CENTER FOR INTERNET SECURITY

CIS Apple OSX 10.8 Benchmark

v1.2.0 - 04-02-2015

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, CIS Apple OSX 10.8 Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Apple OSX 10.8. This guide was tested against Apple OSX 10.8. 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 OSX 10.8.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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://community.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
Blake Frantz , *Center for Internet Security*
Dallas Moore
Khürt Williams MSEE, BSEE, CISSP, CRISC, ITILv3
Taylor Armstrong
Reeves Smith
Stephen Tihor , *Church Pension Group*
Heather Tarallo
Dawn Vincej
Gary Gapinski
Paul Campbell
John Oliver Linux+, Security+, ACTC, ACMT, *SAIC*

Editor
Rael Daruszka , *Center for Internet Security*

Additionally, the CIS community thanks the following individuals for their contributions to previous CIS Apple OS X Benchmarks, which were used in the development of this benchmark: Allan Marcus, Charles Heizer, Ron Colvin, Mark Fleming, Blake Frantz, Eric Hall, and Lawrence Charters.

Recommendations

1 Install Updates, Patches and Additional Security Software

Install Updates, Patches and Additional Security Software

1.1 Verify all application 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.

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 > Software Update - If prompted, enter an admin name and password.
2. Verify that all available updates and software patches are installed.

Alternatively:

1. In Terminal, run the following:

```
sudo softwareupdate -l
```

2. Result: `No new software available`

Remediation:

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

1. Choose Apple (□) menu > Software Update - 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:

```
sudo 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.

References:

1. Rule Version (STIG-ID): OSX00055 M6

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.

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:

```
sudo softwareupdate --schedule
```

2. Make sure the result is: `Automatic check is on`

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 softwareupdate --schedule on
```

References:

1. Rule Version (STIG-ID): OSX00290 M6

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 Disable 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 | grep "Bluetooth:" -A 20 | grep Connectable
```

5. Output should include: Connectable: Yes

Remediation:

Perform the following to implement the prescribed state:

1. In 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.

2.1.2 Disable 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 it's location.

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:

1. Open *System Preferences*
2. Select *Bluetooth*
3. Uncheck *Discoverable*

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.

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" (Not Scored)

Profile Applicability:

- Level 2

Description:

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

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 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 -setnetworktimeserver on
```

Impact:

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.

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 a minute is considered acceptable. That may be too great for your organizations, adjust 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:

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
3. `sudo ntpdate -svd` *`your.time.server`*

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
3. `sudo ntpdate -sv` *`your.time.server`*

Impact:

Accurate time is required for many computer functions.

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 OS X 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 *0* 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 *ScreenSaver*
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 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*

References:

1. SV-37242r1_rule

2.3.3 Verify Display Sleep is set to a value larger than the Screen Saver (Not Scored)

Profile Applicability:

- Level 1

Description:

If the Screen Saver is used to lock the screen, verify the Display Sleep settings are longer than the Screen Saver setting. If the display goes to sleep before the screen saver activates, the computer will appear to be off, but will be unprotected.

Rationale:

Users of the system can easily assume that the computer is protected when the display goes to sleep. The computer should be configured so that the screen is locked whenever the display turns off automatically.

Audit:

In System Preferences: Energy Saver, verify the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.

Alternatively, use the following command:

```
pmset -g | grep displaysleep
```

and verify the value returned is longer than the Screen Saver, if the Screen Saver is used to lock the screen.

Remediation:

In System Preferences: Energy Saver, drag the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.

Alternatively, use the following command:

```
sudo pmset -c displaysleep 0
```

Note: The `-c` flag means "wall power." Different settings must be used for other power sources.

2.3.4 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: Exposé & Spaces, 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: Exposé & Spaces, 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:

1. 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:

1. 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.

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 `nothing found to load`

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:

1. Run the following command in Terminal:

```
system_profiler SPPrintersDataType
```

The output should show "Shared: No" for all printers. If no printers are present, the above command will yield "`Status: The printers list is empty.`"

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 OSX clients, not servers.

