UNCLASSIFIED

MAC OSX 10.6 Workstation Security Technical Implementation Guide

Version: 1

Release: 3

26 Apr 2013

XSL Release 6/19/2012 Sort by: Vulid
Description: MAC OSX 10.6 Workstation Security Technical Implementation Guide

---

Group ID (Vulid): V-773
Group Title: GEN000880
Rule ID: SV-37848r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN000880 M6
Rule Title: The root account must be the only account having a UID of “0”.

Vulnerability Discussion: If an account has a UID of “0”, it has root authority. Multiple accounts with a UID of “0” afford more opportunity for potential intruders to guess a password for a privileged account.

Responsibility: System Administrator
IAControls: ECLP-1, IAIA-1, IAIA-2

Check Content:
Enter the following command to view users with a UID of "0":

grep :0 /etc/passwd

If any user other than root has a UID of "0", this is a finding.

Fix Text: Edit the /etc/passwd file and change the UID of the duplicate to an unused UID.

CCI: CCI-000366

Group ID (Vulid): V-784
Group Title: GEN001140
Rule ID: SV-37853r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001140 M6
Rule Title: System files and directories must not have uneven access permissions.

Vulnerability Discussion: Discretionary access control is undermined if users, other than a file owner, have greater access permissions to system files and directories than the owner.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and use the following command to verify the system directories do not have uneven file permissions.

ls -lL /etc /bin /usr/bin /sbin /usr/sbin

If any directories listed contain uneven file permissions, this is a finding.

Fix Text: Use the "chmod" command to set the mode of files with uneven permissions so the owners do not have less permission than group or world users.

CCI: CCI-000225

Group ID (Vulid): V-785
Group Title: GEN001160
Rule ID: SV-38181r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001160 M6
Rule Title: All files and directories must have a valid owner.

Vulnerability Discussion: Non-ownership files and directories may be unintentionally inherited if a user is assigned the same UID as the UID of the non-ownership files.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

find / -nouser

Review the results. If any files do not have a valid owner, this is a finding.

Fix Text: Determine the legitimate owner of the files and use the "chown" command to set the owner and group to the correct value. If the legitimate owner cannot be determined, examine the files to determine their origin and the reason for their lack of an owner/group.

CCI: CCI-000366

Group ID (Vulid): V-786
Group Title: GEN001180
Rule ID: SV-37882r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001180 M6
Rule Title: All network services daemon files must have mode 0755 or less permissive.

Vulnerability Discussion: Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to check the mode of network services daemons (all on one line).

find /usr/sbin -type f -perm +022 -exec stat -f %Lp:%N {} \;

This will return the octal permissions and name of all files that are group or world-writable. If any network services daemon listed is world or group-writable (either or both of the 2 lowest order digits containing a 2, 3, 6, or 7), this is a finding.

Fix Text: Open a terminal session and use the following command to change the mode of the network services daemon.

chmod 755 <path of network services daemon file>

CCI: CCI-000225

Group ID (Vulid): V-787
Group Title: GEN001260
Rule ID: SV-37890r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001260 M6
Rule Title: System log files must have mode 644 or less permissive.

Vulnerability Discussion: If the system log files are not protected, unauthorized users could change the logged data, eliminating its forensic value.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions.

ls -lLR /var/log /var/audit

If any of the log files have modes more permissive than 644, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the mode of the system log file(s).

chmod 644 <path/to/system log file>

CCI: CCI-001314

Group ID (Vulid): V-792
Group Title: GEN001280
Rule ID: SV-37910r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN001280 M6
Rule Title: Manual page files must have mode 0644 or less permissive.

Vulnerability Discussion: If manual pages are compromised, misleading information could be inserted causing actions to possibly compromise the system.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command to verify the permissions on the man files.

ls -lLR /usr/share/man

If the permissions are not set to 0644 or less permissive, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the manual page files to 0644 or less permissive.

chmod 0644 /usr/share/man

CCI: CCI-000225

Group ID (Vulid): V-793
Group Title: GEN001300
Rule ID: SV-37911r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001300 M6
Rule Title: Library files must have mode 0755 or less permissive.

Vulnerability Discussion: Unauthorized access could destroy the integrity of the library files.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
Open a terminal session and enter the following command to verify the permissions on library and framework files, all on one line.
find /System/Library/Frameworks /Library/Frameworks /usr/lib /usr/local/lib -type f -perm +022 -exec stat -f %Lp:%N {} \;

If any of the library files have a mode more permissive than 0755, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the mode of library files to 0755 or less permissive.

chmod 0755 <path/to/library-file>

NOTE: Library files should have an extension of ".a" or ".so", possibly followed by a version number. Frameworks are directories that may already contain files with more restrictive permissions than 755 and thus should not have their modes changed to 755 recursively.

CCI: CCI-001499

Group ID (Vulid): V-794
Group Title: GEN001200
Rule ID: SV-37987r2_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001200 M6
Rule Title: All system command files must have mode 0755 or less permissive.

Vulnerability Discussion: Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.

Severity Override Guidance:
Elevate to Severity Code I if any file listed is world-writable.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify command file permissions.

find /bin /sbin /usr/bin /usr/sbin -type f -perm +022 -exec stat -f %Lp:%N {} \;

This will return the octal permissions and name of all group or world-writable files.

If any file listed is world or group-writable (either or both of the two lowest order digits contain a "2", "3", "6", or "7"), this is a finding.

Fix Text: Open a terminal session and enter the following command to change the mode for system command files to remove group and world write permissions.

chmod go-w <path/filename>

CCI: CCI-001499

Group ID (Vulid): V-795
Group Title: GEN001220
Rule ID: SV-37988r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001220 M6
Rule Title: All system files, programs, and directories must be owned by a system account.

Vulnerability Discussion: Restricting permissions will protect the files from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership of system files, programs, and directories.

Procedure:
ls -lLa/bin /usr/bin /sbin /usr/sbin

If any of the system files, programs, or directories are not owned by a system account, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the owner of system files, programs, and directories to a system account.

chown root <path/filename>

CCI: CCI-001499

Group ID (Vulid): V-796
Group Title: GEN001240
Rule ID: SV-37989r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001240 M6
Rule Title: System files, programs, and directories must be group-owned by a system group.

Vulnerability Discussion: Restricting permissions will protect the files from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and use the following command to verify group ownership of system files, programs, and directories.

ls -lLa /usr/bin

If any system file, program, or directory is not owned by a system group, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the group ownership of system files, programs, and directories to a system group.

chgrp wheel <path/filename>

CCI: CCI-001499

Group ID (Vulid): V-798
Group Title: GEN001380
Rule ID: SV-37990r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001380 M6
Rule Title: The /etc/passwd file must have mode 0644 or less permissive.

Vulnerability Discussion: If the password file is writable by a group owner or the world, the risk of password file compromise is increased. The password file contains the list of accounts on the system and associated information.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions on the password file.

ls -Ll /etc/passwd

If the permissions are not set to 644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the permissions for the password file.

chmod 644 /etc/passwd

CCI: CCI-000225

Group ID (Vulid): V-806
Group Title: GEN002500
Rule ID: SV-37991r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN002500 M6
Rule Title: The sticky bit must be set on all public directories.

Vulnerability Discussion: Failing to set the sticky bit on the public directories allows unauthorized users to delete files in the directory structure.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Enter the following command to search public directories.

find / -type d -perm -002 -exec ls -ld {} \;

Review the results. If any public directories do not have the sticky bit set, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the sticky bit on all public directories.

chmod 1777 <public directory missing the sticky bit>

CCI: CCI-000366

Group ID (Vulid): V-807
Group Title: GEN002520
Rule ID: SV-37993r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002520 M6
Rule Title: All public directories must be owned by root or an application account.

Vulnerability Discussion: If a public directory has the sticky bit set and is not owned by a privileged UID, unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for

temporary file storage (e.g., /tmp) and for directories requiring global read/write access.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership of all public directories.
find / -type d -perm -1002 -exec ls -ld {} \;

If any public directory is not owned by root or an application user, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the owner of public directories to root or an application account.

chown root /tmp

(Replace root with an application user and/or "/tmp" with another public directory as necessary.)

CCI: CCI-000225

Group ID (Vulid): V-812
Group Title: GEN002680
Rule ID: SV-38619r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002680 M6
Rule Title: System audit logs must be owned by root.

Vulnerability Discussion: Failure to give ownership of system audit log files to root provides the designated owner and unauthorized users with the potential to access sensitive information.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Open a terminal session and use the following command to verify the owner of audit logs in the /var/audit directory.

ls -lL /var/audit

If any file in the /var/audit directory is not owned by root, this is a finding.

Fix Text: Open a terminal session and use the following command to change the owner of the file.

chown root /var/audit/<filename>

CCI: CCI-000162

Group ID (Vulid): V-813
Group Title: GEN002700
Rule ID: SV-38622r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002700 M6
Rule Title: System audit logs must have mode 640 or less permissive.

Vulnerability Discussion: If a user can write to the audit logs, audit trails can be modified or destroyed and system

intrusion may not be detected. System audit logs are those files generated from the audit system and do not include activity, error, or other log files created by application software.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Open a terminal session and use the following command to verify the permissions.

ls -lL /var/audit

If any audit log file has a mode more permissive than 640, this is a finding.

Fix Text: Open a terminal session and use the following command to set the permissions of the audit log file.

chmod 640 /var/audit <filename>

CCI: CCI-000163

Group ID (Vulid): V-823
Group Title: GEN003760
Rule ID: SV-37996r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003760 M6
Rule Title: The services file must be owned by root or bin.

Vulnerability Discussion: Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify ownership of the services file.

ls -lL /etc/services

If the services file is not owned by root or bin, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the ownership of the services file.

chown root /etc/services

CCI: CCI-000225

Group ID (Vulid): V-824
Group Title: GEN003780
Rule ID: SV-37997r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003780 M6
Rule Title: The services file must have mode 0644 or less permissive.

Vulnerability Discussion: The services file is critical to the proper operation of network services and must be protected from unauthorized modification. Unauthorized modification could result in the failure of network services.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the mode of the services file.

ls -lL /etc/services

If the services file has a mode more permissive than 0644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the services file.

chmod 0644 /etc/services

CCI: CCI-000225

Group ID (Vulid): V-904
Group Title: GEN001860
Rule ID: SV-38010r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001860 M6
Rule Title: All local initialization files must be owned by the user or root.

Vulnerability Discussion: Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to verify ownership of local initialization files.

ls -al /<usershomedirectory>/.login
ls -al /<usershomedirectory>/.cshrc
ls -al /<usershomedirectory>/.logout
ls -al /<usershomedirectory>/.profile
ls -al /<usershomedirectory>/.bash_profile
ls -al /<usershomedirectory>/.bashrc
ls -al /<usershomedirectory>/.bash_logout
ls -al /<usershomedirectory>/.env
ls -al /<usershomedirectory>/.dtprofile
ls -al /<usershomedirectory>/.dispatch
ls -al /<usershomedirectory>/.emacs
ls -al /<usershomedirectory>/.exrc
find /<usershomedirectory>/.dt ! -fstype nfs ! -user <username> -exec ls -ld {} \;

If local initialization files are not owned by the home directory's user or root, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the ownership of the start-up and login files in the user’s directory to the user or root, as appropriate. Examine each user’s home directory and verify all filenames beginning with "." are owned by the owner of the directory or root. If they are not, use the chown command to change the owner to the user and research the reasons why the owners were not assigned as required.

chown <username> </directory/filename>

CCI: CCI-000225

Group ID (Vulid): V-906
Group Title: GEN001580
Rule ID: SV-38013r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001580 M6
Rule Title: All run control scripts must have mode 0755 or less permissive.

Vulnerability Discussion: If the startup files are writable by other users, they could modify to insert malicious commands into the startup files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to check the mode of launchctl plist files (all on one line).

find /System/Library/LaunchDaemons /System/Library/LaunchAgents /Library/LaunchAgents /Library /LaunchDaemons -type f -perm +022 -exec stat -f %Lp:%N {} \;

This will return the octal permissions and name of all files that are group or world writeable. If any launchctl plist file listed is world or group writeable (either or both of the 2 lowest order digits containing a 2, 3, 6, or 7), this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the run control script file.

chmod 755 <startup file>

CCI: CCI-000225

Group ID (Vulid): V-913
Group Title: GEN002000
Rule ID: SV-38002r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002000 M6
Rule Title: There must be no .netrc files on the system.

Vulnerability Discussion: Unencrypted passwords for remote FTP servers may be stored in .netrc files. Policy requires passwords be encrypted in storage and not used in access scripts.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2, IAIA-1, IAIA-2

Check Content:
Open a terminal session and enter the following command to check the system for the existence of any .netrc files.

find / -name .netrc

If any .netrc file exists, this is a finding.

Fix Text: To remove the .netrc file(s) enter the following command.

rm .netrc

CCI: CCI-000196

Group ID (Vulid): V-914
Group Title: GEN001540
Rule ID: SV-38182r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN001540 M6
Rule Title: All files and directories contained in interactive user home directories must be owned by the home directory's owner.

Vulnerability Discussion: If users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Documentable: YES
Responsibility: Information Assurance Officer
IAControls: ECCD-1, ECCD-2

Check Content:
NOTE: For each user, check for the presence of files and directories within the user's home directory not owned by the home directory owner.

Open a terminal session and enter the following command.

find /<usershomedirectory> -not -user <username> -exec ls -ld {} \;

If the user's home directories contain files or directories not owned by the home directory owner, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the ownership of files and directories in user home directories to the owner of the home directory.

chown <account-owner> <filename>

CCI: CCI-000225

Group ID (Vulid): V-921
Group Title: GEN002200
Rule ID: SV-38014r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002200 M6
Rule Title: All shell files must be owned by root.

Vulnerability Discussion: If shell files are owned by users other than root or bin, they could be modified by intruders or malicious users to perform unauthorized actions.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership of the system shell files.

cat /etc/shells | xargs -n1 ls -lL

If any shell file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to change the ownership of the shell file with incorrect ownership.

chown root <shell>

CCI: CCI-000225

Group ID (Vulid): V-922
Group Title: GEN002220
Rule ID: SV-38015r1_rule
Severity: CAT I
Rule Version (STIG-ID): GEN002220 M6
Rule Title: All shell files must have mode 0755 or less permissive.

Vulnerability Discussion: Shells with world/group write permissions give the ability to maliciously modify the shell to obtain unauthorized access.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command.

cat /etc/shells | xargs -n1 ls -lL

If any shell has a mode more permissive than 0755, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode.

chmod 0755 <shell file>

CCI: CCI-000225

Group ID (Vulid): V-924
Group Title: GEN002280
Rule ID: SV-38017r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002280 M6
Rule Title: Device files and directories must only be writable by users with a system account or as configured by the vendor.

Vulnerability Discussion: System device files in writable directories could be modified, removed, or used by an unprivileged user to control system hardware.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2, ECLP-1

Check Content:
Open a terminal session and enter the following command to verify permissions.

find / -perm -2 -a \(-type b -o -type c \) > devicelist

Check the permissions on the directories above subdirectories in the devicelist file. If any of the device files or their parent directories are world-writable, except device files specifically intended to be world-writable (such as /dev/null), this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the device file.

chmod 755 <device file>

CCI: CCI-000225

Group ID (Vulid): V-936
Group Title: GEN005900
Rule ID: SV-38158r2_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005900 M6
Rule Title: The nosuid option must be enabled on all NFS client mounts.

Vulnerability Discussion: Enabling the nosuid mount option prevents the system from granting owner or group-owner privileges to programs with the suid or sgid bit set. If the system does not restrict this access, users with unprivileged access to the local system may be able to acquire privileged access by executing suid or sgid files located on the mounted NFS file system.

Responsibility: Information Assurance Manager
IAControls: ECPA-1

Check Content:
Open a terminal session and enter the following command to check the system for NFS mounts not using the "nosuid" option.

mount -t nfs | egrep -v "nosuid"

If anything is returned, the mounted file systems do not have the "nosuid" option and this is a finding.

Fix Text: Open a terminal session and edit /etc/auto_master and add the "nosuid" option at the end of the line that begins with /net.

In the same terminal session, edit /etc/fstab and add the "nosuid" option to any lines for NFS mounts.

Remount the NFS file systems to make the change take effect.

CCI: CCI-000225

Group ID (Vulid): V-1027
Group Title: GEN006100
Rule ID: SV-38183r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006100 M6
Rule Title: The /etc/smb.conf file must be owned by root.

Vulnerability Discussion: The /etc/smb.conf file allows access to other machines on the network and grants permissions to certain users. If it is owned by another user, the file may be maliciously modified and the Samba configuration could be compromised.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership of the file.

ls -lL /etc/smb.conf

If an smb.conf file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner of the smb.conf file to root.

chown root /etc/smb.conf

CCI: CCI-000225

Group ID (Vulid): V-1028
Group Title: GEN006140
Rule ID: SV-38184r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006140 M6
Rule Title: The /etc/smb.conf file must have mode 0644 or less permissive.

Vulnerability Discussion: If the smb.conf file has excessive permissions, the file may be maliciously modified and the Samba configuration could be compromised.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions of the /etc/smb.conf file.

ls -lL /etc/smb.conf

If the value is not set to 0644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the smb.conf file.

chmod 644 /etc/smb.conf

CCI: CCI-000225

Group ID (Vulid): V-4084
Group Title: GEN000800
Rule ID: SV-38632r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN000800 M6
Rule Title: The system must prohibit the reuse of passwords to 15 iterations.

Vulnerability Discussion: If a user, or root, used the same password continuously or was allowed to change it back shortly after being forced to change it to something else, it would provide a potential intruder with the opportunity to keep guessing at the user's password until it was guessed correctly.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Open a terminal session and use the following command to view the setting for password history.

sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep usingHistory

If the value of usingHistory is less than 15, this is a finding.

NOTE: If the command returns a response of password server is not configured, the system is not managed. Use the following command for non-managed systems.

