

CIS Apple OSX 10.8 Benchmark

v1.0.0 - 02-04-2014

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

Table of Contents	2
Overview	3
Intended Audience	3
Consensus Guidance.....	3
Typographical Conventions	4
Scoring Information	4
Profile Definitions	5
Acknowledgements	6
Recommendations	7
1 Install Updates, Patches and Additional Security Software	7
2 System Preferences.....	9
2.1 Bluetooth	9
2.2 Date & Time	13
2.3 Desktop & Screen Saver	13
2.4 Sharing.....	17
2.5 Energy Saver	26
2.6 Security & Privacy	28
3 Logging and Auditing	36
4 Network Configurations.....	44
5 System Access, Authentication and Authorization	48
6 User Accounts and Environment.....	72
6.1 Accounts Preferences Action Items	72
Appendix: Additional Considerations	80
Appendix: Change History	83

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
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	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, *NASA*

Editor

Heather Tarallo, *Center for Internet Security*

Contributor

Taylor Armstrong

Reeves Smith

Gary Gapinski

Dawn Vincej

Stephen Tihor, *Church Pension Group*

Jonathon Brandt Buckley

Charles Heizer

Blake Frantz, *Center for Internet Security*

Dallas Moore

Khürt Williams CISSP, CRISC, ITIL

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

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.

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. Open *System Preferences*
2. Select *Software Update*
3. Select *Check Now*
4. 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 implement the prescribed state:

1. Open *System Preferences*
2. Select *Software Update*

3. Select *Check Now*
4. Download and install all available updates and software patches.

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 connecting them to 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:

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 the computer is compliant only if paired devices exist
4. If step 3 is 1 in Terminal, run the following command:

```
system_profiler | grep -ir paired
```

5. Output should include: (standard input): Paired: 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
```

References:

1. Bluetooth Security, Systems and Network Analysis Center, National Security Agency

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 its 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:

1. Run the following command in Terminal:

```
system_profiler | grep -ir discoverable
```

2. Verify the value returned for `discoverable` is `Off`

Remediation:

Perform the following to implement the prescribed state:

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

2.1.3 Disable “Allow Bluetooth devices to wake this computer” (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

An unauthorized user could use a Bluetooth device to wake a computer and then attempt to gain access.

Audit:

Perform the following to ensure the system is configured as:

1. Open *System Preferences*
2. Select *Bluetooth*
3. Select *Advanced*
4. Verify *Allow Bluetooth devices to wake this computer* is not checked

Remediation:

Perform the following to implement the prescribed state:

1. Open *System Preferences*
2. Select *Bluetooth*
3. Select *Advanced*
4. Uncheck *Allow Bluetooth devices to wake this computer*

2.1.4 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:

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/MenuExtras/Bluetooth.menu

Remediation:

In System Preferences: Bluetooth, turn Show Bluetooth Status In Menu Bar on.

2.2 Date & Time

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 15 minutes or less for the screen saver (Scored)

Profile Applicability:

- Level 1

Description:

The inactivity interval is a measurement of time before the screensaver engages.

Rationale:

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

Audit:

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

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 (< 900)

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 15 minutes or less

Alternatively:

1. In Terminal, run the following command:

```
defaults -currentHost write com.apple.screensaver idleTime -int 900
```

2.3.2 Secure screen saver corners (Not 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:

1. Run the following command in Terminal:

```
read ~/Library/Preferences/com.apple.dock
```

2. Verify the value returned for the corner keys is not 1

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 (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 2

Description:

A user should be able to activate the screen saver quickly. The intent of this control is to resemble the control-alt-delete on Windows Systems. 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, Use the following command:

```
read ~/Library/Preferences/com.apple.dock
```

Verify at least one of the *-corner keys has a value of 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:

1. Run the following command in Terminal:

```
launchctl list | grep -I eppc
```

2. There should be no results.

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

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

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.

Rationale:

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

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

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

Not output should be present.

Remediation:

Perform the following to implement the prescribed state:

1. Run the following commands in Terminal:

```
sudo defaults write /Library/Preferences/SystemConfiguration/com.apple.nat \
NAT -dict Enabled -int 0

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

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:

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:

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). Additionally, the scope of the benchmark is for Apple OSX clients, not servers.

