

CIS Red Hat Enterprise Linux 5 Benchmark

v2.2.1 - 12-21-2020

Terms of Use

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

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

Table of Contents

Terms of Use	1
Overview	12
Intended Audience.....	12
Consensus Guidance.....	12
Typographical Conventions	14
Assessment Status.....	14
Profile Definitions	15
Acknowledgements	16
Recommendations.....	17
1 Install Updates, Patches and Additional Security Software	17
1.1 Filesystem Configuration	18
1.1.1 Create Separate Partition for /tmp (Automated).....	19
1.1.2 Set nodev option for /tmp Partition (Automated).....	21
1.1.3 Set nosuid option for /tmp Partition (Automated).....	22
1.1.4 Set noexec option for /tmp Partition (Automated)	24
1.1.5 Create Separate Partition for /var (Automated)	25
1.1.6 Bind Mount the /var/tmp directory to /tmp (Automated).....	27
1.1.7 Create Separate Partition for /var/log (Automated).....	29
1.1.8 Create Separate Partition for /var/log/audit (Automated).....	30
1.1.9 Create Separate Partition for /home (Automated).....	31
1.1.10 Add nodev Option to /home (Automated)	32
1.1.11 Add nodev Option to Removable Media Partitions (Manual)	34
1.1.12 Add noexec Option to Removable Media Partitions (Manual)	35
1.1.13 Add nosuid Option to Removable Media Partitions (Manual).....	37
1.1.14 Add nodev Option to /dev/shm Partition (Automated)	39
1.1.15 Add nosuid Option to /dev/shm Partition (Automated).....	41
1.1.16 Add noexec Option to /dev/shm Partition (Automated).....	43
1.1.17 Set Sticky Bit on All World-Writable Directories (Automated).....	45
1.1.18 Disable Mounting of cramfs Filesystems (Automated)	47

1.1.19	Disable Mounting of freevxfs Filesystems (Automated)	49
1.1.20	Disable Mounting of jffs2 Filesystems (Automated)	51
1.1.21	Disable Mounting of hfs Filesystems (Automated)	53
1.1.22	Disable Mounting of hfsplus Filesystems (Automated)	55
1.1.23	Disable Mounting of squashfs Filesystems (Automated)	57
1.1.24	Disable Mounting of udf Filesystems (Automated)	59
1.2	Configure Software Updates	61
1.2.1	Configure Connection to the RHN RPM Repositories (Manual)	62
1.2.2	Verify Red Hat GPG Key is Installed (Automated)	63
1.2.3	Verify that gpgcheck is Globally Activated (Automated)	65
1.2.4	Disable the rhnsd Daemon (Manual)	66
1.2.5	Disable yum-updatesd (Automated)	68
1.2.6	Obtain Software Package Updates with yum (Manual)	69
1.2.7	Verify Package Integrity Using RPM (Manual)	70
1.3	Advanced Intrusion Detection Environment (AIDE)	72
1.3.1	Install AIDE (Automated)	73
1.3.2	Implement Periodic Execution of File Integrity (Automated)	75
1.4	Configure SELinux	77
1.4.1	Enable SELinux in /etc/grub.conf (Automated)	78
1.4.2	Set the SELinux State (Automated)	80
1.4.3	Set the SELinux Policy (Automated)	82
1.4.4	Remove SETroubleshoot (Automated)	84
1.4.5	Disable MCS Translation Service (mcstrans) (Automated)	85
1.4.6	Check for Unconfined Daemons (Automated)	86
1.5	Secure Boot Settings	87
1.5.1	Set User/Group Owner on /etc/grub.conf (Automated)	88
1.5.2	Set Permissions on /etc/grub.conf (Automated)	89
1.5.3	Set Boot Loader Password (Automated)	91
1.5.4	Require Authentication for Single-User Mode (Automated)	93
1.5.5	Disable Interactive Boot (Automated)	94