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

Fix Text: Open a terminal session and use the following command to set the value for usingHistory.

sudo pwpolicy -n -setglobalpolicy "usingHistory=15"

NOTE: For non-managed system, use the following command.

pwpolicy -n /Local/Default -setglobalpolicy "usingHistory=15"

CCI: CCI-000200

Group ID (Vulid): V-4089
Group Title: GEN001660
Rule ID: SV-37845r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001660 M6
Rule Title: All system start-up files must be owned by root.

Vulnerability Discussion: System start-up files not owned by root could lead to system compromise by allowing malicious users or applications to modify them for unauthorized purposes. This could lead to system and network compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership is set to the original installation settings.

diskutil verifyPermissions /

If files are shown with incorrect ownership, this is a finding.

Fix Text: Open a terminal session and enter the following command to reset the ownership to the original installation settings.

diskutil repairPermissions /

CCI: CCI-000225

Group ID (Vulid): V-4090
Group Title: GEN001680
Rule ID: SV-38018r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001680 M6
Rule Title: All system start-up files must be group-owned by root, sys, bin, other, or system.

Vulnerability Discussion: If system start-up files do not have a group owner of root or a system group, the files may

be modified by malicious users or intruders.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the ownership is set to the original installation settings.

diskutil verifyPermissions /

If files are shown with incorrect ownership, this is a finding.

Fix Text: Open a terminal session and enter the following command to reset the file ownership to their original settings.

diskutil repairPermissions /

CCI: CCI-000225

Group ID (Vulid): V-4364
Group Title: GEN003400
Rule ID: SV-38019r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003400 M6
Rule Title: The "at" directory must have mode 0755 or less permissive.

Vulnerability Discussion: If the "at" directory has a mode more permissive than 0755, unauthorized users could be allowed to view or to edit files containing sensitive information within the "at" directory. Unauthorized modifications could result in Denial of Service to authorized "at" jobs.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the mode of the "at" directory.

ls -ld /var/at

If the directory mode is more permissive than 0755, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the "at" directory to 755.

chmod 755 /var/at

CCI: CCI-000225

Group ID (Vulid): V-4365
Group Title: GEN003420
Rule ID: SV-38021r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003420 M6
Rule Title: The "at" directory must be owned by root, bin, or sys.

Vulnerability Discussion: If the owner of the "at" directory is not root, bin, or sys, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner of the "at" directory.

ls -ld /var/at

If the directory is not owned by root, bin, sys, or system, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner to root.

chown root /var/at

CCI: CCI-000225

Group ID (Vulid): V-4366
Group Title: GEN003440
Rule ID: SV-38022r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003440 M6
Rule Title: "At" jobs must not set the umask to a value less restrictive than 077.

Vulnerability Discussion: The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is often represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be “0”.

Documentable: YES
Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command to determine what "at" jobs exist on the system.

ls /var/at/spool

If no "at" jobs are present, this is not applicable.

To determine if any of the "at" jobs or any scripts referenced execute the "umask" command check for any umask setting more permissive than 077.

grep umask /var/at/spool<at job or referenced script>

If any "at" job or referenced script sets umask to a value more permissive than 077, this is a finding.

Fix Text: Open a terminal session and edit "at" jobs or referenced scripts to remove "umask" commands setting umask to a value less restrictive than 077.

CCI: CCI-000225

Group ID (Vulid): V-4368
Group Title: GEN003480

Rule ID: SV-38024r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003480 M6
Rule Title: The at.deny file must be owned by root, bin, or sys.

Vulnerability Discussion: If the owner of the at.deny file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner.

ls -lL /var/at/at.deny

If the at.deny file is not owned by root, sys, or bin, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner of the at.deny file.

chown root /var/at/at.deny

CCI: CCI-000225

Group ID (Vulid): V-4369
Group Title: GEN003960
Rule ID: SV-38026r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003960 M6
Rule Title: The traceroute command owner must be root.

Vulnerability Discussion: If the traceroute command owner has not been set to root, an unauthorized user could use this command to obtain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information potentially leading to system and network compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner.

ls -lL /usr/sbin/traceroute

If the traceroute command is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner of the traceroute command.

chown root /usr/sbin/traceroute

CCI: CCI-000225

Group ID (Vulid): V-4370
Group Title: GEN003980

Rule ID: SV-38027r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003980 M6
Rule Title: The traceroute command must be group-owned by wheel.

Vulnerability Discussion: If the group owner of the traceroute command has not been set to a system group, unauthorized users could have access to the command and use it to gain information regarding a network's topology inside of the firewall. This information may allow an attacker to determine trusted routers and other network information potentially leading to system and network compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the traceroute command.

ls -lL /usr/sbin/traceroute

If the traceroute command is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group ownership of the traceroute command.

chgrp wheel /usr/sbin/traceroute

CCI: CCI-000225

Group ID (Vulid): V-4371
Group Title: GEN004000
Rule ID: SV-38028r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN004000 M6
Rule Title: The traceroute file must have mode 0700 or less permissive.

Vulnerability Discussion: If the mode of the traceroute executable is more permissive than 0700, malicious code could be inserted by an attacker and triggered whenever the traceroute command is executed by authorized users. Additionally, if an unauthorized user is granted executable permissions to the traceroute command, it could be used to gain information about the network topology behind the firewall. This information may allow an attacker to determine trusted routers and other network information potentially leading to system and network compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions on the traceroute command.

ls -lL /usr/sbin/traceroute

If the traceroute command has a mode more permissive than 0700, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the traceroute command.

chmod 700 /usr/sbin/traceroute

CCI: CCI-000225

Group ID (Vulid): V-4385
Group Title: GEN004580
Rule ID: SV-38005r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN004580 M6
Rule Title: The system must not use .forward files.

Vulnerability Discussion: The .forward file allows users to automatically forward mail to another system. Use of .forward files could allow the unauthorized forwarding of mail and could potentially create mail loops which could degrade system performance.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to search for any .forward files on the system.

find / -name .forward -print

If any .forward files are found on the system, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove .forward files from the system.

rm <path of .forward files>

CCI: CCI-000366

Group ID (Vulid): V-4393
Group Title: GEN005400
Rule ID: SV-38030r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005400 M6
Rule Title: The /etc/syslog.conf file must be owned by root.

Vulnerability Discussion: If the /etc/syslog.conf file is not owned by root, unauthorized users could be allowed to view, edit, or delete important system messages handled by the syslog facility.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner.

ls -lL /etc/syslog.conf

If the syslog.conf file is not owned by root, this is a finding.

Fix Text: Open a terminal session and use the following command to set the owner of the syslog.conf file.

chown root /etc/syslog.conf

CCI: CCI-000225

Group ID (Vulid): V-4394
Group Title: GEN005420
Rule ID: SV-38051r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005420 M6
Rule Title: The /etc/syslog.conf file must be group-owned by wheel.

Vulnerability Discussion: If the group owner of /etc/syslog.conf is not root, bin, or sys, unauthorized users could be permitted to view, edit, or delete important system messages handled by the syslog facility.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the syslog.conf file.

ls -lL /etc/syslog.conf

If the syslog.conf file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group ownership of the syslog.conf file.

chgrp wheel /etc/syslog.conf

CCI: CCI-000225

Group ID (Vulid): V-4687
Group Title: GEN003820
Rule ID: SV-38052r1_rule
Severity: CAT I
Rule Version (STIG-ID): GEN003820 M6
Rule Title: The rsh daemon must not be running.

Vulnerability Discussion: The rshd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.

Responsibility: Information Assurance Officer
IAControls: EBRU-1

Check Content:
Open a terminal session and use the following command to view the rshd status.

defaults read /var/db/launchd.db/com.apple.launchd/overrides com.apple.rshd

If the command does not return a value of 1, this is a finding.

Fix Text: Open a terminal session and use the following command to disable rshd.

launchctl unload -w /System/Library/LaunchDaemons/shell.plist

NOTE: This command is being run to adjust the overrides file; unloading errors are normal, repeat the check to verify.

CCI: CCI-000068

Group ID (Vulid): V-4688
Group Title: GEN003840
Rule ID: SV-38054r1_rule
Severity: CAT I
Rule Version (STIG-ID): GEN003840 M6
Rule Title: The rexec daemon must not be running.

Vulnerability Discussion: The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.

Documentable: YES
Responsibility: Information Assurance Officer
IAControls: EBRP-1, ECSC-1

Check Content:
Open a terminal session and use the following command to view the rexec status.

defaults read /var/db/launchd.db/com.apple.launchd/overrides com.apple.rexecd

If the command does not return a value of 1, this is a finding.

Fix Text: Open a terminal session and use the following command to set the rexec status.

launchctl unload -w /System/Library/LaunchDaemons/exec.plist

NOTE: This command is being run to adjust the overrides file; unloading errors are normal, repeat the check to verify.

CCI: CCI-001435

Group ID (Vulid): V-4696
Group Title: GEN005280
Rule ID: SV-38055r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005280 M6
Rule Title: The system must not have the UUCP service active.

Vulnerability Discussion: The UUCP utility is designed to assist in transferring files, executing remote commands, and sending email between UNIX systems over phone lines and direct connections between systems. The UUCP utility is a primitive and arcane system with many security issues. There are alternate data transfer utilities/products that can be configured to more securely transfer data by providing for authentication, as well as encryption.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to verify uucp is disabled.

defaults read /System/Library/LaunchDaemons/com.apple.uucp Disabled

If a 1 is not returned, this is a finding.

Fix Text: Open a terminal session and use the following command to disable uucp.

launchctl unload -w /System/Library/LaunchDaemons/com.apple.uucp.plist

NOTE: This command is being run to adjust the overrides file; unloading errors are normal, repeat the check to verify.

CCI: CCI-001436

Group ID (Vulid): V-4701
Group Title: GEN003860
Rule ID: SV-38057r2_rule
Severity: CAT III
Rule Version (STIG-ID): GEN003860 M6
Rule Title: The system must not have the finger service active.

Vulnerability Discussion: The finger service provides information about the system's users to network clients. This information could expose information to be used in subsequent attacks.

Responsibility: System Administrator
IAControls: DCPP-1, EBRU-1

Check Content:
Open a terminal session and enter the following command to verify finger is disabled.

defaults read /var/db/launchd.db/com.apple.launchd/overrides com.apple.fingerd

If a value of 1 is not returned, this is a finding.

Fix Text: Open a terminal session and use the following command to disable finger.

launchctl unload -w /System/Library/LaunchDaemons/finger.plist

NOTE: This command is being run to adjust the overrides file; unloading errors are normal, repeat the check to verify.

CCI: CCI-001551

Group ID (Vulid): V-11981
Group Title: GEN001720
Rule ID: SV-38058r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001720 M6
Rule Title: All global initialization files must have mode 0644 or less permissive.

Vulnerability Discussion: Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to verify the permissions on the global initialization files.

ls -l /etc/bashrc
ls -l /etc/csh.cshrc
ls -l /etc/csh.login
ls -l /etc/csh.logout
ls -l /etc/profile

If any global initialization files are more permissive than 0644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode on the global initialization files.

chmod 644 /etc/<filename>

CCI: CCI-000225

Group ID (Vulid): V-11982
Group Title: GEN001740
Rule ID: SV-38060r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001740 M6
Rule Title: All global initialization files must be owned by root.

Vulnerability Discussion: Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to verify the owner of the global initialization files.

ls -l /etc/bashrc
ls -l /etc/csh.cshrc
ls -l /etc/csh.login
ls -l /etc/csh.logout
ls -l /etc/profile

If any global initialization file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner of the global initialization files.

chown root /etc/<filename>

CCI: CCI-000225

Group ID (Vulid): V-11983
Group Title: GEN001760
Rule ID: SV-38061r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001760 M6
Rule Title: All global initialization files must be group-owned by wheel.

Vulnerability Discussion: Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon. Failure to give ownership of sensitive files or utilities to the group wheel provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to verify the group ownership on the global initialization files.

ls -l /etc/bashrc
ls -l /etc/csh.cshrc
ls -l /etc/csh.login
ls -l /etc/csh.logout
ls -l /etc/profile

If any global initialization file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and use the following command to set the group ownership of the global initialization files.

chgrp wheel /etc/<filename>

CCI: CCI-000225

Group ID (Vulid): V-12023
Group Title: GEN005600
Rule ID: SV-38186r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005600 M6
Rule Title: IP forwarding for IPv4 must not be enabled, unless the system is a router.

Vulnerability Discussion: If the system is configured for IP forwarding and is not a designated router, it could be used to bypass network security by providing a path for communication not filtered by network devices.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

sysctl -a | grep net.inet.ip.fw.enable

If the value of "net.inet.ip.fw.enable" is not set to "0", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.ip.fw.enable=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-000366

Group ID (Vulid): V-12024
Group Title: GEN006000
Rule ID: SV-38067r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006000 M6
Rule Title: The system must not have a public Instant Messaging (IM) client installed.

Vulnerability Discussion: Public IM systems are not approved for use and may result in the unauthorized distribution of information. IM clients provide a way for a user to send a message to one or more users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL

Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger.

IM clients present a security issue when the clients route messages through public servers. The obvious implication is for potentially sensitive information to be intercepted or altered in the course of transmission. This same issue is associated with the use of public email servers. In order to reduce the potential for disclosure of sensitive Government information and to ensure the validity of official Government information, IM clients connecting to public IM services will not be installed. Clients used to access internal or DoD-controlled IM services are permitted.

Responsibility: System Administrator
IAControls: ECIM-1

Check Content:
If an IM client is installed, ask the SA if it has access to any public domain IM servers. If it does have access to public servers, this is a finding.

Fix Text: Uninstall the IM client from the system, or configure the client to only connect to DoD-approved IM services.

CCI: CCI-000366

CCI: CCI-001154

Group ID (Vulid): V-12025
Group Title: GEN006040
Rule ID: SV-38068r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006040 M6
Rule Title: The system must not have any peer-to-peer file-sharing application installed.

Vulnerability Discussion: Peer-to-peer file-sharing software can result in the unintentional exfiltration of information. There are also many legal issues associated with these types of utilities including copyright infringement or other intellectual property issues. The ASD Memo "Use of Peer-to-Peer (P2P) File-Sharing Applications across the DoD" states the following:

“P2P file-sharing applications are authorized for use on DOD networks with approval by the appropriate Designated Approval Authority (DAA). Documented requirements, security architecture, configuration management process, and a training program for users are all requirements within the approval process. The unauthorized use of application or services, including P2P applications, is prohibited, and such applications or services must be eliminated.”

Peer-to-peer applications include, but are not limited to:

-Napster,
-Kazaa,
-ARES,
-Limewire,
-IRC Chat Relay, and
-BitTorrent.

Responsibility: System Administrator
IAControls: DCPD-1, ECSC-1

Check Content:
Ask the SA if any peer-to-peer file-sharing applications are installed. Some examples of these applications include.

- Napster,
- Kazaa,
- ARES,
- Limewire,

- IRC Chat Relay, and
- BitTorrent.

If any of these applications are installed, this is a finding.

Fix Text: Uninstall the peer-to-peer file sharing application(s) from the system.

CCI: CCI-001436

Group ID (Vulid): V-22312
Group Title: GEN001170
Rule ID: SV-38187r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001170 M6
Rule Title: All files and directories must have a valid group owner.

Vulnerability Discussion: Files without a valid group owner may be unintentionally inherited if a group is assigned the same GID as the GID of the files without a valid group owner.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to search the system for files without a valid group owner.

find / -nogroup -print

If any files are found, this is a finding.

Fix Text: Use the following command to change the group owner for each file without a valid group owner.

chgrp <a-valid-group> <path>/<file-without-a-valid-group-owner>

CCI: CCI-000366

Group ID (Vulid): V-22313
Group Title: GEN001190
Rule ID: SV-38070r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001190 M6
Rule Title: All network services daemon files must not have extended ACLs.

Vulnerability Discussion: Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the network services daemon ACLs.

ls -la /usr/sbin

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /usr/sbin/ <file with extended ACL>

CCI: CCI-000225

Group ID (Vulid): V-22314
Group Title: GEN001210
Rule ID: SV-38072r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001210 M6
Rule Title: System command files must not have extended ACLs.

Vulnerability Discussion: Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view extended ACLs.

find /bin /sbin /usr/bin /usr/sbin -print -exec ls -lLd \{\} \; | egrep '^..........+'

If any command files are shown with permissions that include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N <path/file with extended ACL>

CCI: CCI-001499

Group ID (Vulid): V-22315
Group Title: GEN001270
Rule ID: SV-38073r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001270 M6
Rule Title: System log files must not have extended ACLs, except as needed to support authorized software.

Vulnerability Discussion: If the system log files are not protected, unauthorized users could change the logged data, eliminating its forensic value. Authorized software may be given log file access through the use of extended ACLs when needed and configured to provide the least privileges required.

Documentable: YES
Responsibility: System Administrator
IAControls: ECLP-1, ECTP-1

Check Content:
Open a terminal session and enter the following command to view the system log files ACLs.

ls -lLR /var/log

If the permissions include a '+', the file has an extended ACL. If an extended ACL exists, verify with the SA if the ACL is required to support authorized software and provides the minimum necessary permissions. If an extended ACL exists, providing access beyond the needs of authorized software, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /var/log<file with extended ACL>

CCI: CCI-001314

Group ID (Vulid): V-22316
Group Title: GEN001290
Rule ID: SV-38074r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN001290 M6
Rule Title: All manual page files must not have extended ACLs.

Vulnerability Discussion: If manual pages are compromised, misleading information could be inserted causing actions to possibly compromise the system.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the man page ACLs.

ls -lLR /usr/share/man

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -RN /usr/share/man

CCI: CCI-000225

Group ID (Vulid): V-22317
Group Title: GEN001310
Rule ID: SV-38075r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001310 M6
Rule Title: All library files must not have extended ACLs.

Vulnerability Discussion: Unauthorized access could destroy the integrity of the library files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the library file ACLs.

ls -lLR /System/Library/Frameworks /Library/Frameworks /usr/lib /usr/local/lib

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -RN /System/Library/Frameworks /Library/Frameworks /usr/lib /usr/local/lib

CCI: CCI-001499

Group ID (Vulid): V-22319
Group Title: GEN001362
Rule ID: SV-38077r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001362 M6
Rule Title: The /etc/resolv.conf file must be owned by root.