OS X 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. OS X 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 OS X 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:

1. Run the following command in Terminal:

```
sudo systemsetup -setremotelogin off
```

Impact:

The SSH server built-in to OS X 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 OS X 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

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:

1. Run the following command in Terminal:

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

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.

References:

1. Rule Version (STIG-ID): OSX00470 M6

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

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)

The two 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

4. grep -i
   array /Library/Preferences/SystemConfiguration/com.apple.smb.server.plist
5. 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 an OS X 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 to ensure 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

Remediation:

In System Preferences: Sharing, turn off Remote Management.

Impact:

Many organizations utilize ARD for client management.

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 2

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

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:

1. Run the following command in Terminal:
2. `pmset -g | grep -i 'AC Power'`

   and verify the value returned is AC Power-1*

   The asterisk represents the current power source. If the power source is "AC Power"

```
pmset -c -g | grep womp; pmset -b -g | grep womp
```

3. Verify that both values returned are 0

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

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

Note: The `-c` flag means "wall power." Different settings must be used for other power sources.

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.

2.5.2 Disable sleeping the computer when connected to power (Scored)

Profile Applicability:

- Level 2

Description:

In some institutions certain software must be run that requires the computer to be awake. In these situations the computer should not be set to sleep.

Not allowing the computer to sleep will use more power and increase the cost to operate the computer. This must be weighed against the needs of the organization.

Rationale:

The ability to apply security patches and perform vulnerability assessments on the system is reduced when the system is sleeping.

Audit:

In System Preferences: Energy Saver, verify the slider for "Put the computer to sleep..." to never.

Alternatively, use the following commands:

```
pmset -g | grep -i 'AC Power'
```

and verify the value returned is AC Power-1*

The asterisk represents the current power source. If the power source is "AC Power"

```
pmset -g | grep sleep
```

and verify the value returned is `0`

Remediation:

In System Preferences: Energy Saver, drag the slider for "Put the computer to sleep..." to never.

Alternatively, use the following command:

```
sudo pmset -c sleep 0
```

Impact:

Preventing systems from sleeping may increase energy consumption

2.6 Security & Privacy

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

2.6.1 Enable FileVault (Scored)

Profile Applicability:

- Level 1

Description:

FileVault secures a system's data by automatically encrypting its content 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:

```
diskutil cs list | grep -i encryption
```

2. On a booted system the Logical Volume should show as both Encrypted and unlocked

   Encryption Status: Unlocked

   Encryption Type: AES-XTS

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*

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:

1. 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:

1. Run the following command in Terminal:

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

2.6.3 Enable "Automatically update safe downloads list" (Scored)

Profile Applicability:

- Level 1

Description:

Apple maintains a list of known malicious software that is used during the safe download check to determine if a file contains malicious software, the list is updated daily by a background process.

Rationale:

Maintaining an updated safe downloads list mitigates the risk of unintentionally downloading a piece of malicious software.

Audit:

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

1. Run the following command in Terminal:

```
ls -l \
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect.plist
```

2. Check the date on the last update of the plist file for an update in the last four months

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Security & Privacy*
3. Select the *General* tab
4. Select *Advanced*
5. Check *Automatically update safe downloads list*

Alternatively:

- Run the following command in Terminal:

```
sudo /usr/libexec/XProtectUpdater
```

2.6.4 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.

2.6.5 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:

1. 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.

2.6.6 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

2.7 iCloud

iCloud is Apple's service for synchronizing, storing and backing up data from Apple applications in both OS X 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 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 you mission.

Rationale:

Audit:

Remediation:

2.8 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

2.9 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*

2.10 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 OS X. Apple is no longer providing Java updates for OS X 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 is one of the most exploited environments and is no longer maintained by Apple, old versions 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 not installed a dialogue box will offer to go to Oracle to download Java 8

Remediation:

Java 6 can be removed completely or, if necessary Java applications will only work with Java 6, a custom path can be used.

