This page lists all the known findings and mitigations from SECSCN reports generated from a configured HWW system.

Contents

Findings and Mitigations

L1.5

Finding
: Left-over audit configuration files found.

Description
: Ensure that audit data is not stored on critical system partitions

Mitigation
: This is a false positive, no system changes are necessary. If needed, run ?df ?h? and show that /var (containing audit data) is in a separate partition.

L1.7

Finding
: Audit log file and directory permissions are NOT correct

Description
: Check ownership and permissions of audit log directories and file

Mitigation
: /var/log/audit/save, /var/log/audit/hold/, /var/log/audit/purge are directories with permission 700 in order for our logrotation functionality to work.

L1.10

Finding
: Audit data is NOT synchronously flushed to disk.

Description
: Verify that audit data is synchronously flushed to disk to avoid data loss.

Mitigation
: The system is configured to incrementally flushed every 20 audits to minimize chance of losing audit data.. This setting can be changed but may impact performance of the system.

L1.11

Finding
: Notification for low disk space NOT enabled.

Description
: Check that administrators are notified on disk space low.

Mitigation
: The HardwareWall? CI is a Controlled Interface and does not have email services configured. It is appropriate to direct low disk space notifications to SYSLOG.

L1.12

Finding
: Notification for no disk space NOT enabled.

Description
: Check that administrators are notified on disk space critical.

Mitigation

The HardwareWall? CI is a Controlled Interface and does not have email services configured. It is appropriate to direct no disk space notifications to SYSLOG.

L1.13

Finding
: Notification email address is NOT set.

Description
: Check that administrators are notified on disk full.

Mitigation
: The HardwareWall? CI is a Controlled Interface and does not have email services configured. This setting has no effect.

L1.15

Finding
: Auditing rules in audit.rules are not immutable

Description
: Check if auditing rules in /etc/audit/audit.rules are immutable

Mitigation
: The ?e flag has been modified in /etc/audit/audit.rules to render the audit rules immutable.(-e 1) means that the audit rules are enabled and (-e 2) means that the audit rules cannot be modified without a reboot. So the setting could be site's security dependent.

L1.17

Finding
: The System is not configured to record events that modify the system?s data or time

Description
: Ensure that the system is configured to record events that modify the system's date or time.

Mitigation
: This is a false positive, no system changes are necessary. Time changes are monitored (search for "FPT_STM.1" in audit.rules to find the appropriate rules). SECSCN greps for an exact string and our rules are slightly different.

L1.18

Finding
: The system is not configured to record events that modify accounts on the system

Description
: Ensure that the system is configured to record events that modify accounts on the system.

Mitigation
: The HardwareWall audit rules do record events that modify accounts on the system (Look for "password" in our audit rules). The SECSCN tool is looking for the incorrect audit tag.

L1.19

Finding
: The system is not configured to record events that modify network settings.

Description
: Ensure that the system is configured to record events that modify network settings.

Mitigation

This is a false positive, no system changes are necessary. Network setting changes are monitored (search audit.rules for ?issue?, "hosts" and "/etc/sysconfig" if you need to locate our rules). SECSCN greps for an exact string and our rules are slightly different (ours are in fact more secure).

L1.20

Finding

The system is not configured to record events that modify MAC policy

Description

Ensure that the system is configured to record events that modify MAC policy

Mitigation

This is a false positive, the HardwareWall audid.rules does record events that modify MAC policy. The SECSCAN tool is looking and grepping for a different SElinux path

L1.21

Finding

The system is not configured to record logon and logout events

Description

Ensure that the system is configured to record logon and logout events.

Mitigations

The current set of audit rules does record logon and logout events(search audit.rules for ?faillog" and "lastlog" if you need to locate our rules). The rules were modified to only audit unsuccessful logon events of Ticom?s software processes, as those successful events would quickly fill up the audit trails. The SECSCN tool is looking for the incorrect audit tag (the ?k flag).

L1.22

Finding

The system is not configured to record process and session information

Description

Ensure that the system is configured to record process and session information

Mitigations

The HardwareWall does not use the utmp, btmp and wtmp directories.

L1.23

Finding

The system is not configured to record file permission changes for all users and root

Description

Ensure that the system is configured to record file permission changes for all users and root.

Mitigations

The current set of audit rules does record file permission changes, but is tailored to ignore the successful changes by the HardwareWall software. The HardwareWall processes a large amount of files, which involves changing file permissions to allow each component exclusive access. Auditing these successful events would produce too much noise in the audit trails.

L1.24

Finding

The system is not configured to record unauthorized file accesses

Description

Ensure that the system is configured to record unauthorized file accesses.

Mitigations

The current set of audit rules does record unauthorized file accesses (search audit.rules for "truncate"). The SECSCN tool is looking for the incorrect audit tag (the ?k flag).Furthermore, the audit rules audit both 32-bit and 64-bit system calls. The Hardwarewall does not audit successful opens because it would produce too much noise in the audit trails.