Vulnerability Discussion: The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner of the resolv.conf file.

ls -lL /etc/resolv.conf

If the resolv.conf file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner of the resolv.conf file.

chown root /etc/resolv.conf

CCI: CCI-000225

Group ID (Vulid): V-22320
Group Title: GEN001363
Rule ID: SV-38078r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001363 M6
Rule Title: The /etc/resolv.conf file must be group-owned by wheel.

Vulnerability Discussion: The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the resolv.conf file.

ls -lL /etc/resolv.conf

If the resolv.conf file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group ownership of the resolv.conf file.

chgrp wheel /etc/resolv.conf

CCI: CCI-000225

Group ID (Vulid): V-22321
Group Title: GEN001364
Rule ID: SV-38079r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001364 M6
Rule Title: The /etc/resolv.conf file must have mode 0644 or less permissive.

Vulnerability Discussion: The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions on the file.

ls -Ll /etc/resolv.conf

If the permissions are not set to 644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set permissions on the file.

chmod 644 /etc/resolv.conf

CCI: CCI-000225

Group ID (Vulid): V-22322
Group Title: GEN001365
Rule ID: SV-38081r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001365 M6
Rule Title: The /etc/resolv.conf file must not have an extended ACL.

Vulnerability Discussion: The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the resolv.conf file extended ACLs.

ls -lL /etc/resolv.conf

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/resolv.conf

CCI: CCI-000225

Group ID (Vulid): V-22323
Group Title: GEN001366
Rule ID: SV-38082r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001366 M6
Rule Title: The /etc/hosts file must be owned by root.

Vulnerability Discussion: The /etc/hosts file (or equivalent) configures local host name to IP address mappings typically taking precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner of the etc/hosts file.

ls -lL /etc/hosts

If the /etc/hosts file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner to root.

chown root /etc/hosts

CCI: CCI-000225

Group ID (Vulid): V-22324
Group Title: GEN001367
Rule ID: SV-38083r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001367 M6
Rule Title: The /etc/hosts file must be group-owned by wheel.

Vulnerability Discussion: The /etc/hosts file (or equivalent) configures local host name to IP address mappings typically taking precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the etc/hosts file.

ls -lL /etc/hosts

If the /etc/hosts file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group to root.

chgrp wheel /etc/hosts

CCI: CCI-000225

Group ID (Vulid): V-22325
Group Title: GEN001368
Rule ID: SV-38085r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001368 M6
Rule Title: The /etc/hosts file must have mode 0644 or less permissive.

Vulnerability Discussion: The /etc/hosts file (or equivalent) configures local host name to IP address mappings typically taking precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions of the etc/hosts file.

ls -lL /etc/hosts

If the /etc/hosts file permissions are not set to 644, this is a finding.

Fix Text: Open a terminal session and use the following command to set the mode of the etc/hosts file.

chmod 644 /etc/hosts

CCI: CCI-000225

Group ID (Vulid): V-22326
Group Title: GEN001369
Rule ID: SV-38086r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001369 M6
Rule Title: The /etc/hosts file must not have an extended ACL.

Vulnerability Discussion: The /etc/hosts file (or equivalent) configures local host name to IP address mappings typically taking precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, such as time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/hosts file extended ACLs.

ls -lL /etc/hosts

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/hosts

CCI: CCI-000225

Group ID (Vulid): V-22331
Group Title: GEN001375
Rule ID: SV-38766r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN001375 M6
Rule Title: For systems using DNS resolution, at least two name servers must be configured.

Vulnerability Discussion: To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and use the following command to verify the DNS name servers.

grep nameserver /etc/resolv.conf

If less than two lines are returned that are not commented out, this is a finding.

Fix Text: Open a terminal session and use the following command to edit the /etc/resolv.conf and add additional "nameserver" lines until at least two are present.

sudo pico /etc/resolv.conf

CCI: CCI-001182

Group ID (Vulid): V-22332
Group Title: GEN001378
Rule ID: SV-38087r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001378 M6
Rule Title: The /etc/passwd file must be owned by root.

Vulnerability Discussion: The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner of the etc/passwd file.

ls -lL /etc/passwd

If the /etc/passwd file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner to root.

chown root /etc/passwd

CCI: CCI-000225

Group ID (Vulid): V-22333
Group Title: GEN001379
Rule ID: SV-38088r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001379 M6
Rule Title: The /etc/passwd file must be group-owned by wheel.

Vulnerability Discussion: The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the etc/passwd file.

ls -lL /etc/passwd

If the /etc/passwd file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group to wheel.

chgrp wheel /etc/passwd

CCI: CCI-000225

Group ID (Vulid): V-22334
Group Title: GEN001390
Rule ID: SV-38089r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001390 M6
Rule Title: The /etc/passwd file must not have an extended ACL.

Vulnerability Discussion: File system ACLs can provide access to files beyond what is allowed by the mode numbers of the files. The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/passwd file extended ACLs.

ls -lL /etc/passwd

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/passwd

CCI: CCI-000225

Group ID (Vulid): V-22335
Group Title: GEN001391
Rule ID: SV-38090r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001391 M6
Rule Title: The /etc/group file must be owned by root.

Vulnerability Discussion: The /etc/group file is critical to system security and must be owned by a privileged user. The group file contains a list of system groups and associated information.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner of the /etc/group file.

ls -lL /etc/group

If the /etc/group file is not owned by root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner to root.

chown root /etc/group

CCI: CCI-000225

Group ID (Vulid): V-22336
Group Title: GEN001392
Rule ID: SV-38091r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001392 M6
Rule Title: The /etc/group file must be group-owned by wheel.

Vulnerability Discussion: The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the /etc/group file.

ls -lL /etc/group

If the /etc/group file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group to wheel.

chgrp wheel /etc/group

CCI: CCI-000225

Group ID (Vulid): V-22337
Group Title: GEN001393
Rule ID: SV-38092r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001393 M6
Rule Title: The /etc/group file must have mode 0644 or less permissive.

Vulnerability Discussion: The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the permissions of the /etc/group file.

ls -lL /etc/group

If the /etc/group file permissions are not set to 644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the mode of the /etc/group file.

chmod 644 /etc/group

CCI: CCI-000225

Group ID (Vulid): V-22338
Group Title: GEN001394
Rule ID: SV-38093r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001394 M6
Rule Title: The /etc/group file must not have an extended ACL.

Vulnerability Discussion: The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/group file extended ACLs.

ls -lL /etc/group

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/group

CCI: CCI-000225

Group ID (Vulid): V-22350
Group Title: GEN001490
Rule ID: SV-38094r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN001490 M6
Rule Title: User home directories must not have extended ACLs.

Vulnerability Discussion: Excessive permissions on home directories allow unauthorized access to user files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command.

ls -lLd <top level user home directory>

If the permissions include a '+', the directory has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the permissions.

chmod -N <user home directory with extended ACL>

CCI: CCI-000225

Group ID (Vulid): V-22351
Group Title: GEN001550
Rule ID: SV-38215r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001550 M6
Rule Title: All files and directories contained in user home directories must be group-owned by a group where the home directory's owner is a member.

Vulnerability Discussion: If a user's files are group-owned by a group where the user is not a member, unintended users may be able to access them.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to view the group ownership of the user’s directories and files.

ls -l /Users (shows users directory)

ls -lL /Users/ <each user directory>

If any directory or file is not group owned by the user or a know users group, this is a finding.

Fix Text: chgrp <group with user as member> <file with bad group ownership>

CCI: CCI-000225

Group ID (Vulid): V-22352
Group Title: GEN001570
Rule ID: SV-38095r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001570 M6
Rule Title: All files and directories contained in user home directories must not have extended ACLs.

Vulnerability Discussion: Excessive permissions allow unauthorized access to user files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command.

find /Users -print -exec ls -lLd \{\} \; | grep '^..........+'

If files are shown with permissions that include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N <user file with extended ACL>

CCI: CCI-000225

Group ID (Vulid): V-22353
Group Title: GEN001590
Rule ID: SV-38096r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN001590 M6
Rule Title: Launch control scripts must not have extended ACLs.

Vulnerability Discussion: If the launch control scripts are writable by other users, they could modify to insert malicious commands into the startup files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the launch control scripts have no extended ACLs.

ls -lL /System/Library/LaunchDaemons /System/Library/LaunchAgents /Library/LaunchDaemons /Library /LaunchAgents

If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N <launch control script with extended ACL>

CCI: CCI-000225

Group ID (Vulid): V-22366
Group Title: GEN002230
Rule ID: SV-38098r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002230 M6
Rule Title: All shell files must not have extended ACLs.

Vulnerability Discussion: Shells with world/group-write permissions give the ability to maliciously modify the shell to obtain unauthorized access.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view extended ACLs.

cat /etc/shells | xargs -n1 ls -lL

If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.

Fix Text: Open a terminal session and use the following command to remove the extended ACLs.

chmod -N <shell file with extended ACL>

CCI: CCI-000225

Group ID (Vulid): V-22369
Group Title: GEN002710
Rule ID: SV-38102r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002710 M6
Rule Title: All system audit files must not have extended ACLs.

Vulnerability Discussion: If a user can write to the audit logs, then audit trails can be modified or destroyed and system intrusion may not be detected.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Open a terminal session and enter the following command to view the ACLs of the audit files.

ls -Ll /var/audit

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N </var/audit/ file with extended ACL>

CCI: CCI-000163

Group ID (Vulid): V-22373
Group Title: GEN002718
Rule ID: SV-38103r1_rule

Severity: CAT III
Rule Version (STIG-ID): GEN002718 M6
Rule Title: System audit tool executables must not have extended ACLs.

Vulnerability Discussion: To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the ACLs of the audit tool.

ls -lL /usr/sbin/audit /usr/sbin/auditd /usr/sbin/auditreduce /usr/sbin/praudit

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and use the following command to remove the extended ACLs.

chmod -N <audit file with extended ACL>

CCI: CCI-001493

Group ID (Vulid): V-22384
Group Title: GEN002990
Rule ID: SV-38105r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002990 M6
Rule Title: The cron.allow file must not have an extended ACL.

Vulnerability Discussion: A cron.allow file that is readable and/or writable by other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the ACLs of the cron.allow file.

ls -l /private/var/at/cron.allow

If the file exists and the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /private/var/at/cron.allow

CCI: CCI-000225

Group ID (Vulid): V-22385
Group Title: GEN003050
Rule ID: SV-38107r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003050 M6
Rule Title: Crontab files must be group-owned by wheel, cron, or the crontab creator's primary group.

Vulnerability Discussion: To protect the integrity of scheduled system jobs and prevent malicious modification to these jobs, crontab files must be secured.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to verify the group ownership of the "crontab" files.

ls -lL /usr/sbin/cron
ls -lL /usr/lib/cron
ls -lL /usr/bin/crontab
ls -lL /private/var/at/cron.deny

If the group-owner is not wheel or the crontab owner's primary group, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group to wheel.

chgrp wheel <crontab file>

CCI: CCI-000225

Group ID (Vulid): V-22386
Group Title: GEN003090
Rule ID: SV-38110r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003090 M6
Rule Title: Crontab files must not have extended ACLs.

Vulnerability Discussion: To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. ACLs on crontab files may provide unauthorized access to the files.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to view the extended ACLs of the crontab file.

ls -lL /usr/sbin/cron
ls -lL /usr/lib/cron
ls -lL /usr/bin/crontab
ls -lL /private/var/at/cron.deny

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N <crontab file>

CCI: CCI-000225

Group ID (Vulid): V-22387
Group Title: GEN003110
Rule ID: SV-38112r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003110 M6

Rule Title: Cron and crontab directories must not have extended ACLs.

Vulnerability Discussion: To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. ACLs on cron and crontab directories may provide unauthorized access to these directories. Unauthorized modifications to these directories or their contents may result in the addition of unauthorized cron jobs or deny service to authorized cron jobs.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following commands to view the extended ACLs of the crontab directory.

ls -ld /usr/sbin/cron
ls -ld /usr/lib/cron
ls -ld /usr/bin/crontab
ls -ld /private/var/at/cron.deny

If the permissions include a '+', the directory has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N <crontab directory>

CCI: CCI-000225

Group ID (Vulid): V-22389
Group Title: GEN003210
Rule ID: SV-38115r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003210 M6
Rule Title: The cron.deny file must not have an extended ACL.

Vulnerability Discussion: If there are excessive file permissions for the cron.deny file, sensitive information could be viewed or edited by unauthorized users.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the ACLs of the cron.deny file.

ls -l /private/var/at/cron.deny

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /private/var/at/cron.deny

CCI: CCI-000225

Group ID (Vulid): V-22391
Group Title: GEN003250

Rule ID: SV-38117r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003250 M6
Rule Title: The cron.allow file must be group-owned by wheel.

Vulnerability Discussion: If the group of the cron.allow is not set to wheel, the possibility exists for an unauthorized user to view or edit the list of users permitted to use cron. Unauthorized modification of this file could cause Denial of Service to authorized cron users or provide unauthorized users with the ability to run cron jobs.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the cron.allow file.

ls -lL /private/var/at/cron.allow

If the file exists and is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chgrp wheel /private/var/at/cron.allow

CCI: CCI-000225

Group ID (Vulid): V-22394
Group Title: GEN003270
Rule ID: SV-38119r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003270 M6
Rule Title: The cron.deny file must be group-owned by wheel.

Vulnerability Discussion: The cron daemon control files and restricts the scheduling of automated tasks and must be protected. Unauthorized modification of the cron.deny file could result in Denial of Service to authorized cron users or could provide unauthorized users with the ability to run cron jobs.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the "/private/var/at /cron.deny" file.

ls -lL /private/var/at/cron.deny

If the "/private/var/at/cron.deny" file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group.

chgrp wheel /private/var/at/cron.deny

CCI: CCI-000225

Group ID (Vulid): V-22404

Group Title: GEN003510
Rule ID: SV-38198r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003510 M6
Rule Title: Kernel core dumps must be disabled unless needed.

Vulnerability Discussion: Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in Denial of Service by exhausting the available space on the target file system. The kernel core dump process may increase the amount of time a system is unavailable due to a crash. Kernel core dumps can be useful for kernel debugging.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and use the following command to verify the system does not allow core dumps.

sysctl -a | grep kern.coredump

If kern.coredump is not set to 0, this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following entry.

kern.coredump=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-000366

Group ID (Vulid): V-22409
Group Title: GEN003602
Rule ID: SV-38200r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN003602 M6
Rule Title: The system must not process Internet Control Message Protocol (ICMP) timestamp requests.

Vulnerability Discussion: The processing of ICMP timestamp requests increases the attack surface of the system.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the timestamp.

sysctl -a | grep net.inet.icmp.timestamp

If the value of net.inet.icmp.timestamp is not set to "1", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.icmp.timestamp=1

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001551

Group ID (Vulid): V-22410
Group Title: GEN003603
Rule ID: SV-38201r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003603 M6
Rule Title: The system must not respond to Internet Control Message Protocol (ICMPv4) echoes sent to a broadcast address.

Vulnerability Discussion: Responding to broadcast ICMP echoes facilitates network mapping and provides a vector for amplification attacks.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the value of "net.inet.icmp.bmcastecho".

sysctl -a | grep net.inet.icmp.bmcastecho

If the value is not set to "1", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.icmp.bmcastecho=1

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001551

Group ID (Vulid): V-22413
Group Title: GEN003606
Rule ID: SV-38202r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003606 M6
Rule Title: The system must prevent local applications from generating source-routed packets.

Vulnerability Discussion: Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the value of "net.inet.ip.sourceroute".

sysctl -a | grep net.inet.ip.sourceroute

If the value of "net.inet.ip.sourceroute" is not set to "0", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.ip.sourceroute=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001551

Group ID (Vulid): V-22414
Group Title: GEN003607
Rule ID: SV-38203r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003607 M6
Rule Title: The system must not accept source-routed IPv4 packets.

Vulnerability Discussion: Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the handling of source-routed traffic destined to the system itself, not to traffic forwarded by the system to another, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the value of "net.inet.ip.accept_sourceroute".

sysctl -a | grep net.inet.ip.accept_sourceroute

If the value of "net.inet.ip.accept_sourceroute" is not set to "0", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.ip.accept_sourceroute=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001551

Group ID (Vulid): V-22416
Group Title: GEN003609
Rule ID: SV-38204r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003609 M6
Rule Title: The system must ignore IPv4 ICMP redirect messages.

Vulnerability Discussion: ICMP redirect messages are used by routers to inform hosts of a more direct route existing for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the value of "net.inet.icmp.drop_redirect".

sysctl -a | grep net.inet.icmp.drop_redirect

If the value of "net.inet.icmp.drop_redirect" is not set to "0", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.icmp.drop_redirect=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001503

CCI: CCI-001551

Group ID (Vulid): V-22417
Group Title: GEN003610
Rule ID: SV-38205r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003610 M6
Rule Title: The system must not send IPv4 ICMP redirects.

Vulnerability Discussion: ICMP redirect messages are used by routers to inform hosts of a more direct route existing for a particular destination. These messages contain information from the system's route table possibly revealing portions of the network topology.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command to view the value of "net.inet.ip.redirect".

sysctl -a | grep net.inet.ip.redirect

If the value of "net.inet.ip.redirect" is not set to "0", this is a finding.

Fix Text: Open a terminal session and edit the /etc/sysctl.conf file and add the following line.

net.inet.ip.redirect=0

NOTE: If the sysctl.conf file does not exist use the following command to create one.
touch /etc/sysctl.conf

CCI: CCI-001551

Group ID (Vulid): V-22427
Group Title: GEN003770
Rule ID: SV-38122r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003770 M6
Rule Title: The services file must be group-owned by wheel.