Impact:

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

2.11 Configure Secure Empty Trash (Scored)

Profile Applicability:

- Level 2

Description:

Secure Empty Trash not only removes the file information from the file directory, it also overwrites the data in the file with meaningless data, thus preventing the file from being recovered.

Rationale:

Configuring Secure Empty Trash 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.

Audit:

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

1. For each user on the system, run the following command in Terminal:

```
defaults read ~/Library/Preferences/com.apple.finder EmptyTrashSecurely
```

2. Make sure the value returned for each user is `1`.

Remediation:

Perform the following to implement the prescribed state:

1. Select *Finder*
2. Select *Preferences*
3. Select *Advanced*
4. Check *Empty Trash Securely*

Impact:

Secure Empty Trash can take a long time, with FileVault in place the protection is erasing data within an already encrypted volume. This control does not effect the use of the rm command in the terminal. Users who rarely have large files to erase can use rm as a workaround

- cd ~/.Trash
- rm myproject-cui.pptx

3 Logging and Auditing

This section provide guidance on configuring the logging and auditing facilities available in OSX 10.8.

3.1 Configure newsyslog.conf

It is important to save logs long enough to meet organizational requirements. The logs can assist in troubleshooting problems as well as used for forensic investigations in the case of network attacks, malware or employee misuse. Many of the retention and rotation configurations are set in the `/etc/newsyslog.conf` file.

This Benchmark documents how to retain roughly 60 days, 9 weeks or 2 months of logs through rotation and retention settings. The thought was that 30 days is insufficient in most use cases and organizations with other requirements may very well exceed the minimum requirements documented here. The following controls provide specifics on weekly rotations and keeping a minimum of nine instances. Logs may be rotated daily, weekly or monthly and retained as long as needed. More detail are in the man page for `newsyslog.conf`.

Users of this Benchmark should be aware that OS X also uses `/etc/asl.conf`, there are details in the `asl.conf` man page. There are no current suggestions to modify that

configuration of `asl.conf` for this (10.8) benchmark, there are configuration changes to `asl.conf` as part of the 10.9 Benchmark.

3.1.1 Retain system.log for 90 or more days (Scored)

Profile Applicability:

- Level 2

Description:

OSX writes information pertaining to system-related events to the file `/var/log/system.log` and has a configurable retention policy for this file.

Rationale:

Archiving and retaining `system.log` for 90 or more days 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:

```
cat /etc/newsyslog.conf
```

2. Verify the `count` is 3 or higher for `system.log`
3. Verify the `when` contains "M" for `system.log`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo vim /etc/newsyslog.conf
```

2. Consult the newsyslog man page for date format
3. Set the `count` column to 3 or greater for `system.log`
4. Set the `when` column to contain "M" for `system.log`

Impact:

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

Default Value:

7 days

3.1.2 Retain secure.log for 90 or more days (Scored)

Profile Applicability:

- Level 2

Description:

OSX writes information pertaining to system-related events to the file `/var/log/secure.log` and has a configurable retention policy for this file.

Rationale:

Archiving and retaining `secure.log` for 90 or more days 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:

```
cat /etc/newsyslog.conf
```

2. Verify the `count` is 3 or higher for `secure.log`
3. Verify the `when` contains "M" for `secure.log`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo vim /etc/newsyslog.conf
```

2. Consult the `newsyslog` man page for date format
3. Set the `count` column to 3 or greater for `secure.log`

4. Set the when column to contain "M" for `secure.log`

Impact:

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

Default Value:

7 days

3.1.3 Retain appfirewall.log for 90 or more days (Scored)

Profile Applicability:

- Level 2

Description:

OSX writes information pertaining to system-related events to the file `/var/log/appfirewall.log` and has a configurable retention policy for this file.