OS X does not have an IP based firewall, TCP Wrappers, Brute-Force password guessing mitigations, or frequent POSIX patching enabled by default and most OS X computers are mobile workstations. All of these factors can be parts of running a hardened SSH server.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

```
ssh localhost
```

2. Verify the value returned is `ssh: connect to host localhost port 22: Connection refused`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo launchctl unload /System/Library/LaunchDaemons/ssh.plist
```

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 tool-sets that do take advantage of SSH and 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

References:

1. Rule Version (STIG-ID): OSX00495 M6

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.

Audit:

Perform the following to ensure the system is configured as:

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*

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 ensure the system is configured as:

1. Run the following command in Terminal:

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

2. Verify the value returned is 0

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/com.apple.Bluetooth PANServices -int 0  
sudo killall -HUP blued
```

2.4.8 Disable File Sharing (Scored)

Profile Applicability:

- Level 1

Description:

Apple's File Sharing uses a combination of many technologies: FTP, SMB (Windows sharing) and AFP (Mac sharing)

Three common ways to share files using File Sharing are:

1. Apple File Protocol (AFP)
AFP under Snow Leopard 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. File Transfer Protocol (FTP)
FTP send password via clear text and thus is very insecure. FTP is commonly used for anonymous upload and download of files where security is of less concern. FTP should not be used on a client Mac except in rare case for temporary anonymous sharing.
3. 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 in 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:

1. Run the following command in Terminal:

```
sudo launchctl list | egrep '(ftp|nmbd|smbd|AppleFileServer)'
```

2. Ensure no output is present

Remediation:

Perform the following to implement the prescribed state:

1. 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
```

2. Run the following command in Terminal to turn off FTP from the command line:

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

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

```
sudo defaults delete \  
/Library/Preferences/SystemConfiguration/com.apple.smb.server EnabledServices
```

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

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:

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.

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:

1. Run the following command in Terminal:

```
pmset -g | grep womp
```

2. Verify the value returned is 0

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo pmset -c 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 command:

```
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 -ir encryption
```

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

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:

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.

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:

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:
 - 0 = off
 - 1 = on for specific services
 - 2 = on for essential services

2.7 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.

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:

1. Run the following command in Terminal:

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

2. 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 the following to implement the prescribed state:

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>

2.8 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:

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*

2.9 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:

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.

```
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 7

Remediation:

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

2.10 Disable Core Dumps (Scored)

Profile Applicability:

- Level 2

Description:

A core dump occurs when an application encounters a runtime error and the operating system dumps the application's state, including memory contents, to disk.

Rationale:

Since it is possible for a core dump to contain sensitive information, including passwords, it is recommended that core dumps be disabled in high security scenarios.

Audit:

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

1. Run the following command in Terminal:

```
launchctl limit core
```

2. Make sure the value returned is `core 0 0`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
launchctl limit core 0
```

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.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

```
sudo defaults read com.apple.finder EmptyTrashSecurely
```

2. Make sure the value returned is `1`

Remediation:

Perform the following to implement the prescribed state:

1. Select *Finder*
2. Select *Preferences*
3. 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.

3 Logging and Auditing

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

3.1 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:

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

3.2 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.

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:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

```
more /etc/syslog.conf
```

2. Ensure the name or IP address of the site's log server is listed as "your.log.server"

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

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, has begun, or is 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:

1. Run the following command in Terminal:

```
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. For example, DISA recommends filtering failed file attribute access events (`^-fa`), failed file creation events (`^-fc`), and failed file closure events (`^-cl`).

Remediation:

Perform the following to implement the prescribed state:

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

References:

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

3.4 Retain system.log for 30 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 30 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:

1. Run the following command in Terminal:

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

2. Verify the `count` is 30 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. Set the `count` column to 30 for `system.log`

Default Value:

7 days

3.5 Retain wtmp.log for 30 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 `wtm.log` for 30 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:

1. Run the following command in Terminal:

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

2. Verify the `count` is 30 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. Set the `count` column to 30 for `system.log`

Default Value:

7 days

3.6 Retain `secure.log` for 30 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 30 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:

1. Run the following command in Terminal:

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

2. Verify the `count` is 30 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. Set the `count` column to 30 for `secure.log`

Default Value:

7 days

3.7 Retain appfirewall.log for 30 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 30 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:

1. Run the following command in Terminal:

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

2. Verify the `count` is 30 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. Set the `count` column to 30 for `appfirewall.log`

Default Value:

7 days

3.8 Retain `install.log` for 30 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 30 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:

1. Run the following command in Terminal:

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

2. Verify the `count` is 30 for `install.log`

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

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

2. Set the `count` column to 30 for `install.log`

Default Value:

7 days

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:

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.