Vulnerability Discussion: Failure to give ownership of system configuration files to a system group provides the designated owner and unauthorized users with the potential to change the system configuration which could weaken

the system's security posture.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group ownership of the /etc/services file.

ls -lL /etc/services

If the /etc/services file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group.

chgrp wheel /etc/services

CCI: CCI-000225

Group ID (Vulid): V-22428
Group Title: GEN003790
Rule ID: SV-38124r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN003790 M6
Rule Title: The services file must not have an extended ACL.

Vulnerability Discussion: The services file is critical to the proper operation of network services and must be protected from unauthorized modification. If the services file has an extended ACL, it may be possible for unauthorized users to modify the file. Unauthorized modification could result in the failure of network services.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/services file extended ACLs.

ls -lL /etc/services

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/services

CCI: CCI-000225

Group ID (Vulid): V-22437
Group Title: GEN004010
Rule ID: SV-38127r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN004010 M6
Rule Title: The traceroute file must not have an extended ACL.

Vulnerability Discussion: If an extended ACL exists on the traceroute executable file, it may provide unauthorized users with access to the file. Malicious code could be inserted by an attacker and triggered whenever the traceroute

command is executed by authorized users. Additionally, if an unauthorized user is granted executable permissions to the traceroute command, it could be used to gain information about the network topology behind the firewall. This information may allow an attacker to determine trusted routers and other network information potentially leading to system and network compromise.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the "/usr/sbin/traceroute" file extended ACLs.

ls -lL /usr/sbin/traceroute

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /usr/sbin/traceroute

CCI: CCI-000225

Group ID (Vulid): V-22438
Group Title: GEN004370
Rule ID: SV-38128r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN004370 M6
Rule Title: The aliases file must be group-owned by wheel.

Vulnerability Discussion: If the alias file is not group-owned by a system group, an unauthorized user may modify the file to add aliases to run malicious code or redirect email.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and use the following command to verify the group ownership of the /etc/aliases file.

ls -lL /etc/aliases

If the /etc/aliases file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the group.

chgrp wheel /etc/aliases

CCI: CCI-000225

Group ID (Vulid): V-22439
Group Title: GEN004390
Rule ID: SV-38131r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN004390 M6
Rule Title: The alias file must not have an extended ACL.

Vulnerability Discussion: Excessive permissions on the aliases file may permit unauthorized modification. If the alias file is modified by an unauthorized user, they may modify the file to run malicious code or redirect email.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/aliases file extended ACLs.

ls -lL /etc/aliases

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/aliases

CCI: CCI-000225

Group ID (Vulid): V-22454
Group Title: GEN005395
Rule ID: SV-38133r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005395 M6
Rule Title: The /etc/syslog.conf file must not have an extended ACL.

Vulnerability Discussion: Unauthorized users must not be allowed to access or modify the /etc/syslog.conf file.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/syslog.conf file extended ACLs.

ls -lL /etc/syslog.conf

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/syslog.conf

CCI: CCI-000225

Group ID (Vulid): V-22458
Group Title: GEN005505
Rule ID: SV-39360r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005505 M6
Rule Title: The SSH daemon must be configured to only use FIPS 140-2 approved ciphers.

Vulnerability Discussion: DoD information systems are required to use FIPS 140-2 approved ciphers. SSHv2 ciphers meeting this requirement are 3DES and AES.

Responsibility: System Administrator
IAControls: DCNR-1

Check Content:
Open a terminal session and enter the following command.

grep -i ciphers /etc/sshd_config | grep -v '^#'

If no lines are returned, or the returned ciphers list contains any cipher not starting with "3DES" or "AES", this is a finding.

Fix Text: Open a terminal session and edit the SSH daemon configuration file "/etc/sshd_config" to remove any ciphers not starting with "3DES" or "AES".

CCI: CCI-000068

Group ID (Vulid): V-22459
Group Title: GEN005506
Rule ID: SV-39364r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005506 M6
Rule Title: The SSH daemon must be configured to not use CBC ciphers.

Vulnerability Discussion: The Cipher-Block Chaining (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen plaintext attacks and must not be used.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

grep ciphers /etc/sshd_config

If no lines are returned, or the returned ciphers list contains any cipher ending with CBC, this is a finding.

Fix Text: Open a terminal session and edit the SSH daemon configuration file "/etc/sshd_config" and remove any ciphers ending with "CBC". If necessary, add a Ciphers line.

CCI: CCI-000366

Group ID (Vulid): V-22460
Group Title: GEN005507
Rule ID: SV-39369r2_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005507 M6
Rule Title: The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Vulnerability Discussion: DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions.

Responsibility: System Administrator
IAControls: DCNR-1

Check Content:
Open a terminal session and enter the following command.

grep -i macs /etc/sshd_config | grep -v '^#'

If no lines are returned, or the returned MACs list contains any MAC other than "hmac-sha1", this is a finding.

Fix Text: Open a terminal session and edit the SSH daemon configuration file "/etc/sshd_config" and remove any MACs other than "hmac-sha1". If there is no MACs line in "/etc/sshd_config", add "MACs hmac-sha1" to the file.

Restart the SSH daemon for the changes to take effect.

CCI: CCI-001453

Group ID (Vulid): V-22461
Group Title: GEN005510
Rule ID: SV-39371r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005510 M6
Rule Title: The SSH client must be configured to only use FIPS 140-2 approved ciphers.

Vulnerability Discussion: DoD information systems are required to use FIPS 140-2 approved ciphers. SSHv2 ciphers meeting this requirement are 3DES and AES.

Responsibility: System Administrator
IAControls: DCNR-1

Check Content:
Open a terminal session and enter the following command.

grep -i ciphers /etc/ssh_config | grep -v '^#'

If no lines are returned, or the returned ciphers list contains any cipher not starting with "3DES" or "AES", this is a finding.

Fix Text: Open a terminal session and edit the SSH client configuration file "/etc/ssh_config" and remove any ciphers not starting with "3DES" or "AES".

CCI: CCI-000068

Group ID (Vulid): V-22462
Group Title: GEN005511
Rule ID: SV-39374r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005511 M6
Rule Title: The SSH client must be configured to not use CBC-based ciphers.

Vulnerability Discussion: The Cipher-Block Chaining (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen plaintext attacks and must not be used.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Open a terminal session and enter the following command.

grep -i ciphers /etc/ssh_config | grep -v '^#'

If no lines are returned, or the returned ciphers list contains any cipher ending with "CBC", this is a finding.

Fix Text: Open a terminal session and edit the SSH client configuration file "/etc/ssh_config" and remove any ciphers ending with "CBC".

CCI: CCI-000366

Group ID (Vulid): V-22463
Group Title: GEN005512
Rule ID: SV-39376r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN005512 M6
Rule Title: The SSH client must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Vulnerability Discussion: DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions.

Responsibility: System Administrator
IAControls: DCNR-1

Check Content:
Open a terminal session and enter the following command.

grep -i macs /etc/ssh_config | grep -v '^#'

If no lines are returned, or the returned MACs list contains any MAC other than "hmac-sha1", this is a finding.

Fix Text: Open a terminal session and edit the SSH client configuration file "/etc/ssh_config" and remove any MACs other than "hmac-sha1".

CCI: CCI-001453

Group ID (Vulid): V-22497
Group Title: GEN006150
Rule ID: SV-38135r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006150 M6
Rule Title: The /etc/smb.conf file must not have an extended ACL.

Vulnerability Discussion: Excessive permissions could endanger the security of the Samba configuration file and, ultimately, the system and network.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to view the /etc/smb.conf file extended ACLs.

ls -lL /etc/smb.conf

If the permissions include a '+', the file has an extended ACL, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the extended ACLs.

chmod -N /etc/smb.conf

CCI: CCI-000225

Group ID (Vulid): V-22506
Group Title: GEN006565
Rule ID: SV-38138r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN006565 M6
Rule Title: The system package management tool must be used to verify system software periodically.

Vulnerability Discussion: Verification using the system package management tool can be used to determine that system software has not been tampered with.

This requirement is not applicable to systems not using package management tools.

Responsibility: System Administrator
IAControls: ECAT-1

Check Content:
Open a terminal session and enter the following command to verify the permissions are set to the original installation settings.

diskutil verifyPermissions /

Fix Text: Open a terminal session and enter the following command to reset the permissions to the original installation settings.
diskutil repairPermissions /

CCI: CCI-000366

CCI: CCI-000698

Group ID (Vulid): V-22507
Group Title: GEN006570
Rule ID: SV-38139r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN006570 M6
Rule Title: The file integrity tool must be configured to verify ACLs.

Vulnerability Discussion: ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Responsibility: System Administrator
IAControls: ECAT-1

Check Content:
Open a terminal session and enter the following command to verify the permissions are set to the original installation

settings.

diskutil verifyPermissions /

If files are shown with incorrect permissions, this is a finding.

Fix Text: Open a terminal session and enter the following command to reset the permissions to the original installation settings.

diskutil repairPermissions /

CCI: CCI-001297

Group ID (Vulid): V-22508
Group Title: GEN006571
Rule ID: SV-38141r1_rule
Severity: CAT III
Rule Version (STIG-ID): GEN006571 M6
Rule Title: The file integrity tool must be configured to verify extended attributes.

Vulnerability Discussion: Extended attributes in file systems are used to contain arbitrary data and file metadata potentially having security implications.

Responsibility: System Administrator
IAControls: ECAT-1

Check Content:
Open a terminal session and enter the following command to verify the permissions are set to the original installation settings.

diskutil verifyPermissions /

If files are shown with incorrect extended attributes, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove extended attributes.

diskutil repairPermissions /

CCI: CCI-001297

Group ID (Vulid): V-22559
Group Title: GEN008060
Rule ID: SV-38142r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN008060 M6
Rule Title: If the system is using LDAP for authentication or account information the /etc/openldap/ldap.conf (or equivalent) file must have mode 0644 or less permissive.

Vulnerability Discussion: LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:

Open a terminal session and enter the following command to verify the permissions.

ls -Ll /etc/openldap/ldap.conf

If the permissions are not set to 644, this is a finding.

Fix Text: Open a terminal session and enter the following command to set permissions on the file.

chmod 644 /etc/openldap/ldap.conf

CCI: CCI-000225

Group ID (Vulid): V-22560
Group Title: GEN008080
Rule ID: SV-38155r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN008080 M6
Rule Title: If the system is using LDAP for authentication or account information, the /etc/openldap/ldap.conf (or equivalent) file must be owned by root.

Vulnerability Discussion: LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the owner.

ls -Ll /etc/openldap/ldap.conf

If the owner is not set to root, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the owner to root.

chown root /etc/openldap/ldap.conf

CCI: CCI-000225

Group ID (Vulid): V-22561
Group Title: GEN008100
Rule ID: SV-38156r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN008100 M6
Rule Title: If the system is using LDAP for authentication or account information, the /etc/openldap/ldap.conf (or equivalent) file must be group-owned by wheel.

Vulnerability Discussion: LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the group owner.

ls -Ll /etc/openldap/ldap.conf

If the file is not group-owned by wheel, this is a finding.

Fix Text: Open a terminal session and use the following command to set the group owner of the file.

chgrp wheel /etc/openldap/ldap.conf

CCI: CCI-000225

Group ID (Vulid): V-22562
Group Title: GEN008120
Rule ID: SV-38157r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN008120 M6
Rule Title: If the system is using LDAP for authentication or account information, the /etc/openldap/ldap.conf (or equivalent) file must not have an extended ACL.

Vulnerability Discussion: LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.

Responsibility: System Administrator
IAControls: ECLP-1

Check Content:
Open a terminal session and enter the following command to verify the /etc/openldap/ldap.conf has no extended ACLs.

ls -lL /etc/openldap/ldap.conf

If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the ACLs.

chmod -RN /etc/openldap/ldap.conf

CCI: CCI-000225

Group ID (Vulid): V-22583
Group Title: GEN008540
Rule ID: SV-39384r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN008540 M6
Rule Title: The system's local firewall must implement a deny-all, allow-by-exception policy.

Vulnerability Discussion: A local firewall protects the system from exposing unnecessary or undocumented network services to the local enclave. If a system within the enclave is compromised, firewall protection on an individual system continues to protect it from attack.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Determine if the system's local firewall implements a deny-all, allow-by-exception policy. If it does not, this is a finding.

Fix Text: Configure the system's local firewall to implement a deny-all, allow-by-exception policy.

CCI: CCI-001109

Group ID (Vulid): V-22702
Group Title: GEN002690
Rule ID: SV-38144r1_rule
Severity: CAT II
Rule Version (STIG-ID): GEN002690 M6
Rule Title: System audit logs must be group-owned by wheel.

Vulnerability Discussion: Sensitive system and user information could provide a malicious user with enough information to penetrate further into the system.

Responsibility: System Administrator
IAControls: ECLP-1, ECTP-1

Check Content:
Open a terminal session and enter the following command to verify group ownership of the files.

ls -Ll /var/audit

If any file is not group owned by wheel, this is a finding.

Fix Text: Open a terminal session and enter the following command to change group ownership of the file.

chgrp wheel /var/audit/ <audit file>

CCI: CCI-000162

CCI: CCI-000163

Group ID (Vulid): V-24386
Group Title: GEN003850
Rule ID: SV-38213r1_rule
Severity: CAT I
Rule Version (STIG-ID): GEN003850 M6
Rule Title: The telnet daemon must not be running.

Vulnerability Discussion: The telnet daemon provides a typically unencrypted remote access service which does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised.

Responsibility: System Administrator
IAControls: DCPP-1

Check Content:
Open a terminal session and enter the following command to verify telnet is disabled.

defaults read /var/db/launchd.db/com.apple.launchd/overrides com.apple.telnetd

If a 1 is not returned, this is a finding.

Fix Text: Open a terminal session and use the following command to disable telnet.

launchctl unload -w /System/Library/LaunchDaemons/telnet.plist

NOTE: This command is being run to adjust the overrides file; unloading errors are normal, repeat the check to verify.

CCI: CCI-000197

Group ID (Vulid): V-25187
Group Title: OSX00010-Do not install unnecessary packages
Rule ID: SV-37149r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00010 M6
Rule Title: Unnecessary packages must not be installed.

Vulnerability Discussion: Removing unused packages frees disk space and reduces the risk of attackers finding vulnerabilities in unused components.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Verify unnecessary packages are not installed. Open a terminal session and enter the following command.
pkgutil / --pkgs
Review the packages installed, determine if the installed packages are needed. If not, then this is a finding.

Fix Text: Review the packages installed using the following command.
pkgutil / --pkgs
Determine if the installed packages are needed. If not, verify any dependencies and use the rm command to remove them.

Group ID (Vulid): V-25200
Group Title: OSX00015-Admin accounts with difficult names
Rule ID: SV-37153r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00015 M6
Rule Title: Administrator accounts must be created with difficult-to-guess names.

Vulnerability Discussion: The administrator account has unlimited privileges to the system. Creating a complex name improves the protection of this account and the system. Do not use administrator; do not use the name of the machine, etc.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
1. Select Finder.
2. Select Applications.
3. Select System Preferences.
4. Select Accounts.
5. Verify there are no easy to guess administrator account names. If any accounts have easy to guess names, this is a finding.

Fix Text: 1. Select Finder.
2. Select Applications.
3. Select System Preferences.
4. Select Accounts.

5. Rename or recreate accounts with difficult-to-guess names.

Group ID (Vulid): V-25204
Group Title: OSX00020-Maximum password age
Rule ID: SV-37158r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00020 M6
Rule Title: A maximum password age must be set.

Vulnerability Discussion: 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.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Open a terminal session and use the following command to view the setting for maximum password age.
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep maxMinutesUntilChangePassword.
If the value of "maxMinutesUntilChangePassword" is greater than 86400 or set to "0", this is a finding.

NOTE: If the command returns a response of "password server is not configured", the system is not managed. Use the following command for non-managed systems.
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep maxMinutesUntilChangePassword
If the value of "maxMinutesUntilChangePassword" is greater than 86400, this is a finding.

NOTE: The value of "0" will disable this setting and must not be used.

Fix Text: Open a terminal session and use the following command to set the value for maxMinutesUntilChangePassword.

sudo pwpolicy -n -setglobalpolicy "maxMinutesUntilChangePassword=86400"

NOTE: For non-managed system, use the following command.

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

Group ID (Vulid): V-25230
Group Title: OSX00030-Minimum password length
Rule ID: SV-37172r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00030 M6
Rule Title: A minimum password length must be set.

Vulnerability Discussion: 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.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Open a terminal session and enter the following command to view the setting for minimum password length.
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep minChars

If the value of minChars is less than 15, this is a finding.

NOTE: If the command returns a response of "password server is not configured", the system is not managed. Use the following command for non-managed systems.
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep minChars
If the value of minChars is less than 15, this is a finding.

Fix Text: Open a terminal session and use the following command to set the value for minimum password length.
sudo pwpolicy -n -setglobalpolicy "minChars=15"

NOTE: For non-managed system, use the following command.

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

Group ID (Vulid): V-25238
Group Title: OSX00040-Check newly-created password content
Rule ID: SV-37177r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00040 M6
Rule Title: Newly created password content must be checked.

Vulnerability Discussion: Configure the local system to verify newly created passwords do not contain user's account name or parts of the user's full name exceeding two consecutive characters.

Responsibility: System Administrator
IAControls: IAIA-1, IAIA-2

Check Content:
Open a terminal session and use the following command to view the setting for "password cannot be name".
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep passwordCannotBeName
If the value of "passwordCannotBeName" is not equal to "1", this is a finding.

NOTE: If the command returns a response of "password server is not configured", the system is not managed. Use the following command for non-managed systems.
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep passwordCannotBeName
If the value of "passwordCannotBeName" is not equal to "1", this is a finding.

Fix Text: Open a terminal session and use the following command to set the value for "password cannot be name".
sudo pwpolicy -n -setglobalpolicy "passwordCannotBeName=1"

NOTE: For non-managed system, use the following command.

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

Group ID (Vulid): V-25240
Group Title: OSX00045-Account lockout duration
Rule ID: SV-37184r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00045 M6
Rule Title: Account lockout duration must be properly configured.