Rationale:

Archiving and retaining `appfirewall.log` for 90 or more days 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:

```
cat /etc/newsyslog.conf
```

2. Verify the `count` is 3 or higher for `appfirewall.log`
3. Verify the `when` contains "M" for `appfirewall.log`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo vim /etc/newsyslog.conf
```

2. Consult the `newsyslog` man page for date format
3. Set the `count` column to 3 or greater for appfirewall.`log`
4. Set the `when` column to contain "M" for appfirewall.`log`

Impact:

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

Default Value:

7 days

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

Profile Applicability:

- Level 2

Description:

OSX writes information pertaining to system-related events to the file `/var/log/install.log` and has a configurable retention policy for this file.

Rationale:

Archiving and retaining `install.log` for 365 or more days 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:

```
cat /etc/newsyslog.conf
```

2. Verify the `count` is 12 or higher for install.log
3. Verify the `when` contains "M" for install.log

Remediation:

Perform the following to implement the prescribed state:

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

```
sudo vim /etc/newsyslog.conf
```

    2. Consult the newsyslog man page for date format
    3. Set the `count` column to 12 or greater for install.log
    4. Set the when column to contain "M" for install.log

Impact:

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

Default Value:

7 days

3.2 Enable security auditing (Scored)

Profile Applicability:

- Level 1

Description:

OSX'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:

1. Run the following command in Terminal:

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

References:

1. Rule Version (STIG-ID): OSX00140 M6

3.3 Configure Security Auditing Flags (Scored)

Profile Applicability:

- Level 1

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:

Changing configuration files should be done carefully only after backup versions are available. Changing this file in particular incorrectly might break the system until the old file can be restored.

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.

Impact:

Without proper auditing unauthorized changes will not be discovered. Changing this file needs to be done carefully; a misconfigured confguration file will prevent the operating system from booting.

References:

1. Rule Version (STIG-ID): OSX00145 M6

3.4 Enable remote logging for Desktops on trusted networks (Not Scored)

Profile Applicability:

- Level 2

Description:

A log is a file that records the events that occur while an operating system and/or software is running. The built-in syslog capability in OS X runs over UDP without encryption. Broadcasting log unencrypted over the internet is not a good idea. While syslog may be acceptable on some internal trusted networks it is not a solution for mobile devices that hop between networks.

Solutions for logging might include:

- An encrypted tunnel that auto reconnects for each new network the laptop joins
- A third party logging daemon that encrypts the log transmission

- A local store and forward script that bundles the logs and sends periodically through an encrypted transmission (ssh) or when the device is connected to a trusted network

Rationale:

In addition to local logging, remote logging can be enabled for internal computers on trusted networks. Local logs can be altered if the computer is compromised. Remote logging mitigates the risk of having the logs altered.

Audit:

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo pico /etc/syslog.conf
```

2. Add the following line to the top of the file, replacing "`your.log.server`" with the name or IP address of the log server, and keeping all other lines intact. `*.* @your.log.server`
3. Exit, saving changes.
4. Reboot the system.

References:

1. Rule Version (STIG-ID): OSX00155 M6

4 Network Configurations

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

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 Mac OS X 10.8 is integrated with Bonjour and should not be turned off, but 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.

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. Make a backup copy of the `mDNSResponder.plist` file as a precaution.
2. Open the `mDNSResponder.plist` file in Terminal using your preferred text editor. Below is a sample command:

```
sudo nano "/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist"
```

3. Add `<string>-NoMulticastAdvertisements</string>` to the array in the `ProgramArguments` section. For example, the following:

```
    <key>ProgramArguments</key>
    <array>
        <string>/usr/sbin/mDNSResponder</string>
        <string>-launchd</string>
    </array>
```

becomes:

```
    <key>ProgramArguments</key>
    <array>
        <string>/usr/sbin/mDNSResponder</string>
        <string>-launchd</string>
        <string>-NoMulticastAdvertisements</string>
    </array>
```

4. Save the file.

Impact:

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

4.2 Enable "Show Wi-Fi status in menu bar" (Not 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, that has not always been the case, This control only pertains to systems that have a wireless NIC. 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:

```
sudo 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*

Impact:

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

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 attackers 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.

4.4 Ensure http server is not running (Scored)

Profile Applicability:

- Level 1

Description:

Mac OS X 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.

4.5 Ensure ftp server is not running (Scored)

Profile Applicability:

- Level 1

Description:

Mac OS X 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:

Mac OS X can act 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 Web Server is not running and is not set to start at boot

Stop the Web 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 an OS X 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 stepped 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 OS X 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 OS X 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------
```

1. 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>
```

2. sudo chmod -R og-rw /Users/<username>
3. Substitute user name in <username>.
4. 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 Repair permissions regularly to ensure binaries and other System files have appropriate permissions (Not Scored)

Profile Applicability:

- Level 1

Description:

Software installations, Upgrades and updates and end user activity can all end up changing the access controls on the Operating System. On a normal system lots of files get touched and changed and proper maintenance is necessary for good security. The standard software load on an end user system has so many moving parts that have regular updates to require periodic file permissions repair. We believe that a weekly permissions check should be scheduled to fix anything needed.

Rationale:

Permission problems can lead to exploitable gaps in the operating system. Without expected controls in place the system is more likely to be successfully attacked.

Audit:

Check the System logs to ensure that Repair permissions was run in the last week.

sudo cat /var/log/system.log* | grep RepairPermissions

Remediation:

Manually run the check using Disk Utility or through the command line. A schedule should be set in `/etc/periodic/weekly/`

```
sudo diskutil repairPermissions /
```

Impact:

System executables and other important files could be modified much more easily if appropriate permissions are not in place.

5.1.3 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/Bad\ Permissions.app/
```

Impact:

Applications changed will no longer be world writable

5.1.4 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
```

5.1.5 Check Library folder for world writable folders (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 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 "`# Defaults specification`" section, add the line:

```
Defaults timestamp_timeout=0
```

5.3 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 Mac OS X. 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.

5.4 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 Mac OS X. 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.

5.5 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. OS X can check whether the certificate is still valid based on issued parameters within the certificate.

Rationale:

A rogue or compromised certificate should not be trsuted

Audit:

Run the following commands

```
1. defaults read com.apple.security.revocation CRLStyle
2. defaults read com.apple.security.revocation OCSPStyle
```

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

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

Profile Applicability:

- Level 2

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. In the UNIX/Linux world, the system administrator 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 Mac OS X client computer. It is enabled on Mac OS X Server. 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.

5.7 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 -currentHost write com.apple.screensaver askForPassword -int 1
```

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

Impact:

There will be a delay for a user to resume until after he or she is successfully authenticated.

5.8 Require an administrator password to access locked preferences (Scored)

Profile Applicability:

- Level 1

Description:

System Preferences controls system and user settings on an OS X 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 "<false/>"

Remediation:

In System Preferences: Security, General tab under Advanced, check "Require an administrator password to access locked preferences" is checked.

Impact:

Without this control is is more possible that an unauthorized user might change system wide settings.

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:

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

Profile Applicability:

- Level 1

Description:

OSX 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:

```
grep -i "<string>authenticate-session-owner-or-admin</string>"
/etc/authorization
```

2. No results will be returned if the system is configured as recommended.

Remediation:

Perform the following to implement the prescribed state:

1. Open `/etc/authorization`
2. Locate the `system.login.screensaver` setting
3. Set the `string` element beneath the `key` element to `authenticate-session-owner.`

```
<key>system.login.screensaver</key>
<dict>
     <key>class</key>
        <string>rule</string>
        <key>comment</key>
        <string>The owner can unlock the screensaver.</string>
        <key>rule</key>
        <string>authenticate-session-owner</string>
```

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

5.11 Complex passwords must contain an Alphabetic Character (Scored)

Profile Applicability:

- Level 1

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.