1.6 Additional Process Hardening	95
1.6.1 Restrict Core Dumps (Automated).....	96
1.6.2 Configure ExecShield (Automated).....	98
1.6.3 Enable Randomized Virtual Memory Region Placement (Automated)	99
1.6.4 Enable XD/NX Support on 32-bit x86 Systems (Automated).....	101
1.6.5 Disable Prelink (Automated).....	103
1.7 Use the Latest OS Release (Manual).....	104
2 OS Services	106
2.1 Remove Legacy Services.....	107
2.1.1 Remove telnet-server (Automated).....	108
2.1.2 Remove telnet Clients (Automated)	110
2.1.3 Remove rsh-server (Automated).....	112
2.1.4 Remove rsh (Automated).....	113
2.1.5 Remove NIS Client (Automated)	115
2.1.6 Remove NIS Server (Automated).....	117
2.1.7 Remove tftp (Automated).....	119
2.1.8 Remove tftp-server (Automated)	121
2.1.9 Remove talk (Automated)	123
2.1.10 Remove talk-server (Automated)	124
2.1.11 Remove xinetd (Automated).....	125
2.1.12 Disable chargen-dgram (Automated).....	127
2.1.13 Disable chargen-stream (Automated).....	128
2.1.14 Disable daytime-dgram (Automated).....	129
2.1.15 Disable daytime-stream (Automated).....	130
2.1.16 Disable echo-dgram (Automated).....	131
2.1.17 Disable echo-stream (Automated).....	132
2.1.18 Disable tcpmux-server (Automated).....	133
3 Special Purpose Services	134
3.1 Disable Avahi Server	135
3.1.1 Disable Avahi Server (Automated).....	136

3.1.2 Service Only via Required Protocol (Manual).....	138
3.1.3 Check Responses TTL Field (Automated)	140
3.1.4 Prevent Other Programs from Using Avahi's Port (Manual)	141
3.1.5 Disable Publishing (Automated)	142
3.1.6 Restrict Published Information (if publishing is required) (Manual)	144
3.2 Set Daemon umask (Automated).....	146
3.3 Remove X Windows (Automated).....	147
3.4 Disable Print Server - CUPS (Manual)	149
3.5 Remove DHCP Server (Manual)	151
3.6 Configure Network Time Protocol (NTP) (Automated)	152
3.7 Remove LDAP (Automated)	154
3.8 Disable NFS and RPC (Automated)	155
3.9 Remove DNS Server (Automated).....	157
3.10 Remove FTP Server (Automated).....	158
3.11 Remove HTTP Server (Automated)	159
3.12 Remove Dovecot (IMAP and POP3 services) (Automated)	160
3.13 Remove Samba (Automated).....	161
3.14 Remove HTTP Proxy Server (Automated)	162
3.15 Remove SNMP Server (Automated).....	163
3.16 Configure Mail Transfer Agent for Local-Only Mode (Automated)	164
4 Network Configuration and Firewalls	166
4.1 Modify Network Parameters (Host Only).....	167
4.1.1 Disable IP Forwarding (Automated)	168
4.1.2 Disable Send Packet Redirects (Automated).....	170
4.2 Modify Network Parameters (Host and Router).....	172
4.2.1 Disable Source Routed Packet Acceptance (Automated)	173
4.2.2 Disable ICMP Redirect Acceptance (Automated)	175
4.2.3 Disable Secure ICMP Redirect Acceptance (Automated).....	177
4.2.4 Log Suspicious Packets (Automated)	179
4.2.5 Enable Ignore Broadcast Requests (Automated)	181