Vulnerability Discussion: This parameter specifies the amount of time that must pass between two successive login

attempts to ensure a lockout will occur. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.

Responsibility: System Administrator
IAControls: ECLO-1, ECLO-2

Check Content:
Open a terminal session and use the following command to view the setting for Account lockout duration.
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep minutesUntilFailedLoginReset
If the value of "minutesUntilFailedLoginReset" is greater than "0", this is a finding.

NOTE: If the command returns a response of "password server is not configured", the system is not managed. Use the following command for non-managed systems.
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep minutesUntilFailedLoginReset
If the value of "minutesUntilFailedLoginReset" is greater than "0", this is a finding.

Fix Text: Open a terminal session and use the following command to set the value for account lockout duration.
sudo pwpolicy -n -setglobalpolicy "minutesUntilFailedLoginReset=0"

NOTE: For non-managed system, use the following command.

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

Group ID (Vulid): V-25241
Group Title: OSX00050-Account lockout threshold
Rule ID: SV-37186r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00050 M6
Rule Title: Account lockout threshold must be properly configured.

Vulnerability Discussion: The account lockout feature, when enabled, prevents brute-force password attacks on the system. The higher this value is, the less effective the account lockout feature will be in protecting the local system. The number of incorrect logon attempts should be reasonably small to minimize the possibility of a successful password attack, while allowing for honest errors made during a normal user logon.

Responsibility: System Administrator
IAControls: ECLO-1, ECLO-2

Check Content:
Open a terminal session and use the following command to view the setting for account lockout threshold.
sudo pwpolicy -n -getglobalpolicy | tr " " "\n" | grep maxFailedLoginAttempts
If the value of "maxFailedLoginAttempts" is more than "3", or set to "0", this is a finding.

NOTE: If the command returns a response of "password server is not configured", the system is not managed. Use the following command for non-managed systems.
pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep maxFailedLoginAttempts
If the value of "maxFailedLoginAttempts" is more than "3", or set to "0", this is a finding.

Fix Text: Open a terminal session and use the following command to set the value for account lockout threshold.
sudo pwpolicy -n -setglobalpolicy "maxFailedLoginAttempts=3"

NOTE: For non-managed system, use the following command.

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

Group ID (Vulid): V-25251
Group Title: OSX00055-Application software updates
Rule ID: SV-37190r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00055 M6
Rule Title: All application software must be current.

Vulnerability Discussion: Major software vendors release security patches and hot fixes to their products when security vulnerabilities are discovered. It is essential these updates be applied in a timely manner to prevent unauthorized persons from exploiting identified vulnerabilities. If the application software is no longer supported it should be updated or removed.

Severity Override Guidance:
If any of the patches not installed are 'Critical', then this should be elevated to a Category 1.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
Open a terminal session and enter the following command.
sudo softwareupdate --list or sudo softwareupdate --list --all
Review the result for proper versions and current patch level.
GUI procedures:
1. Choose Apple (?) > Software Update.
2. Select Scheduled Check & Installed Updates.
3. Verify all current software updates are installed. If the current software updates are not installed, this is a finding.

NOTE: This check does not show third party software or updates.

Fix Text: Install current software updates and patches.

NOTE: Do not enable Automatic Updating as this will conflict with V-25298.

Group ID (Vulid): V-25252
Group Title: OSX00060-Disable Wi-Fi Support Software
Rule ID: SV-37193r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00060 M6
Rule Title: Wi-Fi support software must be disabled.

Vulnerability Discussion: Many organizations restrict the use of wireless technology in their network environment. However, most Mac computers have wireless capability built-in and simply turning it off may not meet the organization's wireless technology restrictions. Components may need to be removed from Mac OS X to disable them from being turned on in System Preferences. Although wireless technology gives a network more flexibility with its users, it can also cause security vulnerabilities most may be unaware of. It is recommended wherever possible, wireless access is disabled for security reasons. IMPORTANT: Repeat these instructions every time a system update is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and view the /System/Library/Extensions folder.
Ensure the following file does NOT exist.

IO80211Family.kext

If the file exists, this is a finding.

Fix Text: Open a terminal session and enter the following commands.

srm -rf /System/Library/Extensions/IO80211Family.kext

touch /System/Library/Extensions

NOTE: Repeat these instructions every time a system update is installed.

Group ID (Vulid): V-25253
Group Title: OSX00065-Disable Bluetooth Support Software
Rule ID: SV-37198r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00065 M6
Rule Title: Bluetooth support software must be disabled.

Vulnerability Discussion: Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as Denial of Service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Remove Bluetooth support for peripherals such as keyboards, mice, or phones. This task requires administrator privileges. IMPORTANT: Repeat these instructions every time a system update is installed. Support should be removed at kext level.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and view the /System/Library/Extensions folder.
Ensure the following files do NOT exist.

IOBluetoothFamily.kext
IOBluetoothHIDDriver.kext

If any file exists, this is a finding.

Fix Text: Open a terminal session and enter the following commands to remove the files.

srm -rf /System/Library/Extensions/IOBluetoothFamily.kext

srm -rf /System/Library/Extensions/IOBluetoothHIDDriver.kext

sudo touch /System/Library/Extensions

NOTE: Repeat these instructions every time a system update is installed.

Group ID (Vulid): V-25254
Group Title: OSX00070-Disable Audio Recording Support Software
Rule ID: SV-38509r1_rule
Severity: CAT II

Rule Version (STIG-ID): OSX00070 M6
Rule Title: Audio recording support software must be disabled.

Vulnerability Discussion: A computer might be in an environment where recording devices, such as cameras or microphones are not permitted. Protect the organization's privacy by disabling these devices. Remove support for the audio subsystem. This may disable audio playback. IMPORTANT: Repeat these instructions every time a system update is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and view the /System/Library/Extensions/ folder if any of the following files exist, this is a finding.

AppleUSBAudio.kext
IOAudioFamily.kext

Fix Text: Open a terminal session and enter the following commands.

srm -rf /System/Library/Extensions/AppleUSBAudio.kext

srm -rf /System/Library/Extensions/IOAudioFamily.kext

touch /System/Library/Extensions

NOTE: Repeat these instructions every time a system update is installed.

Group ID (Vulid): V-25255
Group Title: OSX00075-Disable Video Recording Support Software
Rule ID: SV-37201r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00075 M6
Rule Title: Video recording support software must be disabled.

Vulnerability Discussion: A computer might be in an environment where recording devices, such as cameras or microphones, are not permitted. Protect the organization's privacy by disabling these devices. Remove support for an external or built-in iSight camera.
NOTE: The support for external iSight cameras should be removed on all machines. Removing only support for internal iSight cameras would still leave support for external cameras available. An Apple Authorized Technician can also remove the built-in video camera hardware from an Apple computer.
IMPORTANT: Repeat these instructions every time a system update is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and view the /System/Library/Extensions folder.
Ensure the following file does NOT exist: Apple_iSight.kext.
Control click the IOUSBFamily.kext and select Show Package Contents.
Open the /Contents/PlugIns/ folder.
Ensure the following file does NOT exist: AppleUSBVideoSupport.kext

If any of the files exist, this is a finding.

Fix Text: Open a terminal session and enter the following commands to remove the files.

sudo srm -rf /System/Library/Extensions/Apple_iSight.kext
sudo srm -rf /System/Library/Extensions/IOUSBFamily.kext/Contents/Plugins/AppleUSBVideoSupport.kext

sudo touch /System/Library/Extensions

NOTE: Repeat these instructions every time a system update is installed.

Group ID (Vulid): V-25258
Group Title: OSX00090-Remove Infrared (IR) Support
Rule ID: SV-37206r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00090 M6
Rule Title: Infrared (IR) support must be removed.

Vulnerability Discussion: To prevent unauthorized users from controlling a computer through the infrared receiver, remove IR hardware support. This task requires administrator privileges. An Apple Authorized Technician can also remove IR hardware from an Apple computer.
IMPORTANT: Repeat these instructions every time a system update is installed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and view the /System/Library/Extensions folder.
Ensure the following file does NOT exist.

AppleIRController.kext

If the file exists, this is a finding.

Fix Text: Open a terminal session and enter the following commands to remove the file.

srm -rf /System/Library/Extensions/AppleIRController.kext

sudo touch /System/Library/Extensions

NOTE: Repeat these instructions every time a system update is installed.

Group ID (Vulid): V-25259
Group Title: OSX00095-Require an Open Firmware or EFI password
Rule ID: SV-38510r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00095 M6
Rule Title: An Extensible Firmware Interface (EFI) password must be used.

Vulnerability Discussion: When a computer starts up, it first starts Extensible Firmware Interface (EFI). 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. 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.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
Log in with an administrator account and open the Firmware Password Utility (located on the Mac OS X installation disc in /Applications/Utilities/).

Verify the "Require password to start this computer from another source" is selected. If not, this is a finding.

Fix Text: Log in with an administrator account and open the Firmware Password Utility (located on the Mac OS X installation disc in /Applications/Utilities/).

Click New.

Select "Require password to start this computer from another source".

In the Password and Verify fields, enter a new EFI password and click OK.

Close the Firmware Password Utility.

Group ID (Vulid): V-25260
Group Title: OSX00100-Create access warning for the login
Rule ID: SV-38556r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00100 M6
Rule Title: Access warning for the login window must be present.

Vulnerability Discussion: Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources. A login window or Terminal access warning can be used to provide notice of a computer’s ownership, to warn against unauthorized access, or to remind authorized users of their consent to monitoring.

Responsibility: System Administrator
IAControls: ECWM-1

Check Content:
If the following DoD warning banner is not displayed at the top of the login panel before entering the user name and password, this is a finding.

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or

monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

NOTE: Any OS versions that do not support the full text version must state the following:
"I've read & consent to terms in IS user agreem't."

NOTE: Deviations are not permitted except as authorized by the Deputy Assistant Secretary of Defense for Information and Identity Assurance.

Fix Text: Open a terminal session and enter the following command.
sudo defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Log off the system and verify the banner is displayed at the login screen.

Group ID (Vulid): V-25261
Group Title: OSX00105-Access warning for command line
Rule ID: SV-38513r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00105 M6
Rule Title: Access warning for the command line must be present.

Vulnerability Discussion: Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources. When a user opens a terminal locally or connects to the computer remotely, the user sees the access warning.

Responsibility: System Administrator
IAControls: ECWM-1

Check Content:
Open a terminal session. The warning banner should be displayed in the terminal. If the following DoD warning banner is not displayed, this is a finding.

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Note: Any OS versions not supporting the full text version must state the following:
"I've read and consent to terms in IS user agreem't".

Note: Deviations are not permitted except as authorized by the Deputy Assistant Secretary of Defense for Information and Identity Assurance.

Fix Text: 1. Open a terminal session
2. Verify the /etc/motd file exists. If not, use the touch command to create the file.
3. Edit the file and enter the appropriate DoD warning banner information.
4. Save the file.
5. Open a new terminal session and verify the banner is displayed.

Group ID (Vulid): V-25262
Group Title: OSX00110-Restrict sudo usage
Rule ID: SV-38614r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00110 M6
Rule Title: sudo usage must be restricted to a single terminal, and for only one sudo instance at a time.

Vulnerability Discussion: 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.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and use the following command to view the values.

grep Defaults /etc/sudoers

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

If the values are not present, this is a finding.

Fix Text: Open a terminal session and enter the following commands to set the values in the /etc/sudoers file.

VISUAL=pico visudo

Enter the following two lines in the file.

Defaults tty_tickets
Defaults timestamp_timeout=0

Save and exit the file.

Group ID (Vulid): V-25263
Group Title: OSX00115-Securely configure LDAPv3
Rule ID: SV-38514r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00115 M6
Rule Title: LDAPv3 access must be securely configured (if it is used).

Vulnerability Discussion: When configuring LDAPv3, do not add DHCP supplied LDAP servers to automatic search policies if the network the computer is running on is not secure. If the network is unsecure, someone can create a rogue DHCP.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click the Connection tab and verify "Encrypt using SSL" is selected. If "Encrypt using SSL" is not selected, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click the Connection tab and select "Encrypt using SSL".

Group ID (Vulid): V-25264
Group Title: OSX00120-LDAP Authentication
Rule ID: SV-38516r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00120 M6
Rule Title: LDAP Authentication must use authentication when connecting to LDAPv3.

Vulnerability Discussion: When configuring LDAPv3, do not add DHCP-supplied LDAP servers to automatic search policies if the network the computer is running on is not secure. If the network is unsecure, someone can create a rogue DHCP. Use authentication when connecting to LDAPv3 directories; disable clear text passwords for all LDAPv3 directories; digitally sign all LDAPv3 packets (requires Kerberos); encrypt all LDAPv3 packets (requires SSL or Kerberos); and block man-in-the-middle attacks (requires Kerberos).

Responsibility: System Administrator
IAControls: DCNR-1, ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click the Security tab and verify the "Use authentication when connecting" is checked. If option is not checked, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.

Click on Security tab and select "Use authentication when connecting".

Group ID (Vulid): V-25265
Group Title: OSX00125-Securely configure AD Access
Rule ID: SV-38518r1_rule

Severity: CAT I
Rule Version (STIG-ID): OSX00125 M6
Rule Title: Active Directory Access must be securely configured.

Vulnerability Discussion: The “Allow administration by” setting should not be used in sensitive environments. It can cause unintended privilege escalation issues because any member of the group specified will have administrator privileges on a computer.

Responsibility: System Administrator
IAControls: DCNR-1, ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Services tab.
Double Click on Active Directory.
Click on Show Advanced Options.
Click on Administrative tab and ensure "Allow administration by" is not selected. If "Allow administration by" is selected, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Services tab.
Double Click on Active Directory.
Click on Show Advanced Options.
Click on Administrative tab and deselect "Allow administration by" option.

Group ID (Vulid): V-25267
Group Title: OSX00135-POSIX access permissions
Rule ID: SV-37208r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00135 M6
Rule Title: POSIX access permissions must be assigned based on user categories.

Vulnerability Discussion: POSIX access permissions must be assigned based on user categories. Changing permissions on a user's home directory from 750 to 700 will disable Apple file sharing. User's home directory POSIX permissions should be set to 700.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

ls -ld <users home directory>

If permissions are not set to 700, this is a finding.

Fix Text: Open a terminal session and enter the following command.

sudo chmod 700 <user's home directory>

Group ID (Vulid): V-25268
Group Title: OSX00140-Enable security auditing
Rule ID: SV-38520r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00140 M6
Rule Title: Security auditing must be enabled.

Vulnerability Discussion: Auditing is the capture and maintenance of information about security-related events. Auditing helps determine the causes and the methods used for successful and failed access attempts.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
Open a terminal session and run the following command.

sudo launchctl list

Verify "com.apple.auditd" appears. If the file does not appear, this is a finding.

Fix Text: Open a terminal session and run the following command.

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

---

Group ID (Vulid): V-25269
Group Title: OSX00145-Configure security auditing
Rule ID: SV-38521r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00145 M6
Rule Title: Security auditing must be configured.

Vulnerability Discussion: 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. Without an audit trail providing information as to what occurred and if it was successful or unsuccessful, it is difficult to analyze a series of events to determine the steps used by an attacker to compromise a system or network, or what exactly happened that led to a Denial of Service. Collecting data such as the successful and unsuccessful events is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
Open a terminal session and enter the following command view the audit flags.

more /etc/security/audit_control file.

Review the entries and ensure the line includes the following: flags: lo,ad,-all,-fr,fd,fm,^-fa,^-fc,^-cl.
If the file does not contain the appropriate flags, this is a finding.

Fix Text: Open a terminal session and edit the /etc/security/audit_control file.
Find the line beginning with "flags".
Replace that line with the following: flags:lo,ad,-all,-fr,fd,fm,^-fa,^-fc,^-cl.
Save the file.

Group ID (Vulid): V-25270
Group Title: OSX00150-Enable local logging
Rule ID: SV-38522r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00150 M6
Rule Title: Local logging must be enabled.

Vulnerability Discussion: Logging is essential for tracking system events, in the event of unauthorized access, logs may contain information about how and when the access occurred. Ensure logging is enabled and log files are properly rotated. The default configuration in /etc/newsyslog.conf is used to configure local logging in the /var/log folder. The computer is set to rotate log files using the periodic launchd job according to time intervals specified in the /etc/newsyslog.conf file.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
Open a terminal session and enter the following command.

more /etc/newsyslog.conf

If the count values are not set to "14", this is a finding.

Fix Text: Open a terminal session and edit the following file and set the count value(s) to "14".

/etc/newsyslog.conf

Group ID (Vulid): V-25271
Group Title: OSX00155-Enable remote logging
Rule ID: SV-38523r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00155 M6
Rule Title: Remote logging must be enabled.

Vulnerability Discussion: In addition to local logging, remote logging must also be enabled. Local logs can be altered if the computer is compromised. Remote logging mitigates the risk of having the logs altered.

Responsibility: System Administrator
IAControls: ECAR-1, ECAR-2, ECAR-3

Check Content:
Open a terminal session and enter the following command.

more /etc/syslog.conf

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

If the name or IP address of the log server is not listed, this is a finding.

Fix Text: Open a terminal session and enter the following command.

sudo pico /etc/syslog.conf

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
Exit, saving changes.
Reboot the system.

Group ID (Vulid): V-25272
Group Title: OSX00160-Install an antivirus tool
Rule ID: SV-38524r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00160 M6
Rule Title: An antivirus tool must be installed.

Vulnerability Discussion: Installing antivirus tools helps prevent virus infection on a computer, and helps prevent a computer from becoming a host used to spread viruses to other computers. These tools quickly identify suspicious content and compare them to known malicious content. See the https://www.cybercom.mil web site for approved antivirus tools.

Responsibility: System Administrator
IAControls: ECVP-1

Check Content:
Verify an approved antivirus tool is installed on the system.

Fix Text: Install an approved antivirus tool on the system.

Group ID (Vulid): V-25273
Group Title: OSX00165-Prevent root login
Rule ID: SV-38525r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00165 M6
Rule Title: Prevent root login must be securely configured in /etc/sshd_config.