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 -getglobalpolicy | tr " " "\n" | grep requiresAlpha
```

2. Verify the value returned has requiresAlpha=1 or greater

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls

1. Run the following command in Terminal:

```
sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=5 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"
```

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.

5.12 Complex passwords must contain a Numeric Character (Scored)

Profile Applicability:

- Level 1

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.

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 -getglobalpolicy | tr " " "\n" | grep requiresNumeric
```

2. Verify the value returned has requiresSymbol=1 or greater

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls

1. Run the following command in Terminal:

```
sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=5 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"
```

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.

5.13 Complex passwords must contain a Symbolic Character (Scored)

Profile Applicability:

- Level 1

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.

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 -getglobalpolicy | tr " " "\n" | grep requiresSymbol
```

2. Verify the value returned has requiresSymbol=1 or greater

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls

1. Run the following command in Terminal:

```
sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=5 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"
```

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.

References:

1. Rule Version (STIG-ID): OSX00038 M6

5.14 Set a minimum password length (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Information systems not protected with strong password schemes including passwords of minimum length provide the opportunity for anyone to crack the password and gain access to the system, and cause the device, information, or the local network to be compromised or a Denial of Service.

Audit:

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

1. Run the following command in Terminal:

```
pwpolicy -getglobalpolicy | tr " " "\n" | grep minChars
```

2. Verify the value returned has minChars=15 or greater

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls

1. Run the following command in Terminal:

```
sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=5 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"
```

Impact:

Short passwords can be easily attacked.

5.15 Configure account lockout threshold (Scored)

Profile Applicability:

- Level 1

Description:

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

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 -getglobalpolicy | tr " " "\n" | grep maxFailedLoginAttempts
```

2. Verify the value returned has maxFailedLoginAttempts=5 or less

Remediation:

Perform the following to implement the prescribed state for all pwpolicy controls

1. Run the following command in Terminal:

```
sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=5 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"
```

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.

5.16 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:

1. 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.

5.17 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:

1. 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

5.18 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

5.19 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.

5.20 Secure individual keychain items (Not Scored)

Profile Applicability:

- Level 2

Description:

By default, the keychains 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 the keychains to something different than the logon password, and doing so would keep that keychains locked until they are needed after login.

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.

5.21 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 Mac OS X. 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.

6 User Accounts and Environment

Account management is a central part of security for any computer system including OS X. General practices should be followed to ensure that all accounts on a system are still needed and that default accounts should be 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 OS X if the computer is in 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.

OS X 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:

1. 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:

1. 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:

1. 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.

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:

1. Run the following command in Terminal:

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

For SMB sharing:

1. 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.

6.2 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`

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 files safety on the files type. The files considered safe include word files, PDF documents, and picture files.

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. The attackers make sure that the malicious file type will fall within Safari's safe files policy and will download and run 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 Use parental controls for systems that are not centrally managed (Not Scored)

Profile Applicability:

- Level 1

Description:

Many aspects and features of OS X 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 OS X security guides.

7.1 Wireless Adapters on Mobile Clients (Not Scored)

Profile Applicability:

- Level 2

Description:

Wireless access is part of the feature set required for mobile computers and is considered essential for most users. There are specialized environments where the use of wireless networking is considered unacceptable. This is not the general use case for OS X and is beyond a level 2 requirement. If you have comsec requirements turn off Wi-FI as needed.

Rationale:

Audit:

Remediation:

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. General rule should be that if the camera can capture images that could cause embarrassment or an adverse impact the camera should be covered unless it is in use.

Rationale:

Audit:

Remediation:

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 easier.

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.

Rationale:

Audit:

Remediation:

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 corporate 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.