4.2.6 Enable Bad Error Message Protection (Automated).....	183
4.2.7 Enable RFC-recommended Source Route Validation (Automated)	185
4.2.8 Enable TCP SYN Cookies (Automated)	187
4.3 Wireless Networking	189
4.3.1 Deactivate Wireless Interfaces (Manual).....	190
4.4 Disable IPv6.....	191
4.4.1 Configure IPv6.....	192
4.4.1.1 Disable IPv6 Router Advertisements (Automated)	193
4.4.1.2 Disable IPv6 Redirect Acceptance (Automated)	195
4.4.2 Disable IPv6 (Manual).....	197
4.5 Install TCP Wrappers.....	198
4.5.1 Install TCP Wrappers (Automated)	199
4.5.2 Create /etc/hosts.allow (Automated).....	201
4.5.3 Verify Permissions on /etc/hosts.allow (Automated)	202
4.5.4 Create /etc/hosts.deny (Automated).....	203
4.5.5 Verify Permissions on /etc/hosts.deny (Automated).....	204
4.6 Uncommon Network Protocols	205
4.6.1 Disable DCCP (Automated)	206
4.6.2 Disable SCTP (Automated)	208
4.6.3 Disable RDS (Automated)	210
4.6.4 Disable TIPC (Automated).....	211
4.7 Enable IPtables (Automated).....	212
4.8 Enable IP6tables (Automated)	213
5 Logging and Auditing.....	214
5.1 Configure Syslog	215
5.1.1 Configure /etc/syslog.conf (Manual)	216
5.1.2 Create and Set Permissions on syslog Log Files (Automated)	218
5.1.3 Configure syslog to Send Logs to a Remote Log Host (Automated)	220
5.1.4 Accept Remote syslog Messages Only on Designated Log Hosts (Manual).222	
5.2 Configure rsyslog.....	224

5.2.1 Install the rsyslog package (Automated)	225
5.2.2 Activate the rsyslog Service (Automated)	227
5.2.3 Configure /etc/rsyslog.conf (Manual)	228
5.2.4 Create and Set Permissions on rsyslog Log Files (Automated).....	230
5.2.5 Configure rsyslog to Send Logs to a Remote Log Host (Automated)	232
5.2.6 Accept Remote rsyslog Messages Only on Designated Log Hosts (Manual)	234
5.3 Configure System Accounting (auditd).....	236
5.3.1 Configure Data Retention	237
5.3.1.1 Configure Audit Log Storage Size (Manual)	238
5.3.1.2 Disable System on Audit Log Full (Manual)	239
5.3.1.3 Keep All Auditing Information (Automated)	240
5.3.2 Enable auditd Service (Automated).....	241
5.3.3 Keep All Auditing Information (Automated).....	242
5.3.4 Enable Auditing for Processes That Start Prior to auditd (Automated).....	243
5.3.5 Record Events That Modify Date and Time Information (Automated)	245
5.3.6 Record Events That Modify User/Group Information (Automated).....	247
5.3.7 Record Events That Modify the System's Network Environment (Automated)	249
5.3.8 Record Events That Modify the System's Mandatory Access Controls (Automated).....	252
5.3.9 Collect Login and Logout Events (Automated).....	254
5.3.10 Collect Session Initiation Information (Automated)	256
5.3.11 Collect Discretionary Access Control Permission Modification Events (Automated).....	258
5.3.12 Collect Unsuccessful Unauthorized Access Attempts to Files (Automated)	262
5.3.13 Collect Use of Privileged Commands (Automated)	265
5.3.14 Collect Successful File System Mounts (Automated).....	267
5.3.15 Collect File Deletion Events by User (Automated)	270
5.3.16 Collect Changes to System Administration Scope (sudoers) (Automated)	272

5.3.17 Collect System Administrator Actions (sudolog) (Automated).....	274
5.3.18 Collect Kernel Module Loading and Unloading (Automated)	276
5.3.19 Make the Audit Configuration Immutable (Automated).....	278
5.4 Configure logrotate (Manual)	280
6 System Access, Authentication and Authorization.....	282
6.1 Configure cron and anacron.....	283
6.1.1 Enable anacron Daemon (Automated)	284
6.1.2 Enable cron Daemon (Automated)	286
6.1.3 Set User/Group Owner and Permission on /etc/anacrontab (Automated)	287
6.1.4 Set User/Group Owner and Permission on /etc/crontab (Automated).....	289
6.1.5 Set User/Group Owner and Permission on /etc/cron.hourly (Automated)	291
6.1.6 Set User/Group Owner and Permission on /etc/cron.daily (Automated) ..	293
6.1.7 Set User/Group Owner and Permission on /etc/cron.weekly (Automated)	295
6.1.8 Set User/Group Owner and Permission on /etc/cron.monthly (Automated)	297
6.1.9 Set User/Group Owner and Permission on /etc/cron.d (Automated).....	299
6.1.10 Restrict at/cron to Authorized Users (Automated)	301
6.2 Configure SSH	303
6.2.1 Set SSH Protocol to 2 (Automated)	304
6.2.2 Set LogLevel to INFO (Automated)	305
6.2.3 Set Permissions on /etc/ssh/sshd_config (Automated).....	307
6.2.4 Disable SSH X11 Forwarding (Automated).....	309
6.2.5 Set SSH MaxAuthTries to 4 or Less (Automated)	310
6.2.6 Set SSH IgnoreRhosts to Yes (Automated).....	311
6.2.7 Set SSH HostbasedAuthentication to No (Automated).....	312
6.2.8 Disable SSH Root Login (Automated)	314
6.2.9 Set SSH PermitEmptyPasswords to No (Automated)	316
6.2.10 Do Not Allow Users to Set Environment Options (Automated)	317
6.2.11 Use Only Approved Ciphers in Counter Mode (Automated)	319