Vulnerability Discussion: Prevents logging in as root through SSH. This should be set for all SSH methods of authenticating.

Responsibility: System Administrator
IAControls: COBR-1, ECPA-1

Check Content:
Open a terminal session and enter the following command.

more /etc/sshd_config

Ensure the value "PermitRootLogin" is set to "No". If the value "PermitRootLogin" is not set to "No", this is a finding.

NOTE: If the line starts with a # sign this is a comment and the command to disable root login would be invalid regardless of the value, this is a finding.

Fix Text: Open a terminal session and enter the following command.

sudo pico /etc/sshd_config

Edit the value "PermitRootLogin" and set it to "No".
Save the file.

Group ID (Vulid): V-25274
Group Title: OSX00170-Securely configure /etc/sshd_config
Rule ID: SV-38526r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00170 M6
Rule Title: Login Grace Time must be securely configured in /etc/sshd_config.

Vulnerability Discussion: This setting controls the time allowed to authenticate over an ssh connection. It is recommended the value be set to 30 seconds or less. By allowing a connection to stay open for longer periods of time could allow an attacker to take advantage of the port.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

more /etc/sshd_config

Ensure the value "LoginGraceTime" is set to 30 or less. If the value "LoginGraceTime" is not set to 30 or less, this is a finding.

NOTE: If the value is set to "0", this is a finding.

Fix Text: Open a terminal session and enter the following command.

sudo pico /etc/sshd_config

Edit the value "LoginGraceTime" and set it to "30".
Save the file.

Group ID (Vulid): V-25275
Group Title: OSX00175-Securely configure sshd Protocol version
Rule ID: SV-37209r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00175 M6
Rule Title: /etc/sshd_config - Protocol version must be securely configured.

Vulnerability Discussion: Restricts OpenSSH so it uses only SSH Protocol 2. This should be set for all SSH methods of

authenticating.

Responsibility: System Administrator
IAControls: ECSC-1

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

more /etc/sshd_config

2. Ensure the value Protocol is set to "2". If the value Protocol is not set to "2", this is a finding.

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

sudo pico /etc/sshd_config

2. Edit the value "Protocol" and set it to "2".
3. Save the file.

Group ID (Vulid): V-25276
Group Title: OSX00180-sshd Empty passwords
Rule ID: SV-40699r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00180 M6
Rule Title: OSX00180-SSH must not allow empty passwords.

Vulnerability Discussion: Denies access to accounts without passwords. This should be set for all SSH methods of authenticating.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the command.

more /etc/sshd_config

If the value of PermitEmptyPasswords is set to Yes, this is a finding. If the PermitEmptyPasswords option is not set, this is not a finding.

Fix Text: Open a terminal session and edit the following file.

/etc/sshd_config

Set the value of PermitEmptyPasswords to No.

Group ID (Vulid): V-25278
Group Title: OSX00190-Remove the MobileMe preference pane
Rule ID: SV-38527r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00190 M6
Rule Title: The MobileMe preference pane must be removed from System Preferences.

Vulnerability Discussion: Remove the MobileMe preference pane from System Preferences. MobileMe is a suite of Internet tools capable of synchronizing data and other important information while an individual is away from the computer, sensitive environments do not use MobileMe. If critical data must be stored, only store it on a local computer. Data should only be transferred over a secure network connection to a secure internal server. If MobileMe is used, enable it only for user accounts without access to critical data. It is not recommended to enable MobileMe for administrator or root user accounts.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and navigate to the /System/Library/PreferencePanes folder.

Ensure the following file does NOT exist.

MobileMe.prefPane

If this file exists, this is a finding.

Fix Text: Open a terminal session and enter the following command to remove the file.

sudo rm -R /System/Library/PreferencePanes/MobileMe.prefPane

Group ID (Vulid): V-25279
Group Title: OSX00195-Software Update Server URL
Rule ID: SV-38528r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00195 M6
Rule Title: The Software Update Server URL must be assigned to an organizational value.

Vulnerability Discussion: A computer can look for software updates on an internal software update server (SUS). Using an internal software update server reduces the amount of data transferred outside of the network. The organization can control which updates can be installed on a computer.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
Open a terminal session and enter the following command.

defaults read com.apple.SoftwareUpdate CatalogURL

The value returned is the current Software Update Server. Verify it is an approved SUS. If no value is returned, the system is using a default Apple Update Server and this is a finding.
NOTE: If the system is not using an authorized DoD SUS server, it should point to a null address.

Fix Text: Open a terminal session and enter the following command.

defaults write com.apple.SoftwareUpdate CatalogURL 'new_SUS_URL'

(Where 'new_SUS_URL' is the URL or the address of the appropriate government SUS to be used.)

Group ID (Vulid): V-25280
Group Title: OSX00200-Admin unlock Screen Saver
Rule ID: SV-37214r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00200 M6
Rule Title: The ability for administrative accounts to unlock screen saver must be disabled.

Vulnerability Discussion: The default setting creates a possible point of attack, because the more users in the admin group the more dependent on those users to protect their user names and passwords. By changing the rule in “system.login.screensaver” to “authenticatesession-owner”, users of the admin group cannot unlock the screen saver.

Responsibility: System Administrator
IAControls: ECPA-1, PESL-1

Check Content:
Open a terminal session and enter the following command.

more /etc/authorization

Ensure the "system.login.screensaver" key includes the value "authenticate-session-owner". If not, this is a finding.

Fix Text: Open a terminal session and edit the following file.

/etc/authorization

Change "authenticate-session-owner-or-admin " to "authenticate-session-owner" in the "system.login.screensaver" key.
Save the file.

Group ID (Vulid): V-25283
Group Title: OSX00215-Remove setuid bit from Apple Remote Dsk
Rule ID: SV-38223r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00215 M6
Rule Title: Setuid bit must be removed from Apple Remote Desktop.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -la /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent

Verify the file permissions are set to 755 or more restrictive. If not, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 755 /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent

---

Group ID (Vulid): V-25291
Group Title: OSX00255-Remove setuid bit from IPC Statistics
Rule ID: SV-38233r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00255 M6
Rule Title: The setuid bit must be removed from the IPC Statistics.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -ld /usr/bin/ipcs

Ensure the file permissions are set to 511. If the permission is not the same or more restrictive, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 511 /usr/bin/ipcs

Group ID (Vulid): V-25292
Group Title: OSX00260-Remove setuid bit from Remote Access
Rule ID: SV-38235r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00260 M6
Rule Title: The setuid bit from Remote Access (unsecure) must be removed.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -ld /bin/rcp

Verify the file permissions are set to 555 or more restrictive. If not, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 555 /bin/rcp

Group ID (Vulid): V-25293
Group Title: OSX00265-setuid rlogin
Rule ID: SV-38237r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00265 M6
Rule Title: The setuid bit from rlogin must be removed.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -ld /usr/bin/rlogin
Verify the file permissions are set to 555 or more restrictive. If not, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 555 /usr/bin/rlogin

Group ID (Vulid): V-25294
Group Title: OSX00270-setuid rsh
Rule ID: SV-38238r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00270 M6
Rule Title: The setuid bit from Remote Access shell (unsecure) must be removed.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -ld /usr/bin/rsh

Verify the file permissions are set to 555 or more restrictive. If not, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 555 /usr/bin/rsh

Group ID (Vulid): V-25295
Group Title: OSX00275-setuid System Activity Reporting
Rule ID: SV-38239r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00275 M6
Rule Title: The setuid bit from System Activity Reporting must be removed.

Vulnerability Discussion: Because attackers try to influence or co-opt the execution of setuid programs in order to try to elevate their privileges, there is benefit in removing the setuid bit from programs that may not need it. There is also benefit in restricting to administrators the right to execute a setuid program.

Responsibility: System Administrator
IAControls: ECCD-1, ECCD-2

Check Content:
Open a terminal session and enter the following command.

ls -ld /usr/lib/sa/sadc

Verify the file permissions are set to 555 or more restrictive. If not, this is a finding.

Fix Text: Open a terminal session and enter the following command.

chmod 555 /usr/lib/sa/sadc

Group ID (Vulid): V-25296
Group Title: OSX00280-Set the correct date and time
Rule ID: SV-38529r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00280 M6
Rule Title: The correct date and time must be set.

Vulnerability Discussion: Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Date&Time Panel.
2. Ensure the correct date and time is set. If the date and time are not correct, this is a finding.

Fix Text: 1. Open System Preferences->Date&Time Panel.
2. Set the correct date and time.

Group ID (Vulid): V-25297
Group Title: OSX00285-secure time server
Rule ID: SV-38530r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00285 M6
Rule Title: A secure time server must be referenced.

Vulnerability Discussion: Correct date and time settings are required for authentication protocols, like Kerberos. Incorrect date and time settings can cause security issues. Date and time preferences can be used to set the date and time based on a Network Time Protocol (NTP) server. If you require automatic date and time, use a trusted, internal NTP server.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Date & Time Panel.
2. Ensure "Set date & time automatically" is selected.
3. In the box for the time server, ensure the URL is entered along with either the address of a valid federal government NTP server or address of a local domain controller.

Fix Text: 1. Open System Preferences> Date & Time Panel.
2. Select "Set date & time automatically".
3. In the box for the time server, type either the URL or IP address of a valid federal government NTP server or local domain controller.

Group ID (Vulid): V-25298
Group Title: OSX00290-Disable Auto Update
Rule ID: SV-38531r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00290 M6
Rule Title: The Auto Update feature must be disabled.

Vulnerability Discussion: By disabling automatic updates, updates can be downloaded and tested in a non production environment before they are distributed to the production workstations. This reduces the risk of accidental or malicious software updates being applied before they are properly tested.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

softwareupdate --schedule

Verify "Automatic check" is off. If the option is not off, this is a finding.

Fix Text: Open a terminal session and enter the following command to disable the auto update feature.

softwareupdate --schedule off

Group ID (Vulid): V-25299
Group Title: OSX00295-Disable Guest Account login
Rule ID: SV-37218r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00295 M6
Rule Title: The guest account must be disabled.

Vulnerability Discussion: The guest account is used to give a user temporary access to a computer. The guest account should be disabled by default because it does not require a password to login on the computer. If this account is enabled and is not securely configured malicious users can gain access to a computer without the use of a password.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
1. Open System Preferences->Accounts Panel.
2. Click on Guest Account.
3. Ensure "Allow guests to login to this computer" option is unchecked. If the option is checked, this is a finding.

Fix Text: 1. Open System Preferences->Accounts Panel.
2. Click on Guest Account.
3. Deselect "Allow guests to login to this computer".

Group ID (Vulid): V-25300
Group Title: OSX00300-disable shared folders
Rule ID: SV-37219r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00300 M6
Rule Title: Shared folders must be disabled.

Vulnerability Discussion: Whether or not the guest account itself is enabled, disable guest account access to shared files and folders by deselecting the “Allow guest to connect to shared folders” checkbox. If the guest account is permitted to access shared folders, an attacker can easily attempt to access shared folders without a password.

Responsibility: System Administrator
IAControls: ECAN-1, ECSC-1

Check Content:
1. Open System Preferences->Accounts Panel.
2. Click on Guest Account.
3. Ensure "Allow Guests to connect to shared folders" option is unchecked. If the option is checked, this is a finding.

Fix Text: 1. Open System Preferences->Accounts Panel.
2. Click on Guest Account.

3. Deselect "Allow Guests to connect to shared folders".

Group ID (Vulid): V-25302
Group Title: OSX00310-login display name/password
Rule ID: SV-37221r1_rule
Severity: CAT II

Rule Version (STIG-ID): OSX00310 M6
Rule Title: Login window must be properly configured.

Vulnerability Discussion: If not properly configured, the logon screen provides a list of local user names available for logon. A user could use this information to attempt to login as a different user.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Accounts Panel.
2. Select Login Options.
3. Ensure "Display login window as:" is set to "Name & password". If the option is not set to "Name & Password", this is a finding.

Fix Text: 1. Open System Preferences->Accounts Panel.
2. Select Login Options.

3. Set "Display login window as:" to 'Name & password'.

Group ID (Vulid): V-25304
Group Title: OSX00320-Do not show Input menu in login window
Rule ID: SV-37225r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00320 M6
Rule Title: Input menu must not be shown in login window.

Vulnerability Discussion: Showing input in the login window could compromise the integrity of the information, and could also allow someone shoulder surfing to gain unauthorized access to the system.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
1. Open System Preferences->Accounts Panel.
2. Select Login Options.
3. Ensure the "Show input menu in login window" is not checked. If the option is checked, this is a finding.

Fix Text: 1. Open System Preferences->Accounts Panel.
2. Select Login Options.

3. Deselect "Show input menu in login window" to disable this option.

Group ID (Vulid): V-25305
Group Title: OSX00325-Do not show password hints
Rule ID: SV-37226r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00325 M6
Rule Title: The system must be configured to not show password hints.

Vulnerability Discussion: Providing information in the password hint field could compromise the integrity of the password. Showing password hint could allow someone shoulder surfing to gain information leading to unauthorized access to the system.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
1. Open System Preferences->Accounts Panel.
2. Select Login Options.
3. Ensure the "Show password hints" is not checked. If the option is checked, this is a finding.

Fix Text: 1. Open System Preferences->Accounts Panel.
2. Select Login Options.

3. Deselect "Show password hints" to disable this option.

Group ID (Vulid): V-25306
Group Title: OSX00330-Disable Fast User Switching
Rule ID: SV-37229r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00330 M6
Rule Title: Fast User Switching must be disabled.

Vulnerability Discussion: Fast User Switching allows multiple users to log in simultaneously. This makes it difficult to track user actions and allows users to run malicious applications in the background while another user is using the computer.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Open System Preferences->Accounts Panel.
Select Login Options.
Ensure the "Show fast user switching menu as" is not checked. If the option is checked, this is a finding.

Fix Text: Open System Preferences->Accounts Panel.
Select Login Options.

Deselect "Show fast user switching menu as" to disable this option.

Group ID (Vulid): V-25307
Group Title: OSX00335-Do not use password-related hint field
Rule ID: SV-38532r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00335 M6
Rule Title: The password-related hint field must not be used.

Vulnerability Discussion: If a hint is provided, the user is presented with the hint after three failed authentication attempts. Password-related information provided in the field could compromise the integrity of the password. Adding contact information for your organization’s technical support is convenient and does not compromise password integrity.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
1. Open System Preferences->Accounts Panel, for each account.
2. Click 'reset password' (Change Password for current user).
3. Ensure no data exists in the password hints field.
4. Click Cancel.

If any accounts have hints data, this is a finding.
NOTE: The password hints field may include contact information for the organization's technical support.

Fix Text: 1. Open System Preferences -> Accounts Panel, for each account.
2. Click 'reset password' (Change Password for current user).
3. Remove any data in the password hints field.
NOTE: The password hints field may include contact information for the organization's technical support.

Group ID (Vulid): V-25308
Group Title: OSX00340-Securely configure System Preferences
Rule ID: SV-37230r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00340 M6
Rule Title: Automatic actions must be disabled for blank CDs.

Vulnerability Discussion: To secure CDs and DVDs, do not allow the computer to perform automatic actions when the user inserts a disc. When disabling automatic actions in System Preferences, these actions must be disabled for every user account on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

defaults read /Library/Preferences/com.apple.digihub com.apple.digihub.blank.cd.appeared -dict

If the action is not set to "1", this is a finding.

Fix Text: Open a terminal session and enter the following command.

defaults write /Library/Preferences/com.apple.digihub com.apple.digihub.blank.cd.appeared -dict action 1

Group ID (Vulid): V-25309
Group Title: OSX00345-Secure System Preferences music
Rule ID: SV-37231r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00345
Rule Title: Automatic actions must be disabled for music CDs.

Vulnerability Discussion: To secure CDs and DVDs (music), do not allow the computer to perform automatic actions when the user inserts a disc. When disabling automatic actions in System Preferences, these actions must be disabled for every user account on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > CDs and DVDs.
Ensure "When you insert a music CD" is set to "Ignore". If the option is not set to "Ignore", this is a finding.

Fix Text: Open System Preferences - > CDs and DVDs.

Set "When you insert a music CD" to "Ignore".

Group ID (Vulid): V-25310
Group Title: OSX00350-System Preferences pictures
Rule ID: SV-37235r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00350 M6
Rule Title: Automatic actions must be disabled for picture CDs.

Vulnerability Discussion: To secure CDs and DVDs, do not allow the computer to perform automatic actions when the user inserts a disc. When disabling automatic actions in System Preferences, these actions must be disabled for every user account on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > CDs and DVDs.
Ensure "When you insert a picture CD" is set to "Ignore". If the option is not set to "Ignore", this is a finding.

Fix Text: Open System Preferences - > CDs and DVDs.

Set "When you insert a picture CD" to "Ignore".

Group ID (Vulid): V-25311
Group Title: OSX00355-System Preferences Video
Rule ID: SV-37236r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00355 M6
Rule Title: Automatic actions must be disabled for video DVDs.

Vulnerability Discussion: To secure CDs and DVDs, do not allow the computer to perform automatic actions when the user inserts a disc. When disabling automatic actions in System Preferences, these actions must be disabled for every user account on the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > CDs and DVDs.
Ensure "When you insert a video DVD" is set to "Ignore". If the option is not set to "Ignore", this is a finding.

Fix Text: Open System Preferences - > CDs and DVDs.

Set "When you insert a video DVD" to "Ignore".

Group ID (Vulid): V-25312
Group Title: OSX00360-Password Protected Screen Saver
Rule ID: SV-38533r1_rule
Severity: CAT II

Rule Version (STIG-ID): OSX00360 M6
Rule Title: System must have a password-protected screen saver configured to DoD requirements.

Vulnerability Discussion: User needs to configure a password-protected screen saver to prevent unauthorized users from accessing unattended computers. A short inactivity interval should also be set to decrease the amount of time the unattended computer is unlocked.

Responsibility: System Administrator
IAControls: PESL-1

Check Content:
Open System Preferences->Desktop & Screen Saver.
Select the screen saver tab.
Ensure the "Start screen saver" slider is set to 15 minutes or less. If not, this is a finding.