Rationale:

Audit:

Remediation:

7.5 Firewall Consideration (Not Scored)

Profile Applicability:

- Level 2

Description:

In addition to the Application Layer Firewall (`alf`) mentioned in the benchmark, OSX 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/

Rationale:

Audit:

Remediation:

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

Rationale:

Audit:

Remediation:

7.7 AirDrop (Not Scored)

Profile Applicability:

- Level 2

Description:

Airdrop is an adhoc file transfer capability that on OS X works over wireless networks. Each user must select "AirDrop" in a Finder Window. After the other computer is visible a file can be drag-and-dropped from one computer to another. Each file must be explicitly accepted. When AirDrop is no longer selected the discoverable portion as well as the file transfer capabilities are off. This transfer is limited to the range of adhoc wireless networks, is not always available like file sharing services, and does not involve data storage on public clouds or the creation of additional electronic copies on infrastructure file, email, ftp servers. Compared to many of the common file transfer methods AirDrop is both simpler and more secure.

If all other file transfer methods are heavily audited or blocked this methodology may circumvent audit controls. AirDrop does not respect network segmentation in the same physical space. If your organization has computers located in the same physical location that have logical controls to prevent any data from transferring between them (including the use of third party servers) you should disable Air Drop.

http://siliconchaos.com/2012/07/disable-airdrop-in-mac-os-x-lion/

http://www.macprovideo.com/hub/mac-osx/osx-airdrop-great-for-sharing-why-it-will-never-work

Rationale:

Audit:

Remediation:

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 Mac OS X 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 OS X 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 well if used more critical.

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/

Rationale:

Audit:

Remediation:

7.9 Apple ID password reset (Not Scored)

Profile Applicability:

- Level 2

Description:

Apple has a service that will allow a user that has turned it on to reset their login password by signing in to Apple with their Apple ID. This sounds like a service that needs to be explicitly turned off in an Enterprise environment. There are however many factors here.

- You cannot reset your password if the computer is using FileVault
- You cannot reset anything but a local account
- You need physical access to the computer on a network that can phone home to Apple
- The current login keychain will have to be discarded unless the user remembers the old password

The main use case I see for disabling this service is where you are not using FileVault to encrypt the Mac but are using Firmware controls to limit boot options with local accounts. Otherwise the user has other options for resetting a password that are more time consuming but just as effective when they have physical access to the computer.

Rationale:

Audit:

Remediation:

Appendix: Change History

Date	Version	Changes for this version
03-19-2015	1.1.0	"Turn on filename extensions" - update remediation
03-19-2015	1.1.0	"Retain system.log" - updated title/audit/remediation
03-19-2015	1.1.0	"Retain secure.log" - updated title/audit/remediation
03-19-2015	1.1.0	"Retain appfirewall.log" - updated title/audit/remediation
03-19-2015	1.1.0	"Retain install.log" - updated title/audit/remediation
03-19-2015	1.1.0	"Enable 'Show Wi-Fi status in menu bar'" updated decription
03-19-2015	1.1.0	"Disable IPv6" - removed
03-19-2015	1.1.0	Added "File System Permissions and Access Controls" sectin
03-19-2015	1.1.0	5.6 - updated title/scoring level/scoring status/audit/remediation
03-19-2015	1.1.0	"Disable automatic login" - updated audit/remediation procedures
03-19-2015	1.1.0	"Set a maximum password age" - removed
03-19-2015	1.1.0	"Verify newly created password content" - removed
03-19-2015	1.1.0	"Configure account lockout duration" - removed