6.2.12 Set Idle Timeout Interval for User Login (Manual)	321
6.2.13 Limit Access via SSH (Automated).....	323
6.2.14 Set SSH Banner (Automated).....	325
6.2.15 Enable SSH UsePrivilegeSeparation (Automated)	327
6.3 Configure PAM.....	328
6.3.1 Set Password Creation Requirement Parameters Using pam_cracklib (Automated).....	329
6.3.2 Set Lockout for Failed Password Attempts (Manual)	331
6.3.3 Use pam_deny.so to Deny Services (Manual).....	333
6.3.4 Upgrade Password Hashing Algorithm to SHA-512 (Automated).....	335
6.3.5 Limit Password Reuse (Automated).....	337
6.3.6 Remove the pam_ccreds Package (Automated)	338
6.4 Restrict root Login to System Console (Manual).....	339
6.5 Restrict Access to the su Command (Automated)	340
7 User Accounts and Environment.....	342
7.1 Set Shadow Password Suite Parameters (/etc/login.defs).....	343
7.1.1 Set Password Expiration Days (Automated)	344
7.1.2 Set Password Change Minimum Number of Days (Automated).....	346
7.1.3 Set Password Expiring Warning Days (Automated)	348
7.2 Disable System Accounts (Automated).....	350
7.3 Set Default Group for root Account (Automated)	352
7.4 Set Default umask for Users (Automated)	353
7.5 Lock Inactive User Accounts (Automated)	355
8 Warning Banners.....	356
8.1 Set Warning Banner for Standard Login Services	357
8.1.1 Set Warning Banner for Standard Login Services (Automated).....	358
8.1.2 Remove OS Information from Login Warning Banners (Automated)	360
8.2 Set GNOME Warning Banner (Manual).....	362
9 System Maintenance.....	364
9.1 Verify System File Permissions.....	365
9.1.1 Verify System File Permissions (Manual).....	366

9.1.2 Verify Permissions on /etc/passwd (Automated)	369
9.1.3 Verify Permissions on /etc/shadow (Automated).....	371
9.1.4 Verify Permissions on /etc/gshadow (Automated)	373
9.1.5 Verify Permissions on /etc/group (Automated)	375
9.1.6 Verify User/Group Ownership on /etc/passwd (Automated)	377
9.1.7 Verify User/Group Ownership on /etc/shadow (Automated).....	379
9.1.8 Verify User/Group Ownership on /etc/gshadow (Automated)	381
9.1.9 Verify User/Group Ownership on /etc/group (Automated)	383
9.1.10 Find World Writable Files (Automated).....	385
9.1.11 Find Un-owned Files and Directories (Automated).....	387
9.1.12 Find Un-grouped Files and Directories (Automated)	388
9.1.13 Find SUID System Executables (Manual)	390
9.1.14 Find SGID System Executables (Manual)	392
9.2 Review User and Group Settings.....	394
9.2.1 Ensure Password Fields are Not Empty (Automated).....	395
9.2.2 Verify No Legacy "+" Entries Exist in /etc/passwd File (Automated)	397
9.2.3 Verify No Legacy "+" Entries Exist in /etc/shadow File (Automated)	398
9.2.4 Verify No Legacy "+" Entries Exist in /etc/group File (Automated).....	399
9.2.5 Verify No UID 0 Accounts Exist Other Than root (Automated)	400
9.2.6 Ensure root PATH Integrity (Automated)	401
9.2.7 Check Permissions on User Home Directories (Automated).....	403
9.2.8 Check User Dot File Permissions (Automated)	405
9.2.9 Check Permissions on User .netrc Files (Automated).....	407
9.2.10 Check for Presence of User .rhosts Files (Automated)	409
9.2.11 Check Groups in /etc/passwd (Automated).....	411
9.2.12 Check That Users Are Assigned Valid Home Directories (Automated).....	413
9.2.13 Check User Home Directory Ownership (Automated)	415
9.2.14 Check for Duplicate UIDs (Automated).....	417
9.2.15 Check for Duplicate GIDs (Automated).....	419
9.2.16 Check That Reserved UIDs Are Assigned to System Accounts (Automated)	420