Fix Text: Open System Preferences->Desktop & Screen Saver.
Select the screen saver tab.
Set the "Start screen saver" slider to 15 minutes or less.

Group ID (Vulid): V-25317
Group Title: OSX00375-Secure screen saver corners
Rule ID: SV-37242r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00375 M6
Rule Title: The ability to use corners to disable the screen saver must be disabled.

Vulnerability Discussion: A computer should require authentication when waking from sleep or screen saver. Exposé & Spaces preferences can be configured to disable the screen saver by moving the mouse cursor to a corner of the screen. Do not configure a corner to disable the screen saver.

Responsibility: System Administrator
IAControls: PESL-1

Check Content:
Open System Preferences->Exposé & Spaces, Exposé pane.
Ensure no corners are set to "Disable Screen saver" in the "Active Screen Corners" section for each user account. If any account is set to disable screen savers via corners, this is a finding.

NOTE: Do this for each user on the system.

Fix Text: Open System Preferences->Exposé & Spaces, Exposé pane.
Remove any corners which are set to "Disable Screen saver" in the "Active Screen Corners" section for each user

account.

Group ID (Vulid): V-25318
Group Title: OSX00380-Disable Bluetooth awake the computer
Rule ID: SV-38535r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00380 M6
Rule Title: Bluetooth devices must not be allowed to wake the computer.

Vulnerability Discussion: If Bluetooth is not required, turn it off. If Bluetooth is necessary, disable allowing Bluetooth devices to awake the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences -> Bluetooth.
Click Advanced.
Ensure "Allow Bluetooth devices to wake this computer" is not checked.
If the option is checked, this is a finding.

Fix Text: Open System Preferences -> Bluetooth.
Click Advanced.

Deselect "Allow Bluetooth devices to wake this computer".

Group ID (Vulid): V-25320
Group Title: OSX00385-Disable unused hardware
Rule ID: SV-37245r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00385 M6
Rule Title: Unused hardware devices must be disabled for AirPort.

Vulnerability Discussion: It is recommended to disable unused hardware devices listed in Network preferences. Enabled, unused devices (such as AirPort and Bluetooth) are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > Network.
From the list of hardware devices, select AirPort.
Ensure the "Status" is set to "Off".
If the service is not set to off or removed, this is a finding.

Fix Text: Open System Preferences - > Network.
From the list of hardware devices, select AirPort.
Set this service to "Off" by clicking the gear sign and selecting "Turn service off".

Remove service if required by site requirements by clicking the minus sign.

Group ID (Vulid): V-25321
Group Title: OSX00390-Disable unused devices
Rule ID: SV-38536r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00390 M6
Rule Title: Unused hardware devices must be disabled for Bluetooth.

Vulnerability Discussion: It is recommended to disable unused hardware devices listed in Network preferences. Enabled, unused devices (such as AirPort and Bluetooth) are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Open System Preferences - > Network.
From the list of hardware devices, select Bluetooth.
Ensure the "Status" is set to "Inactive". If the service is not inactive or removed, this is a finding.

Fix Text: Open System Preferences - > Network.
From the list of hardware devices, select Bluetooth.
Set this service to "Inactive" by clicking the gear sign and selecting "Make Service Inactive". Remove service if required by site requirements by clicking the minus sign. (From the "Configure" pop-up menu, choose "Manually".)

Group ID (Vulid): V-25323
Group Title: OSX00395-Disable unused hardware Firewire
Rule ID: SV-38538r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00395 M6
Rule Title: Unused hardware devices must be disabled for Firewire.

Vulnerability Discussion: It is recommended to disable unused hardware devices listed in Network preferences. Enabled, unused devices (Firewire) are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > Network.
From the list of hardware devices, select Firewire.
Ensure the "Status" is set to "Inactive". If the service is not set to inactive or removed, this is a finding.

Fix Text: Open System Preferences - > Network.
From the list of hardware devices, select Firewire.
Set this service to "Inactive" by clicking the gear sign and selecting "Make Service Inactive". Remove service if required by site requirements by clicking the minus sign. (From the "Configure" pop-up menu, choose "Manually".)

Group ID (Vulid): V-25324
Group Title: OSX00400-Disable IPv6
Rule ID: SV-37247r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00400 M6
Rule Title: System Preferences must be securely configured so IPv6 is turned off if not being used.

Vulnerability Discussion: It is recommended to disable unused hardware devices listed in Network preferences. Enabled, unused devices are a security risk. Hardware is listed in Network preferences only if the hardware is installed in the computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences - > Network.
Click Advanced.
Click the TCP/IP tab.

Ensure "Configure IPv6" is set to "Off".

If the option is not set to "Off", this is a finding.

NOTE: This must be checked on all network interfaces.

Fix Text: Open System Preferences - > Network.
Click Advanced.
Click the TCP/IP tab and set "Configure IPv6" to "Off", if not actively being used.

NOTE: This must be disabled on each network interface.

Group ID (Vulid): V-25328
Group Title: OSX00420-Require password to wake computer
Rule ID: SV-38560r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00420 M6
Rule Title: A password must be required to wake a computer from sleep or screen saver.

Vulnerability Discussion: Require a password to wake a computer from sleep or screen saver. This helps prevent unauthorized access on unattended computers. Although there is a lock button for Security references, users do not need to be authorized as an administrator to make changes. Enable this password requirement for every user account on the computer.

Responsibility: System Administrator
IAControls: PESL-1

Check Content:
Open a terminal session and enter the following command.

defaults -currentHost read com.apple.screensaver askForPassword -int

If the action value is not set to "1", this is a finding.

Fix Text: Open a terminal session and enter the following command.

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

Group ID (Vulid): V-25329
Group Title: OSX00425-Disable automatic login
Rule ID: SV-37251r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00425 M6
Rule Title: Automatic login must be disabled.

Vulnerability Discussion: Disabling automatic login is necessary for any level of security. If automatic login is enabled, an intruder can log in without authenticating. Even automatically logging in with a restricted user account, it is still easier to perform malicious actions on the computer.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
1. Open System Preferences->Security.
2. Select General tab.
3. Ensure "Disable automatic login" option is checked. If option is not checked, this is a finding.

Fix Text: 1. Open System Preferences->Security.
2. Select General tab.

3. Select "Disable automatic login".

Group ID (Vulid): V-25330
Group Title: OSX00430-Require password to unlock System Panes
Rule ID: SV-37254r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00430 M6
Rule Title: A password must be required to unlock each System Preference Pane.

Vulnerability Discussion: Some system preferences are unlocked when logged in with an administrator account. By requiring a password, digital token, smart card, or biometric reader to unlock secure system preferences, this requires extra authentication.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Security.
2. Select General tab.
3. Ensure "Require password to unlock each System Preferences Pane" is checked. If option is not checked, this is a finding.

Fix Text: 1. Open System Preferences->Security.
2. Select General tab.

3. Select "Require password to unlock each System Preferences Pane".

Group ID (Vulid): V-25331
Group Title: OSX00435-Log out after X minutes of activity
Rule ID: SV-37262r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00435 M6
Rule Title: Automatic logout due to inactivity must be disabled.

Vulnerability Discussion: Although some might want to enable automatic logout based on inactivity, there are reasons why this feature should be disabled. First, it can disrupt workflow. Second, it can close applications or processes without approval (but a password-protected screen saver will not close applications). Third, because automatic logout can be interrupted, it provides a false sense of security.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Security.
2. Select General tab.
3. Ensure "Log out after x minutes of inactivity" is not checked. If it is checked, this is a finding.

Fix Text: 1. Open System Preferences->Security.
2. Select General tab.

3. Deselect "Log out after x minutes of inactivity".

Group ID (Vulid): V-25332
Group Title: OSX00440-Use secure virtual memory
Rule ID: SV-37263r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00440 M6
Rule Title: Secure virtual memory must be used.

Vulnerability Discussion: Use secure virtual memory. The system's virtual memory swap file stores inactive physical memory contents, freeing physical memory. By default on some systems, the swap file is unencrypted. This file can contain confidential data, such as documents and passwords. Using secure virtual memory will secure the swap file at a cost of slightly slower speed (because Mac OS X must encrypt and decrypt the secure swap file).

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
1. Open System Preferences->Security.
2. Select General tab.
3. Ensure "Use Secure Virtual Memory" is checked. If option is not checked, this is a finding.

Fix Text: 1. Open System Preferences->Security.
2. Select General tab.

3. Select "Use Secure Virtual Memory".

Group ID (Vulid): V-25333
Group Title: OSX00445-Disable remote control in IR receiver
Rule ID: SV-38561r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00445 M6
Rule Title: Remote control infrared receiver must be disabled.

Vulnerability Discussion: If not using a remote control, disable the infrared receiver. This prevents unauthorized users from controlling a computer through the infrared receiver.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
1. Open System Preferences->Security.
2. Select General tab.
3. Ensure "Disable remote control infrared receiver" is checked. If the option is not checked, this is a finding.

Fix Text: 1. Open System Preferences->Security.
2. Select General tab.
3. Select "Disable remote control infrared receiver".

Group ID (Vulid): V-25335
Group Title: OSX00455-Allow essential services through firewall
Rule ID: SV-38563r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00455 M6
Rule Title: Only essential services must be allowed through firewall.

Vulnerability Discussion: Allowing only essential services through the firewall alleviates the potential for unwanted services to run on the system, and cuts down on system usage.

Responsibility: System Administrator
IAControls: ECND-1

Check Content:
Open System Preferences->Security.

Select Firewall tab.

Select Advanced (firewall should be started).

Either "Block all incoming connections" should be checked or only essential services and applications should be allowed. If not, this is a finding.

Fix Text: Open System Preferences -> Security.

Select Firewall tab.

Select the Advanced button.

Check "Block all incoming connections" or remove any non-essential services and applications.

Group ID (Vulid): V-25337
Group Title: OSX00465-Enable Stealth Mode on the firewall
Rule ID: SV-37266r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00465 M6
Rule Title: Stealth Mode must be enabled on the firewall.

Vulnerability Discussion: Enable Stealth Mode to prevent the computer from sending responses to uninvited traffic.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

sudo ipfw print

If no line contains "deny icmp from any to me in icmptypes 8" or a more restrictive rule, this is a finding.

Fix Text: Open a terminal session and edit or create /Library/LaunchDaemons/org.freebsd.ipfw.plist and ensure it contains the following.

