disable Internet Plugins for global use (Not Scored)	☐	☐
6.5	Use parental controls for systems that are not centrally managed (Not Scored)	☐	☐
7	**Appendix: Additional Considerations**		
7.1	Wireless technology on macOS (Not Scored)	☐	☐
7.2	iSight Camera Privacy and Confidentiality Concerns (Not Scored)	☐	☐
7.3	Computer Name Considerations (Not Scored)	☐	☐
7.4	Software Inventory Considerations (Not Scored)	☐	☐
7.5	Firewall Consideration (Not Scored)	☐	☐
7.6	Automatic Actions for Optical Media (Not Scored)	☐	☐
7.7	App Store Automatically download apps purchased on other Macs Considerations (Not Scored)	☐	☐
7.8	Extensible Firmware Interface (EFI) password (Not Scored)	☐	☐
7.9	FileVault and Local Account Password Reset using AppleID (Not Scored)	☐	☐
7.10	Repairing permissions is no longer needed (Not Scored)	☐	☐
7.11	App Store Password Settings (Not Scored)	☐	☐
7.12	Siri on macOS (Not Scored)	☐	☐
7.13	Apple Watch features with macOS (Not Scored)	☐	☐
7.14	Apple File System (APFS) (Not Scored)	☐	☐
7.15	System information backup to remote computers (Not Scored)	☐	☐
7.16	Unified logging (Not Scored)	☐	☐
7.17	AirDrop security considerations (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 6, 2016	1.0.0	Initial Release
Sep 6, 2018	1.1.0	Changed FileVault check to work on APFS and Core Storage
Sep 6, 2018	1.1.0	The audit for "Time Machine Volumes Are Encrypted" Corrected
Sep 6, 2018	1.1.0	Added APFS encrypted check and Core Storage encryption check
Sep 6, 2018	1.1.0	Password controls have been rewritten
Sep 6, 2018	1.1.0	Updated "Discoverable" to "Bluetooth Discoverable" and set as unscored
Sep 6, 2018	1.1.0	Enable system data files and security update installs audit procedure updated
Sep 6, 2018	1.1.0	Control to ensure firewall set to log added
Sep 6, 2018	1.1.0	unscored control on unified logging info added
Sep 6, 2018	1.1.0	removed the display sleep control
Sep 6, 2018	1.1.0	Corrected inconstant formatting