9.2.17 Check for Duplicate User Names (Automated)	422
9.2.18 Check for Duplicate Group Names (Automated).....	423
9.2.19 Check for Presence of User .netrc Files (Automated).....	424
9.2.20 Check for Presence of User .forward Files (Automated).....	426
Appendix: Summary Table	428
Appendix: Change History	436

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Red Hat Enterprise Linux 5.x systems running on x86 and x64 platforms. This guide was tested against RHEL 5.10

This will be the final release of the Red Hat Enterprise Linux 5, "Tikanga," CIS Benchmark. Red Hat Enterprise Linux 5 reached the end of Maintenance Support on March 31, 2017. Please see <https://access.redhat.com/support/policy/updates/errata/> for more details. Users of Red Hat Enterprise Linux 5 are encouraged to move to the most current Red Hat Stable release in order to continue receiving security updates and the benefit of actively maintained CIS Benchmarks.

Many lists are included including filesystem types, services, clients, and network protocols. Not all items in these lists are guaranteed to exist on all distributions and additional similar items may exist which should be considered in addition to those explicitly mentioned.

The guidance within broadly assumes that operations are being performed as the root user. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify root users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.

To obtain the latest version of this guide, please visit. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Red Hat Enterprise Linux 5 on x86 and x64 platforms.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Rael Daruszka

Editor

Eric Pinnell

Recommendations

1 Install Updates, Patches and Additional Security Software

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. User's data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations. The directives in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system. Note: If you are repartitioning a system that has already been installed, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the /tmp directory, this data will still consume space in / once the /tmp filesystem is mounted unless it is removed first.

1.1.1 Create Separate Partition for /tmp (Automated)

Profile Applicability:

- Level 1

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Audit:

Verify that there is a `/tmp` file partition in the `/etc/fstab` file.

```
# grep /tmp /etc/fstab
```

Remediation:

For new installations, check the box to "Review and modify partitioning" and create a separate partition for `/tmp`. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

Default Value:

No

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. CCE-14161-4

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.2 Set `nodev` option for `/tmp` Partition (Automated)

Profile Applicability:

- Level 1

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/tmp`.

Audit:

Run the following commands to determine if the system is configured as recommended.

```
# grep /tmp /etc/fstab | grep nodev
# mount | grep /tmp | grep nodev
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /tmp
```

Default Value:

OS Default: N/A

References:

1. CCE-14412-1

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3 Set nosuid option for /tmp Partition (Automated)

Profile Applicability:

- Level 1

Description:

The `nosuid` mount option specifies that the filesystem cannot contain set userid files.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create set userid files in `/tmp`.

```
# mount -o remount,nosuid /tmp
```

Audit:

Run the following commands to determine if the system is configured as recommended.

```
# grep /tmp /etc/fstab | grep nosuid  
# mount | grep /tmp | grep nosuid
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

References:

1. CCE-14940-1

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.4 Set noexec option for /tmp Partition (Automated)

Profile Applicability:

- Level 1

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/tmp`.

Audit:

Run the following commands to determine if the system is configured as recommended.

```
# grep /tmp /etc/fstab | grep noexec  
# mount | grep /tmp | grep noexec
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

```
# mount -o remount,noexec /tmp
```

References:

1. CCE-14412-1

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

1.1.5 Create Separate Partition for /var (Automated)

Profile Applicability:

- Level 1

Description:

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

Rationale:

Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Audit:

Run the following command:

```
# grep /var /etc/fstab  
  
<volume> /var ext3 <options>
```

Remediation:

For new installations, check the box to "Review and modify partitioning" and create a separate partition for `/var`.