<?xml version="1.0" encoding="UTF-8"?>

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/ PropertyList-1.0.dtd"> <plist version="1.0">
<dict>
<key>Label</key>
<string>org.freebsd.ipfw</string>
<key>Program</key>
<string>/sbin/ipfw</string>
<key>ProgramArguments</key>
<array>
<string>/sbin/ipfw</string>
<string>/etc/ipfw.conf</string>
</array>
<key>RunAtLoad</key>
<true />
</dict>
</plist>
```

Edit or create /etc/ipfw.conf and ensure it contains the following line (the first number, a line number, may need to be changed if another line already begins with that number).

Add 20 deny icmp from any to me in icmptypes 8

Group ID (Vulid): V-25338
Group Title: OSX00470-DVD or CD Sharing
Rule ID: SV-37268r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00470 M6
Rule Title: DVD or CD Sharing must be disabled.

Vulnerability Discussion: DVD or CD sharing must be disabled because it allows users of other computers to remotely use the DVD or CD drive on a computer.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Open System Preferences->Sharing.
Ensure "DVD or CD Sharing" service does not have the "On" box checked. If the box is checked, this is a finding.

Fix Text: Open System Preferences->Sharing.

Uncheck the "On" box for "DVD or CD Sharing" service.

Group ID (Vulid): V-25339
Group Title: OSX00475-Screen Sharing
Rule ID: SV-37273r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00475 M6
Rule Title: Screen Sharing must be disabled.

Vulnerability Discussion: Screen sharing must be disabled because it allows users of other computers to remotely view and control the computer.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Open System Preferences->Sharing.
Ensure "Screen Sharing" service does not have the "On" box checked. If the box is checked, this is a finding.

Fix Text: Open System Preferences->Sharing.
Uncheck the "On" box for "Screen Sharing" service.

Group ID (Vulid): V-25340
Group Title: OSX00480-File Sharing
Rule ID: SV-37274r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00480 M6
Rule Title: File Sharing must be disabled.

Vulnerability Discussion: File sharing must be disabled because it gives users of other computers access to each user's Public folder.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "File Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.

2. Uncheck the "On" box for "File Sharing" service.

Group ID (Vulid): V-25341
Group Title: OSX00485-Printer Sharing
Rule ID: SV-37278r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00485 M6
Rule Title: Printer Sharing must be disabled.

Vulnerability Discussion: Printer sharing must be disabled because it allows other computers to access a printer connected to the computer.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "Printer Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.

2. Uncheck the "On" box for "Printer Sharing" service.

Group ID (Vulid): V-25342
Group Title: OSX00490-Web Sharing
Rule ID: SV-37282r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00490 M6
Rule Title: Web Sharing must be disabled.

Vulnerability Discussion: Web Sharing must be disabled because it allows a network user to view websites located in /Sites.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On'" box for "Web Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.

2. Uncheck the "On" box for "Web Sharing" service.

Group ID (Vulid): V-25343
Group Title: OSX00495-Remote Login
Rule ID: SV-37284r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00495 M6
Rule Title: Remote Login must be disabled.

Vulnerability Discussion: Remote Login must be disabled because it allows users to access the computer remotely.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "Remote Login" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.

2. Uncheck the "On" box for "Remote Login" service.

Group ID (Vulid): V-25346
Group Title: OSX00500-Remote Management
Rule ID: SV-37288r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00500 M6
Rule Title: Apple Remote Desktop must be disabled.

Vulnerability Discussion: Apple Remote Desktop must be disabled because it allows the computer to be accessed using Apple Remote Desktop.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Open System Preferences->Sharing.

Ensure the "On" box for "Remote Management" service is not checked. If the box is checked, this is a finding.

Fix Text: Open System Preferences->Sharing.

Uncheck the "On" box for "Remote Management" service.

Group ID (Vulid): V-25348
Group Title: OSX00505-Remote Apple Events
Rule ID: SV-37290r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00505 M6
Rule Title: Remote Apple Events must be disabled.

Vulnerability Discussion: Remote Apple Events must be disabled because it allows the computer to receive Apple events from other computers.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Open System Preferences->Sharing.

Ensure the "On" box for "Remote Apple Events" service is not checked. If the box is checked, this is a finding.

Fix Text: Open System Preferences->Sharing.

Uncheck the "On" box for "Remote Apple Events" service.

Group ID (Vulid): V-25349
Group Title: OSX00510-Xgrid Sharing
Rule ID: SV-37293r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00510 M6
Rule Title: Xgrid Sharing must be disabled.

Vulnerability Discussion: Xgrid Sharing must be disabled because it allows computers on a network to work together in a grid to process a job.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "Xgrid Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.
2. Uncheck the "On" box for "Xgrid Sharing" service.

Group ID (Vulid): V-25350
Group Title: OSX00515-Internet Sharing
Rule ID: SV-37296r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00515 M6
Rule Title: Internet Sharing must be disabled.

Vulnerability Discussion: Internet Sharing must be disabled because it allows other users to connect with computers on your local network, through your internet connection.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "Internet Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.
2. Uncheck the "On" box for "Internet Sharing" service.

Group ID (Vulid): V-25351
Group Title: OSX00520-Bluetooth Sharing
Rule ID: SV-37299r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00520 M6
Rule Title: Bluetooth Sharing must be disabled.

Vulnerability Discussion: Bluetooth Sharing must be disabled because it allows other Bluetooth-enabled computers and devices to share files with your computer.

Responsibility: System Administrator
IAControls: ECCD-1, ECWN-1

Check Content:
1. Open System Preferences->Sharing.
2. Ensure the "On" box for "Bluetooth Sharing" service is not checked. If the box is checked, this is a finding.

Fix Text: 1. Open System Preferences->Sharing.

2. Uncheck the "On" box for "Bluetooth Sharing" service.

Group ID (Vulid): V-25354
Group Title: OSX00525-Configure Mail using SSL
Rule ID: SV-38567r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00525 M6
Rule Title: Mail must be configured using SSL.

Vulnerability Discussion: When setting up user mail accounts, select "use SSL" in advanced options. This setting is for the Mail app included with OS X. Instructions will be different for other mail applications, but all mail applications should be set up secured using some form of encryption.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
NOTE: If you are not using the Mac Mail Application, this check does not apply.

Choose Mail > Preferences, and then click Accounts.
Select an account, and then click Advanced.
Ensure "Use SSL" is selected.
From the Authentication pop-up menu, ensure an authentication method is selected (e.g., MD5 Challenge-Response, NTLM, Kerberos Version 5 (GSSAPI), or Authenticated POP (APOP)).

If not, this is a finding.

Click Account Information.
From the Outgoing Mail Server (SMTP) pop-up menu, select Edit Server List.
From the server list, select the outgoing mail server, and then click Advanced.
Ensure Secure Socket Layer (SSL) is selected.
From the Authentication pop-up menu, ensure an authentication method is selected (e.g., MD5 Challenge-Response, NTLM, Kerberos Version 5 (GSSAPI), or Authenticated POP (APOP)).
If not, this is a finding.

Fix Text: Choose Mail > Preferences, Click Accounts.
Select an account, Click Advanced.
Select "Use SSL".
From the Authentication pop-up menu, select authentication method (e.g., MD5 Challenge-Response, NTLM, Kerberos Version 5 (GSSAPI), or Authenticated POP (APOP)).
Click Account Information.
From the Outgoing Mail Server (SMTP) pop-up menu, select Edit Server List.
From the server list, select your outgoing mail server and then click Advanced.
Select "Secure Socket Layer (SSL)".
From the Authentication pop-up menu, select authentication method (e.g., MD5 Challenge-Response, NTLM, Kerberos Version 5 (GSSAPI), or Authenticated POP (APOP)).
Close the preferences window, and then click "Save" in the message that appears.

Group ID (Vulid): V-25355
Group Title: OSX00530-Disable iTunes Store
Rule ID: SV-37301r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00530 M6
Rule Title: iTunes Store must be disabled.

Vulnerability Discussion: iTunes store allows a user to purchase and download music, videos, and podcasts, which could inadvertently introduce malware on the system. NOTE: The fix must be performed for each user.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open iTunes.
Choose iTunes -> Preferences.
Choose the "Parental" tab.
In the "Disable:" section, ensure the following items are checked.
"Podcasts"
"Radio streaming"
"iTunes Store"
"Allow Access to iTunesU"
"Ping" (if it exists)
"Shared Libraries"
If not, this is a finding.

Fix Text: Open Finder.
Select Applications.
Double click the iTunes application.
On the top menu bar click iTunes and from the drop down menu select Preferences.
Click on the Parental icon.
Check the following items to disable.
"Podcasts"
"Radio streaming"
"iTunes Store"
"Allow Access to iTunesU"
"Ping" (if it exists)
"Shared Libraries"

NOTE: This must be performed for each user.

Group ID (Vulid): V-25356
Group Title: OSX00535-Empty Trash securely
Rule ID: SV-37303r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00535 M6
Rule Title: Finder must be set to always empty Trash securely.

Vulnerability Discussion: In Mac OS X Finder can be configured to always securely erase items placed in the Trash. This prevents data placed in the Trash from being restored.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
1. Open Finder-> Preferences -> Advanced.
2. Ensure "Empty Trash Securely" is checked. If the option is not checked, this is a finding. This must be done for each user on the system.

Fix Text: 1. Open Finder-> Preferences -> Advanced.
2. Select "Empty Trash Securely".

This must be done for each user on the system.

Group ID (Vulid): V-25358
Group Title: OSX00540-Remove iDisk from Finder sidebar
Rule ID: SV-37308r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00540 M6
Rule Title: iDisk must be removed from Finder sidebar.

Vulnerability Discussion: iDisk data is stored on Internet servers and is protected by MobileMe account. However, if MobileMe account is accessed by an unauthorized user, data can be compromised. Do not store sensitive data on iDisk. Keep sensitive data local and encrypted on a computer.

Responsibility: System Administrator
IAControls: ECRC-1

Check Content:
1. Open Finder > Preferences > Sidebar.
2. Ensure the iDisk icon is not selected. If the option is selected, this is a finding.
This must be done for each user on the system.

Fix Text: 1. Open Finder -> Preferences -> Sidebar.
2. De-select the iDisk icon.

This must be done for each user on the system.

Group ID (Vulid): V-25371
Group Title: OSX00655-Securing the System Admin Account
Rule ID: SV-38568r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00655 M6
Rule Title: The root account must be disabled.

Vulnerability Discussion: The most powerful user account in Mac OS X is the system administrator or root account. By default, the root account on Mac OS X is disabled and it is recommended to not enable it. The root account is primarily used for performing UNIX commands. Generally, actions involving critical system files require performing those actions as root.

Responsibility: System Administrator
IAControls: IAAC-1

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Lock and enter the password to unlock the options.
Click the Edit menu (Directory Utility bar on top) and verify that "Enable Root User" appears. If the "Disable Root User" option is visible, this is a finding.

Fix Text: Open Finder
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.

Double Click Directory Utility.
Click the Lock and enter the password to unlock the options.
Click the Edit menu (Directory Utility bar on top).

Click Disable Root User.

Group ID (Vulid): V-25372
Group Title: OSX00660-Physical Security
Rule ID: SV-38583r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00660 M6
Rule Title: Physical security of the system must meet DoD requirements.

Vulnerability Discussion: Inadequate physical protection can undermine all other security precautions utilized to protect the system. This can jeopardize the confidentiality, availability, and integrity of the system. Physical security of the AIS is the first line protection of any system.
Physical security of the Automated Information System (AIS) must meet DoD requirements.

Responsibility: System Administrator
IAControls: PECF-2

Check Content:
Interview the SA to determine if equipment is located in a controlled access area.

Fix Text: Relocate equipment to a controlled access area.

Group ID (Vulid): V-25373
Group Title: OSX00665-Shared User Accounts
Rule ID: SV-37313r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00665 M6
Rule Title: Shared User Accounts must be disabled.

Vulnerability Discussion: Shared accounts do not provide individual accountability for system access and resource usage.
Shared user accounts are not permitted on the system.

Responsibility: System Administrator
IAControls: IAGA-1

Check Content:
Interview the SA to determine if any shared accounts exist. Any shared account must be documented with the IAO. Documentation should include the reason for the account,
who has access to this account, and how the risk of using a shared account (which provides no individual identification and accountability) is mitigated.

NOTE: As an example, a shared account may be permitted for a help desk or a site security personnel machine, if the machine is stand-alone and has no access to the network.

Fix Text: Remove any shared accounts not meeting the exception requirements listed.

Group ID (Vulid): V-25374
Group Title: OSX00670-Operating System Updates
Rule ID: SV-38569r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00670 M6
Rule Title: The Operating System must be current and at the latest release level.

Vulnerability Discussion: Failure to install the most current Operating System (OS) updates leaves a system vulnerable to exploitation. Current OS updates and patches correct known security and system vulnerabilities. If an OS is not at a supported level this will be upgraded to a Category I finding.

Severity Override Guidance:
If an OS is at an unsupported release level, this will be upgraded to a Category I finding since new vulnerabilities may not be patched.

Responsibility: System Administrator
IAControls: VIVM-1

Check Content:
Open a terminal session and enter one of the following commands.

sudo softwareupdate --list

OR

sudo softwareupdate --list --all

Review the results and verify the system is at the current release level. If not, this is a finding.

Fix Text: Install the current OS updates and patches.

Group ID (Vulid): V-25375
Group Title: OSX00675-System Recovery Backups
Rule ID: SV-37320r1_rule
Severity: CAT III
Rule Version (STIG-ID): OSX00675 M6
Rule Title: System Recovery Backup procedures must be configured to comply with DoD requirements.

Vulnerability Discussion: Recovery of a damaged or compromised system in a timely basis is difficult without a system information backup. A system backup will usually include sensitive information, such as user accounts that could be used in an attack. As a valuable system resource, the system backup should be protected and stored in a physically secure location.

Responsibility: System Administrator
IAControls: CODB-1

Check Content:
Interview the SA to determine if system recovery backup procedures are in place complying with DoD requirements.

Any of the following would be a finding:

• The site does not maintain emergency system recovery data.
• The emergency system recovery data is not protected from destruction and stored in a locked storage container.
• The emergency system recovery data has not been updated following the last system modification.

Fix Text: Implement data backup procedures complying with DoD requirements.

Group ID (Vulid): V-25376
Group Title: OSX00685-Emergency Administrator Account
Rule ID: SV-37322r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00685 M6
Rule Title: An Emergency Administrator Account must be created.

Vulnerability Discussion: This check verifies an emergency administrator account has been created to ensure system availability in the event no administrators are able or available to access the system.

Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
Interview the SA to determine if an emergency administrator account exists and is stored with its password in a secure location.

Fix Text: Create and maintain an emergency administrator account for emergency situations.

Group ID (Vulid): V-25377
Group Title: OSX00690-Administrator Account Password Changes
Rule ID: SV-37325r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00690 M6
Rule Title: Default and Emergency Administrator passwords must be changed when necessary.

Vulnerability Discussion: This check verifies the passwords for the default and emergency administrator accounts are changed at least annually or when any member of the administrative team leaves the organization.

Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
Interview the SA or IAM to determine if the site has a policy requiring the default and backup administrator passwords to be changed at least annually or when any member of the administrative team leaves the organization.

Fix Text: Define a policy for required password changes for the default and backup administrator account.

Group ID (Vulid): V-25378
Group Title: OSX00695-Application Account Passwords
Rule ID: SV-37329r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00695 M6
Rule Title: Application/service account passwords must be changed at least annually or whenever a system administrator with knowledge of the password leaves the organization.

Vulnerability Discussion: Setting application accounts to expire may cause applications to stop functioning. The site will have a policy for application account passwords manually generated and entered by a system administrator to be changed at least annually or when a system administrator with knowledge of the password leaves the organization. Application/service account passwords will be at least 15 characters and follow complexity requirements for all passwords.

Responsibility: System Administrator
IAControls: ECPA-1

Check Content:
The site should have a local policy ensuring passwords for application/service accounts are at least 15 characters in length and meet complexity requirements for all passwords. Application/service account passwords manually generated and entered by a system administrator must be changed at least annually or whenever a system administrator with knowledge of the password leaves the organization.

Interview the system administrators on their policy for application/service accounts. If it does not meet the above requirements, this is a finding.

Fix Text: Create application/service account passwords at least 15 characters in length and meet complexity requirements. Change of application/service account passwords are manually generated and entered by a system administrator at least annually or whenever an administrator with knowledge of the password leaves the

organization.

Group ID (Vulid): V-25379
Group Title: OSX00700-Automatic Screen Saver
Rule ID: SV-38572r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00700 M6
Rule Title: Automatic Screen Saver initiation must be enabled when smart card is removed from machine.

Vulnerability Discussion: When using a smart card for authentication the system must be configured to automatically lock the system when the smart card is removed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open System Preferences.
Click the Security Icon.
Click the General Tab.
Ensure "Activate screen saver when login token is removed" option is selected. If the option is not selected, this is a finding.

NOTE: If you are not using a smart card application, this check does not apply.
NOTE: This configuration option is still available if a smart card application is not installed.

Fix Text: Open System Preferences.
Click the Security Icon.
Click the General Tab.
Select "Activate screen saver when login token is removed".

Group ID (Vulid): V-25380
Group Title: OSX00680
Rule ID: SV-38570r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00680 M6
Rule Title: Access to audit configuration files must be restricted.

Vulnerability Discussion: Audit configuration files are susceptible to unauthorized, and possibly anonymous, tampering if proper permissions are not applied.

Responsibility: System Administrator
IAControls: ECTP-1

Check Content:
Open a terminal session and enter the following command to view the permissions on the audit control files.

ls -lL /etc/security

If any audit control file has a permission less restricted than 555, this is a finding.

Fix Text: Open a terminal session and enter the following command to set the file permissions.

chmod 555 /etc/security/ <audit control file>

Group ID (Vulid): V-25413
Group Title: OSX00705-Securely configure Spotlight Panel
Rule ID: SV-37331r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00705 M6
Rule Title: Spotlight Panel must be securely configured.

Vulnerability Discussion: Spotlight can be used to search a computer for files. Spotlight searches the name, the meta-information associated with each file, and the contents of each file. Spotlight finds files regardless of their placement in the file system. This still must be properly set access permissions on folders containing confidential files.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
To securely configure Spotlight preferences:
Open System Preferences.
Click the Spotlight Icon.
In the Search Results pane, verify the categories not wanted as searchable by Spotlight are unchecked.
Click the Privacy pane.
Verify the correct folders and disks are in the Privacy pane; these are not searchable by Spotlight.

If searchable categories or folders are found that should not be searchable, this is a finding.

Fix Text: To securely configure Spotlight preferences:
Open System Preferences.
Click the Spotlight Icon.
In the Search Results pane, deselect categories not wanted searchable by Spotlight.
Click the Privacy pane.

Click the Add button or drag a folder or disk into the Privacy pane.

Folders and disks in the Privacy pane are now not searchable by Spotlight.

Group ID (Vulid): V-25557
Group Title: OSX00121-Disable clear text passwords for all LDAP
Rule ID: SV-38573r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00121 M6
Rule Title: Clear text passwords for all LDAPv3 directories must be disabled.

Vulnerability Discussion: Allowing passwords to be transmitted over the network in clear text could allow an attacker to monitor the network and capture the password packets. This clear text function must be disabled when accessing LDAPv3 directories.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and verify the "Disable clear text passwords" is checked. If the value is not checked, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.

Click the Security tab and select "Disable clear text passwords".

Group ID (Vulid): V-25559
Group Title: OSX00122-Digitally sign all LDAPv3 packets
Rule ID: SV-38575r1_rule
Severity: CAT II

Rule Version (STIG-ID): OSX00122 M6
Rule Title: All LDAPv3 packets must be digitally signed.

Vulnerability Discussion: To protect the data between the client and LDAPv3 directory the traffic should be digitally signed.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and verify the "Digitally sign all packets (requires Kerberos) " is checked. If the value is not checked, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and select "Digitally sign all packets (requires Kerberos)".

Group ID (Vulid): V-25561
Group Title: OSX00123-Encrypt all LDAPv3 packets
Rule ID: SV-38577r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00123 M6
Rule Title: All LDAPv3 packets must be encrypted.

Vulnerability Discussion: All traffic between the client and the LDAPv3 should be encrypted to ensure confidentiality of data.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.

Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and verify the "Encrypt all packets (requires SSL or Kerberos) " is checked. If the value is not checked, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and select "Encrypt all packets (requires SSL or Kerberos)".

Group ID (Vulid): V-25563
Group Title: OSX00124-LDAPv3 Block man-in-the-middle attacks
Rule ID: SV-38578r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00124 M6
Rule Title: LDAPv3 must block man-in-the-middle attacks.

Vulnerability Discussion: To prevent LDAPv3 man-in-the middle attacks the system must be properly configured.

Responsibility: System Administrator
IAControls: ECCT-1, ECCT-2

Check Content:
Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click on Security tab and verify the "Block man-in-the-middle attacks (requires Kerberos)" is checked. If the value is

not checked, this is a finding.

Fix Text: Open Finder.
Click the Hard Drive icon.
Double Click System.
Double Click Library.
Double Click CoreServices.
Double Click Directory Utility.
Click the Show Advanced Options button.
Click Services tab.
Click the Lock and enter the password to unlock the options (if needed).
Click the LDAPv3 service.
Click the Pencil icon.
Highlight the Server Name/Configuration Name.
Click Edit.
Click the Security tab and select "Block man-in-the-middle attacks (requires Kerberos)".

Group ID (Vulid): V-25606
Group Title: OSX00341-automatic actions for blank DVD
Rule ID: SV-37333r1_rule
Severity: CAT I
Rule Version (STIG-ID): OSX00341 M6
Rule Title: Automatic actions must be disabled for blank DVDs.

Vulnerability Discussion: To secure CDs and DVDs (blank), do not allow the computer to perform automatic actions when the user inserts a disc. When disabling automatic actions in System Preferences, these actions must be disabled for every user account on the computer.

Responsibility: System Administrator
IAControls: ECCD-1

Check Content:
Open a terminal session and enter the following command.

defaults read /Library/Preferences/com.apple.digihub com.apple.digihub.blank.dvd.appeared -dict

If the action value is not set to "1", this is a finding.

Fix Text: Open a terminal session and enter the following command.

defaults write /Library/Preferences/com.apple.digihub com.apple.digihub.blank.dvd.appeared -dict action 1

Group ID (Vulid): V-25882
Group Title: OSX00467-Disable Bonjour
Rule ID: SV-38581r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00467 M6
Rule Title: Bonjour must be disabled.

Vulnerability Discussion: Bonjour is unnecessary in a managed environment and presents an attack surface. Its

behavior, which trusts the local network, is especially inappropriate on portable devices which may connect to untrusted networks.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a terminal session and enter the following command.

sudo ipfw print.

If no line contains "deny udp from any to me dst-port 5353" or a more restrictive rule, this is a finding.

Fix Text: Open a terminal session and edit or create /Library/LaunchDaemons/org.freebsd.ipfw.plist and ensure it contains the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/ PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
        <string>org.freebsd.ipfw</string>
    <key>Program</key>
        <string>/sbin/ipfw</string>
    <key>ProgramArguments</key>
        <array>
            <string>/sbin/ipfw</string>
            <string>/etc/ipfw.conf</string>
        </array>
    <key>RunAtLoad</key>
        <true />
</dict>
</plist>
```

Edit or create /etc/ipfw.conf and ensure it contains the following line (the first number, a line number, may need to be changed if another line already begins with that number):

Add 10 deny udp from any to me dst-port 5353

Group ID (Vulid): V-29437
Group Title: Complex passwords must be created Alpha check
Rule ID: SV-38603r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00036 M6
Rule Title: Complex passwords must contain Alphabetic Character.

Vulnerability Discussion: Configure the local system to verify newly created passwords conform to DoD password complexity policy. Passwords must contain 1 character from the following 4 classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Sites are responsible for installing password complexity software complying with the current DoD requirements.

Responsibility: System Administrator
IAControls: IAIA-1

Check Content:
Open a terminal session and run the following command.

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

If the value of requiresAlpha is not set to 1, this is a finding.

NOTE: If the command returns a response of: password server is not configured, the system is not managed. Add the path /Local/Default to the above command, an example would be: pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep requiresAlpha

Fix Text: Open a terminal session and run the following command.

sudo pwpolicy -n -setglobalpolicy "requiresAlpha=1"

For non managed systems the path /Local/Default would need to be added to the command, an example would be:

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

Group ID (Vulid): V-29439
Group Title: Complex passwords must be created symbol check
Rule ID: SV-38607r1_rule
Severity: CAT II
Rule Version (STIG-ID): OSX00038 M6
Rule Title: Complex passwords must contain a Symbolic Character.

Vulnerability Discussion: Configure the local system to verify newly created passwords conform to the DoD password complexity policy. Passwords must contain 1 character from the following 4 classes: English uppercase letters, English lowercase letters, Westernized Arabic numerals, and non-alphanumeric characters. Sites are responsible for installing password complexity software that complies with current DoD requirements.

Responsibility: System Administrator
IAControls: IAIA-1

Check Content:
Open a terminal session and run the following command.

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

If the value of requireSymbol is not set to 1, this is a finding.

NOTE: If the command returns a response of password server is not configured, the system is not managed. Add the path /Local/Default to the above commands, an example would be: pwpolicy -n /Local/Default -getglobalpolicy | tr " " "\n" | grep requiresSymbol

Fix Text: Open a terminal session and run the following command.

sudo pwpolicy -n -setglobalpolicy "requiresSymbol=1"

For non managed systems the path /Local/Default would need to be added to the command, an example would be:

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