L1.25

Finding

The system is not configured to record execution of privileged commands

Description

Ensure that the system is configured to record execution of privileged commands

Mitigations

The current set of audit rules does record privileged commands used by the system (search audit.rules for "privileged" if you need to locate our rules). The SECSCAN tool greps for an exact string that is slightly different in our rules

L1.26

Finding

The system is not configured to record media exportation events.

Description

Ensure that the system is configured to record media exportation events.

Mitigation

This is a false positive, no system changes are necessary. Network setting changes are monitored (search audit.rules for search for "mount" if you need to locate our rules). SECSCN greps for an exact string and our rules are slightly different (ours are in fact more secure).

L1.27

Finding

The system is not configured to record file deletion events

Description

Ensure that the system is configured to record file deletion events.

Mitigation

The current set of audit rules does record file deletion events, but is tailored to ignore the successful deletions by the HardwareWall software (search audit.rules for "delete" if you need to locate our rules). The HardwareWall processes a large amount of files, which involves creating and deleting temporary files. Auditing these successful events would produce too much noise in the audit trails.

L1.28

Finding

The system is not configured to record system administrator actions

Description

Ensure that the system is configured to record system administrator actions (search audit.rules for "sudoers" if you need to locate our rules).

Mitigation

The current set of audit rules does record system administrator actions. The SECSCN tool is looking for the incorrect audit tag (the ?k flag).

L2.4

Finding

Critical system file permissions require hardening

Description

Verify permissions are not more permissible than the expected results for system critical files (if exists).

Mitigation

The permissions for system critical files were changed to not be more permissible than the expected results, except for the following cases: Removing the root executable bit from /etc/rc.d/rc.local and /etc/rc.local would interfere with the startup of critical system daemons /var/log/wtmp (root:utmp:0664) and /var/log/dmesg(root:root:0644) are system-critical files whose permissions are set by RedHat provided startup processes.

L2.5

Finding

Critical system file permissions require hardening

Description

Verify permissions are not more permissible than the expected results for system critical directories (if exists).

Mitigation

The permissions for system critical directories were changed to not be more permissible than the expected results, except for the following cases:

Removing the search bit from /usr/share/doc and /usr/share/man would prevent users from accessing system documentation such as man pages. Removing the search bit from /var/log/audit would interfere with automated log and audit rotation on the system. The SELinux policy will still prevent unauthorized access to the contents of /var/log/audit

L2.6

Finding

Identified 1 world writable file on the system

Description

Determine if there are any world writable files on the system.

Mitigation

The world-writable files found were from system integration activities and have been removed.

L2.7

Finding

Identified 5 world writable directories on the system

Description

Determine if there are any world writable directories

Mitigation

The world-writable directories are temporary directories that have the sticky bit set. This is a security measure to avoid deletion of Linux critical folders and their content(sub-folders and files).

L2.8

Finding

Identified 3 file or directories owned by non-existent UID's on the system.

Description

Determine if there are any files or directories owned by non-existent user ids on the system.

Mitigation

If directories are not needed by the system, then they will need to be removed.

L2.10

Finding

Identified 22 Set-UID executables on the system. Manual review required to ensure there are no unknown Root Set-UID's on the system. The Root Set-UID file listing must be documented in the TFM.

Description

Determine if there are any Root Set-UID executables on the system.

Mitigation

All SUID system executables are the expected set provided by RedHat.

L2.12

Finding

Identified 7 Set-GID binaries on the system. Manual review required to ensure there are no unknown Set-GID files on the system. The Set-GID file listing must be documented in the TFM.

Description

Determine if there are any Set-GID binaries on the system.

Mitigation

All SGID system executables are the expected set provided by RedHat and eXMeritus.

L2.13

Finding

Identified 71 non-stripped binaries on the system. Manual review required to ensure there are no unknown non-stripped binaries on the system. The non-stripped binary listing must be documented in the TFM.

Description

Non-stripped binaries

Mitigation

The HardwareWall binaries are left non-stripped to assist in technical support and provide debugging information.

L2.16

Finding

The default system UMASK is not set securely.

Description

Verify system default umask is set properly.

Mitigation

The umask for users is set to 077 in /etc/profile.d/exmeritus.sh.

L2.17

Finding

The following files have weak desault user UMASKs set: /etc/profile, /etc/profile

Description

Ensure users have more secure umask values by checking values defined in the following files: /etc/profile, /etc/csh.login, /etc/csh.cshrc, /etc/bashrc, /root/.bash_profile, /root/.bashrc, /root/.cshrc, /root/.tcshrc

Mitigation

The umask for users is set to 077 in /etc/profile.d/exmeritus.sh.

L2.18

Finding

Partitions in the /etc/fstab file do not have the "nodev" option.

Description

Verify nodev options are set properly in the /etc/fstab file.

Mitigation

The ?nodev? option is not set for the partitions hosting the chroot services, as that would disrupt the operations of the baseline chroot services.

L2.19

Finding

Partitions in the /etc/fstab file do not have the ?nosuid? option

Description

Verify nosuid options are set properly in the /etc/fstab file

Mitigation

The nosuid option is not invoked on specific mount points used by the HardwareWall to explicitly allow for use of setuid commands within those partitions and is required for the correct operation of the HardwareWall processes.