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:

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/MenuExtras/AirPort.menu`

Remediation:

Perform the following to implement the prescribed state:

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

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.

Create network locations as needed. Ideally, if your goal is to limit which interfaces can be used at any given time, one network location for each interface should be created. See the Appendix C for an example.

4.4 Disable IPv6 (Scored)

Profile Applicability:

- Level 1

Description:

Unless used, IPv6 should be turned off for each interface. IPv6 is not widely used yet, so most people can turn this off until needed. If IPv6 will be required it should be enabled in a separate location the user can switch to when v4 is not available.

Rationale:

Many network security controls are not IPv6 capable and there is additional risk in running a network stack that is not required.

Audit:

1. Run the following commands in Terminal:

```
ifconfig en0 | grep -ir inet6  
ifconfig en1 | grep -ir inet6
```

1. Neither output should contain "inet6" followed by an address

Remediation:

1. Run the following command in Terminal:

```
networksetup -getcurrentlocation
```


2. If the output does not identify it as a v6 location disable IPv6
3. Run the following command in Terminal:

```
sudo networksetup -setv6off Wi-Fi Ethernet
```

5 System Access, Authentication and Authorization

System Access, Authentication and Authorization

5.1 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:

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
```

5.2 Automatically lock the login keychain after 15 minutes of inactivity and when sleeping (Scored)

Profile Applicability:

- Level 1

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.

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 the value returned is: Keychain "<NULL>" lock-on-sleep timeout=900s

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 15 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.

5.3 Do not enable the “root” account (Scored)

Profile Applicability:

- Level 2

Description:

The root account is a super user 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 the root account puts the system at risk since any exploit would 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.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

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

2. Verify the value returned is:

```
No such key: AuthenticationAuthority
```

Remediation:

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).

5.4 Secure Home Folders (Scored)

Profile Applicability:

- Level 1
- Level 2

Description:

By default OS X 10.8 is set up to allow users to see into the top level of the home folder of all other networked users. This allows the user to drop files into the "Drop Box" folders of other users. Users are unable to see the sub-folders of the other networked users; folders such as My Documents and Library.

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 recommended above:

1. Run the following command in Terminal:

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

2. Verify the value returned is:

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

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo chmod 700 /Users/<username>
```

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

Impact:

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

5.5 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:

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.

5.6 Require a password to unlock each System Preferences pane (Scored)

Profile Applicability:

- Level 2

Description:

System Preference panes are a dynamically loaded plugin that allows the user to set personal preferences for specific applications or the system via a graphic user interface.

Rationale:

By requiring a password to unlock System Preferences, a casual user is less likely to compromise the security of the Mac.

Audit:

Perform the following to determine if the system is configured as prescribed:

```
security authorizationdb read system.preferences | grep "<key>shared</key>" | -A1
```

Ensure the output of the above command is as follows:

```
YES (0)
<key>shared</key>
<false/>
```

Remediation:

Perform the following to implement the prescribed state:

1. Using `sudo`, edit the `/private/etc/authorization` file. This file should be backed up first and then edited. This is a critical file for OS X operations and should be edited with the greatest of care.
1.
 1. Find `<key>system.preferences</key>`
 2. Then find the subsequent `<key>shared</key>`
 3. Then replace the subsequent `<true/>` with `<false/>`.

5.7 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/.GlobalPreferences \  
com.apple.userspref.DisableAutoLogin
```

2. Verify the value returned is 1.

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/.GlobalPreferences \  
com.apple.userspref.DisableAutoLogin -bool yes
```

5.8 Configure an 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 determine which partition or disk to load Mac OS X from. It also determines whether the user can enter single-user mode

Rationale:

Not setting a password for EFI is a possible point of intrusion. Protecting it from unauthorized access can prevent attackers from gaining access to a computer.