03-19-2015	1.1.0	"Configure account lockout threshold" - updated audit/remediation procedures
03-19-2015	1.1.0	"Disable Show password hints" - updated audit/remediation procedures
03-19-2015	1.1.0	"Disable guest account login" - updated audit/remediation procedure
03-19-2015	1.1.0	"Disable 'Allow guests to connect to shared folders'" - updated audit procedure
03-19-2015	1.1.0	Added "Configure newsyslog.conf"
03-19-2015	1.1.0	"Configure Secure Empty Trash" - updated audit/remediation procedures
03-19-2015	1.0.0	Initial Release
03-19-2015	1.1.0	1.1 - Updated Audit/Remediation Procedures
03-19-2015	1.1.0	2.1.1 - Updated Audit/Remediation Procedures
03-19-2015	1.1.0	"Disable Bluetooth "Discoverable" mode when not pairing devices" - updated audit/remediation procedures
03-19-2015	1.1.0	Remove "Disable 'Allow Bluetooth devices to wake this computer'"
03-19-2015	1.1.0	"Show Bluetooth status in menu bar" - updated audit procedure
03-19-2015	1.1.0	"Enable "Set time and date automatically" - updated audit/remediation procedures
03-19-2015	1.1.0	2.3.1 - Updated title/description/remediation/audit
03-19-2015	1.1.0	"Secure screen saver corners" - changed from Not Scored to Scored
03-19-2015	1.1.0	"Verify Display Sleep is set to a value larger

		than the Screen Saver" - Changed from Scored to Not Scored
03-19-2015	1.1.0	"Pair the remote control infrared receiver if enabled" - updated remediation procedure
03-19-2015	1.1.0	"Enable FileVault" - updated audit procedure
03-19-2015	1.1.0	"Disable 'Wake for network access'" - updated remediation procedure
03-19-2015	1.1.0	"Disable Remote Login" - updated audit/remediation procedures
03-19-2015	1.1.0	"Disable Internet Sharing" - updated audit procedure
03-19-2015	1.1.0	"Disable Remote Apple Events" - updated audit/remediation procedures
03-19-2015	1.1.0	"Set a screen corner to Start Screen Saver" - updated audit procedure
03-31-2015	1.2.0	Updated 2.2.1 description (Ticket #155)
03-31-2015	1.2.0	Changed 2.2.1 to Level 2 unscored (Ticket #155)
03-31-2015	1.2.0	Updated 2.2.1 remediation (Ticket #131)
03-31-2015	1.2.0	Updated 2.4.2 audit and remediation (Ticket #166)
03-31-2015	1.2.0	Removed 3.4 audit (Ticket #160)
03-31-2015	1.2.0	Updated 2.4.7 audit (Ticket #147)
03-31-2015	1.2.0	Updated 2.5.1 audit (Ticket #141)
03-31-2015	1.2.0	Update 2.8 description and audit (Ticket #129)
03-31-2015	1.2.0	Updated 5.1.1 description (Ticket #137)

03-31-2015	1.2.0	Updated 5.8 Audit (Ticket #186)
03-31-2015	1.2.0	Moved NFS from 2.4.8 to new recommendation 4.6 (Ticket #187)
03-31-2015	1.2.0	Updated 2.4.8 Audit audit and remediation (Ticket #185)
03-31-2015	1.2.0	Updated 2.5.2 audit (Ticket #140)
03-31-2015	1.2.0	Updated 5.4 to not duplicate 5.3 (Ticket #181)
03-31-2015	1.2.0	Removed FTP from recommendation 2.4.8 (Ticket #118)
03-31-2015	1.2.0	Split 5.3 into 5.3 and 5.4 (Ticket #138)
03-31-2015	1.2.0	Changed 5.1.5 to Level 2 (Ticket #132)
03-31-2015	1.2.0	Added recommendation 2.6.5 (Ticket #180)
03-31-2015	1.2.0	Added recommendation 7.9 (Ticket #179)
03-31-2015	1.2.0	Added recommendation 2.2.2 (Ticket #163)
03-31-2015	1.2.0	Updated 2.2.1 impact (Ticket #176)
03-31-2015	1.2.0	Removed recommendation 2.10 (Ticket #178)
03-31-2015	1.2.0	Added recommendation 4.4 (Ticket #171)
03-31-2015	1.2.0	Updated 1.1 description (Ticket #167)
03-31-2015	1.2.0	Added recommendation 5.17 (Ticket #154, Ticket #128)
03-31-2015	1.2.0	Added recommendation 4.5 (Ticket #118)
03-31-2015	1.2.0	Added recommendation 5.5 (Ticket #152)