L2.21

Finding

Single user mode is not password protected

Description

Verify single user mode is password protected.

Mitigation

This is a false positive. Single user behavior is no longer configured in /etc/inittab on RHEL6. Run "grep sulogin /etc/sysconfig/init" and observe that sulogin will be run in single user mode.

single user behavior is no longer configured in /etc/inittab on RHEL6. Run "grep sulogin /etc/sysconfig/init" and observe that sulogin will be run in single user mode.

L2.22

Finding

Interactive boot is enabled.

Description

Verify interactive boot is disabled.

Mitigation

This is a false positive. The SECSCN tool is looking for the exact "PROMPT=no" and it is actually needs to be "PROMPT="no"" in the file.

L3.2

Finding

Insecure services are enabled presenting a potential security risk.

Description

Identify each ?active? service listed by the chkconfig --list command.

Mitigation

mcstrans is a service that should be enabled as category labeling is used extensively in the MLS policy used by the HardwareWall. Any non-essential service should be deactivated and update SDD

L3.3

Finding

Finding: FTP is enabled and access is not appropriately restricted

Description

Verify existence of /etc/vsftp/ftpusers (or may be /etc/ftpusers).

Mitigation

If vsftp is not used by the system, this is a false positive as FTP access is disabled and the file will not exist. If vsftp is used by the system, the file will be under vsftpd_netA.users in /HardwareWall/Configuration/<host>/

L3.4

Finding

Finding: FTP is enabled and access is not appropriately restricted

Description

Verify system/privileged accounts are disallowed ftp login privileges.

Mitigation

If vsftp is not used by the system, this is a false positive as FTP access is disabled and the file will not exist. If vsftp is used by the system, the file will be under vsftpd_netA.users in /HardwareWall/Configuration/<host>/

L5.5

Finding

X Server is not configured to prevent listening on port 6000/tcp

Description

Ensure X server is configured to prevent listening on port 6000/tcp

Mitigation

None of the X server packages are installed on the system.

L6.1

Finding

The system does not meet the individual accountability requirements as stated in DCID 6/3 4.B.2.a(7) I&A2; JDCSISSS 6.3.1

Description

Identify system accounts

Mitigation

All existing system accounts are necessary for the operations of the system. Non-essential accounts, such as the user ?ftp?, have been removed.

L7.3

Finding

The rp_filter setting requires hardening./sbin/sysctl net.ipv4.conf.all.rp_filter is set to 0 instead of 1

Description

Check the rp_filter setting.

Mitigation

This should be fixed in /etc/shorewall.conf where ROUTE_FILTER should be equal to "Yes" and after restarting shorewall service. If already set to 1 when doing a cat /proc/sys/net/ipv4/conf/default/rp_filter, then this is a false positive

L7.7

Finding

The rp_filter setting requires hardening. /sbin/sysctl net.ipv4.conf.default.rp_filter is set to 0 instead of 1

Description

Check the rp_filter setting

Mitigation

This should be fixed in /etc/shorewall.conf where ROUTE_FILTER should be equal to "Yes" and after restarting shorewall service. If already set to 1 when doing a cat /proc/sys/net/ipv4/conf/default/rp_filter, then this is a false positive.

L7.15

Finding

The /etc/xinetd.conf file is not properly configured to restrict access to local subnets.

Description

Ensure xinetd is configured to restrict access to appropriate subnets if installed.

Mitigation

Xinetd is not installed on the HardwareWall.

L8.1

Finding

The /etc/motd file exists but may not present the proper DoD statutory warning message.

Description

Verify appropriate warning banners are in place for xterm launch and logon.

Mitigation

The xterm package is not installed on the HardwareWall.

L8.2

Finding

The file /etc/issue exists but may not contain a recommended DoD statutory warning message.

Description

Verify appropriate warning banners are in place for xterm launch and login. Also, telnet and ftp banners.

Mitigation

The xterm package is not installed and in use. Telnet is disabled on the HardwareWall. The chrooted FTP service does use the latest provided logon banners.

L8.3

Finding

The file /etc/issue.net exists but may not contain a recommended DoD statutory warning message.

Description

Verify appropriate warning banners are in place for xterm launch and login. Also, telnet and ftp banners.

Mitigation

The xterm package is not installed and in use. Telnet is disabled on the HardwareWall. The chrooted FTP service does use the latest provided logon banners.

L8.4

Finding

The system does not have the /usr/share/gdm/themes/RHEL/RHEL.xml file to present a DoD statutory warning message at login time

Description

Verify warnings for GUI-based logins.

Mitigation

GUI packages are not installed on the system, so the HardwareWall does not provide GUI-based logon. Console logon does use the latest provided banners.

L10.1

Finding

Manual Review of the installed software packages. Ensure that only the required packages are installed on the system.

Description

Identify all packages installed on the system.

Mitigation

All packages on the system has been identified and deemed necessary for system operation.