Audit:

Perform the following to ensure the system is configured as:

1. Log in with an administrator account and open the Firmware Password Utility located on the Mac OS X installation disc in */Applications/Utilities/*
2. Click *New*
3. Select *"Require password to start this computer from another source"*
4. In the *Password* and *Verify* fields, verify a new EFI password has been entered

Remediation:

Perform the following to implement the prescribed state:

1. Log in with an administrator account and open the Firmware Password Utility located on the Mac OS X installation disc in */Applications/Utilities/*
2. Click *New*
3. Select *"Require password to start this computer from another source"*
4. In the *Password* and *Verify* fields, enter a new EFI password and click OK

References:

1. Rule Version (STIG-ID): OSX00095 M6

5.9 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:

1. Run the following command in Terminal:

```
grep -ir "<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

5.10 Restrict sudo usage to a single terminal and for only one sudo instance at a time. (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:

Do not allow direct root login because the logs cannot identify which administrator logged in. Instead, log in using accounts with administrator privileges, and then use the `sudo` command to perform actions as root. These limit the use of the `sudo` command to a single command per authentication and also ensure, even if a timeout is activated, that later `sudo` commands are limited to the terminal in which authentication occurred.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

```
grep Defaults /etc/sudoers
```

2. Ensure the following items exist: "`Defaults tty_tickets`" and "`Defaults timestamp_timeout=0`"

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal: to set the values in the `/etc/sudoers` file:

```
VISUAL=pico visudo
```

2. Enter the following two lines in the file: `Defaults tty_tickets Defaults timestamp_timeout=0`
3. Save and exit the file.

References:

1. Rule Version (STIG-ID): OSX00110 M6

5.11 Disable "automatic logout" after a period of inactivity (Scored)

Profile Applicability:

- Level 1

Description:

Logging out occurs when a user intentionally closes off their access to a computer system. Automatic logout closes off a user's access without their consent after a period of inactivity.

Rationale:

The risk of losing unsaved work is mitigated by disabling automatic logout.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/.GlobalPreferences \  
com.apple.autologout.AutoLogOutDelay
```

2. Verify the value returned is 0.

Remediation:

Perform the following to implement the prescribed state:

1. Run the following command in Terminal:

```
sudo defaults write /Library/Preferences/.GlobalPreferences \  
com.apple.autologout.AutoLogOutDelay -int 0
```

5.12 Complex passwords must contain 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:

For a managed system:

1. Run the following command in Terminal:

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

2. Verify the value for `requiresAlpha` returned is 1

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep requiresAlpha
```

2. Verify the value for `requiresAlpha` returned is 1

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "requiresAlpha=1"
```

For a non-managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresAlpha=1"
```

References:

1. Rule Version (STIG-ID): OSX00036 M6

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:

For a managed system:

1. Run the following command in Terminal:

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

2. Verify the value returned for `requiresSymbol` is 1

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | \ngrep requiresSymbol
```

2. Verify the value returned for `requiresSymbol` is 1

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "requiresSymbol=1"
```

For non managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresSymbol=1"
```

References:

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

5.14 Set a maximum password age (Scored)

Profile Applicability:

- Level 1

Description:

A maximum password age is a set number of days a password can be used before the user is prompted by the system to change it.

Rationale:

The longer a password is in use, the greater the opportunity for someone to gain unauthorized knowledge of the passwords. Further, scheduled changing of passwords hinders the ability of unauthorized system users to crack passwords and gain access to a system.

Audit:

Perform the following to ensure the system is configured as:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | \
grep maxMinutesUntilChangePassword
```

2. Verify the value returned for `maxMinutesUntilChangePassword` is greater than 86400 or set to 0

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | \
grep maxMinutesUntilChangePassword
```

2. Verify the value returned for `maxMinutesUntilChangePassword` is greater than 86400

Remediation:

Perform the following to ensure the system is configured as:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "maxMinutesUntilChangePassword=86400"
```

For non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -setglobalpolicy \
"maxMinutesUntilChangePassword=86400"
```

References:

1. Rule Version (STIG-ID): OSX00020 M6

5.15 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:

For a managed system:

1. Run the following command in Terminal:

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

2. Verify the value returned for `minChars` is 15 or more

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep minChars
```

2. Verify the value returned for `minChars` is more than 15 or more

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "minChars=15"
```

For non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -setglobalpolicy "minChars=15"
```

References:

1. Rule Version (STIG-ID): OSX00030 M6

5.16 Verify newly created password content (Scored)

Profile Applicability:

- Level 1

Description:

Verifying newly created password content verifies that the user's password does not contain the user's account name and/or parts of the user's full name exceeding two consecutive characters.

Rationale:

Passwords that contain the user's account name and/or parts of the user's full name present a security risk since they make it easier for unauthorized persons to guess the user's password and gain access to the system.

Audit:

Perform the following to ensure the system is configured as:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep passwordCannotBeName
```

2. Verify the value returned for `passwordCannotBeName` is 1

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n/Local/Default -getglobalpolicy | tr " " "\n" | \ngrep passwordCannotBeName
```

2. Verify the value returned for `passwordCannotBeName` is 1

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "passwordCannotBeName=1"
```

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -setglobalpolicy "passwordCannotBeName=1"
```

References:

1. Rule Version (STIG-ID): OSX00040 M6

5.17 Configure account lockout duration (Scored)

Profile Applicability:

- Level 1

Description:

The account lockout duration specifies the amount of time that must pass between two successive login attempts to ensure a lockout will occur.

Rationale:

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

Audit:

Perform the following to ensure the system is configured as:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | \
grep minutesUntilFailedLoginReset
```

2. Verify the value returned for `minutesUntilFailedLoginReset` is 0

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | \
grep minutesUntilFailedLoginReset
```

2. Verify the value returned for `minutesUntilFailedLoginReset` is 0

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "minutesUntilFailedLoginReset=0"
```

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -setglobalpolicy "minutesUntilFailedLoginReset=0"
```

References:

1. Rule Version (STIG-ID): OSX00045 M6

5.18 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 prevents brute-force password attacks on the system.

Audit:

Perform the following to ensure the system is configured as:

For a managed system:

1. Run the following command in Terminal:

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

2. Verify the value returned for `maxFailedLoginAttempts` is between 1 and 3

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | \ngrep maxFailedLoginAttempts
```

2. Verify the value returned for `maxFailedLoginAttempts` is between 1 and 3

Remediation:

Perform the following to implement the prescribed state:

For a managed system:

1. Run the following command in Terminal:

```
sudo pwpolicy -n -setglobalpolicy "maxFailedLoginAttempts=3"
```

For a non-managed system:

1. Run the following command in Terminal:

```
pwpolicy -n /Local/Default -setglobalpolicy "maxFailedLoginAttempts=3"
```

Impact:

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

References:

1. Rule Version (STIG-ID): OSX00050 M

5.19 Create an access warning for the login window (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
```

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
```

5.20 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

5.21 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.

5.22 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.

5.23 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 key chains 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 key chains. Not all keychain-aware applications may provide an interface to choose secondary key chains.

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 credentials.

Audit:

Perform the following to ensure the system is configured as:

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:

1. Run the following command in Terminal:

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

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 *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
```

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 use privilege escalation attacks to take control of the system.

Audit:

Perform the following to ensure the system is configured as:

1. Run the following command in Terminal:

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

2. Make sure the value returned is:

```
AuthenticationAuthority: ;basic;
```

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 dscl . -create /Users/Guest AuthenticationAuthority ";basic;"
sudo dscl . -create /Users/Guest passwd "*"
sudo dscl . -create /Users/Guest UserShell "/sbin/nologin"
```

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:

For AFP sharing:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/com.apple.AppleFileServer \
guestAccess
```

2. Make sure the value returned is 0

For SMB sharing:

1. Run the following command in Terminal:

```
defaults read /Library/Preferences/SystemConfiguration/com.apple.smb.server \
AllowGuestAccess
```

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 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
```

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:

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*

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:

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*

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 10.8 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.

Appendix: Additional Considerations

This section is for guidance on topics the Benchmark does not include a prescribed state and security controls that were previously represented in OSX security guides.

iCloud configuration

Apple's iCloud is a consumer oriented service that allows 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.

Wireless Adapters on Mobile Clients

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.

iSight Camera Privacy and Confidentiality Concerns

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.

Computer Name Considerations

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.

Software Inventory Considerations

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 patch compliance and appropriateness.

A single user desktop whether 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.

Firewall Consideration

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/>

Automatic Actions for Optical Media

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

Appendix: Change History

Date	Version	Changes for this version
2/3/2014	1.0.0	Initial Public Release