For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. CCE-14777-7

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.6 Bind Mount the /var/tmp directory to /tmp (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/tmp` directory is normally a standalone directory in the `/var` file system. Binding `/var/tmp` to `/tmp` establishes an unbreakable link to `/tmp` that cannot be removed (even by the root user). It also allows `/var/tmp` to inherit the same mount options that `/tmp` owns, allowing `/var/tmp` to be protected in the same `/tmp` is protected. It will also prevent `/var` from filling up with temporary files as the contents of `/var/tmp` will actually reside in the file system containing `/tmp`.

Rationale:

All programs that use `/var/tmp` and `/tmp` to read/write temporary files will always be written to the `/tmp` file system, preventing a user from running the `/var` file system out of space or trying to perform operations that have been blocked in the `/tmp` filesystem.

Audit:

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

```
# grep -e "^/tmp" /etc/fstab | grep '/var/tmp'

/tmp /var/tmp none bind 0 0

# mount | grep -e "^/tmp" | grep '/var/tmp'

/tmp on /var/tmp type none (rw,bind)
```

If the above commands emit no output then the system is not configured as recommended.

Remediation:

Run the following command

```
# mount --bind /tmp /var/tmp
```

Edit the `/etc/fstab` file to contain the following line:

```
/tmp /var/tmp none bind 0 0
```

References:

1. CCE-14584-7

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7 Create Separate Partition for /var/log (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/log` directory is used by system services to store log data.

Rationale:

There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Audit:

Run the following command:

```
# grep /var/log /etc/fstab  
<volume> /var/log ext3 <options>
```

Remediation:

For new installations, check the box to "Review and modify partitioning" and create a separate partition for `/var/log`. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. CCE-14011-1

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

1.1.8 Create Separate Partition for /var/log/audit (Automated)

Profile Applicability:

- Level 1

Description:

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

Rationale:

There are two important reasons to ensure that data gathered by `auditd` is stored on a separate partition: protection against resource exhaustion (since the `audit.log` file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as `syslog`) consume space in the same partition as `auditd`, it may not perform as desired.

Audit:

Run the following command

```
# grep /var/log/audit /etc/fstab  
<volume> /var/log/audit ext3 <options>
```

Remediation:

For new installations, check the box to "Review and modify partitioning" and create a separate partition for `/var/log/audit`. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. CCE-14171-3

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

1.1.9 Create Separate Partition for /home (Automated)

Profile Applicability:

- Level 1

Description:

The `/home` directory is used to support disk storage needs of local users.

Rationale:

If the system is intended to support local users, create a separate partition for the `/home` directory to protect against resource exhaustion and restrict the type of files that can be stored under `/home`.

Audit:

Run the following command:

```
# grep /home /etc/fstab  
<volume> /home ext3 <options>
```

Remediation:

For new installations, check the box to "Review and modify partitioning" and create a separate partition for `/home`. For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. CCE-14559-9

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.10 Add nodev Option to /home (Automated)

Profile Applicability:

- Level 1

Description:

When set on a file system, this option prevents character and block special devices from being defined, or if they exist, from being used as character and block special devices.

Rationale:

Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Note: The actions in the item refer to the `/home` partition, which is the default user partition that is defined in `RHEL5`. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

Audit:

Run the following commands:

```
# grep /home /etc/fstab
Verify that nodev is an option
# mount | grep /home
<each user partition> on <mount point> type <fstype> (nodev)
```

Note: There may be other options listed for this filesystem

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /home
```

References:

1. CCE-4249-9

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.11 Add `nodev` Option to Removable Media Partitions (Manual)

Profile Applicability:

- Level 1

Description:

Set `nodev` on removable media to prevent character and block special devices that are present on the removable be treated as these device files.

Rationale:

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as `/dev/kmem` or the raw disk partitions.

Audit:

Run the following command:

```
# grep <each removable media mountpoint> /etc/fstab
Verify that nodev is an option
```

Remediation:

Edit the `/etc/fstab` file and add "`nodev`" to the fourth field (mounting options). Look for entries that have mount points that contain words such as `floppy` or `cdrom`. See the `fstab(5)` manual page for more information.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.12 Add noexec Option to Removable Media Partitions (Manual)

Profile Applicability:

- Level 1

Description:

Set `noexec` on removable media to prevent programs from executing from the removable media.

Rationale:

Setting this option on a file system prevents users from executing programs from the removable. This deters users from being to introduce potentially malicious software on the system.

Audit:

Run the following command:

```
# grep <each removable media mountpoint> /etc/fstab  
Verify that noexec is an option
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options). Look for entries that have mount points that contain words such as `floppy` or `cdrom`. See the `fstab(5)` manual page for more information.

Default Value:

OS Default: N/A

References:

1. CCE-4275-4

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.13 Add nosuid Option to Removable Media Partitions (Manual)

Profile Applicability:

- Level 1

Description:

Set `nosuid` on removable media to prevent `setuid` and `setgid` executable files that are on that media from being executed as `setuid` and `setgid`.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Run the following command:

```
# grep <each removable media mountpoint> /etc/fstab  
Verify that nosuid is an option
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options). Look for entries that have mount points that contain words such as `floppy` or `cdrom`. See the `fstab(5)` manual page for more information.

Default Value:

OS Default: N/A

References:

1. CCE-4042-8

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.14 Add `nodev` Option to `/dev/shm` Partition (Automated)

Profile Applicability:

- Level 1

Description:

The `nodev` mount option specifies that the `/dev/shm` (temporary filesystem stored in memory) cannot contain block or character special devices.

Rationale:

Since the `/dev/shm` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in `/dev/shm` partitions.

Audit:

Run the following commands to determine if the system is in configured as recommended:

```
# grep /dev/shm /etc/fstab | grep nodev
# mount | grep /dev/shm | grep nodev
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options of entries that have mount points that contain `/dev/shm`). See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /dev/shm
```

Default Value:

OS Default: N/A

References:

1. CCE-15007-8

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.15 Add nosuid Option to /dev/shm Partition (Automated)

Profile Applicability:

- Level 1

Description:

The `nosuid` mount option specifies that the `/dev/shm` (temporary filesystem stored in memory) will not execute `setuid` and `setgid` on executable programs as such, but rather execute them with the `uid` and `gid` of the user executing the program.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Run the following commands to determine if the system is in configured as recommended:

```
# grep /dev/shm /etc/fstab | grep nosuid
# mount | grep /dev/shm | grep nosuid
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options). Look for entries that have mount points that contain `/dev/shm`. See the `fstab(5)` manual page for more information.

```
# mount -o remount,nosuid /dev/shm
```

Default Value:

OS Default: N/A

References:

1. CCE-14306-5

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.16 Add noexec Option to /dev/shm Partition (Automated)

Profile Applicability:

- Level 1

Description:

Set `noexec` on the shared memory partition to prevent programs from executing from there.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Audit:

Run the following commands to determine if the system is in configured as recommended:

```
# grep /dev/shm /etc/fstab | grep noexec  
# mount | grep /dev/shm | grep noexec
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options). Look for entries that have mount points that contain `/dev/shm`. See the `fstab(5)` manual page for more information.

```
# mount -o remount,noexec /dev/shm
```

Default Value:

OS Default: N/A

References:

1. CCE-14927-8

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.17 Set Sticky Bit on All World-Writable Directories (Automated)

Profile Applicability:

- Level 1

Description:

Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.

Rationale:

This feature prevents the ability to delete or rename files in world writable directories (such as `/tmp`) that are owned by another user.

Audit:

Run the following command to verify no world writable directories exist without the sticky bit set:

```
# df --local -P 2> /dev/null | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

No output should be returned.

Remediation:

Run the following command to set the sticky bit on all world writable directories:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

Default Value:

OS Default: N/A

References:

1. CCE-3399-3

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection

Data Protection

1.1.18 Disable Mounting of cramfs Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v cramfs
install /bin/true
# /sbin/lsmmod | grep cramfs
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/cramfs.conf`

Add the following line:

```
install cramfs /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14089-7

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.19 Disable Mounting of freevxfs Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `freevxfs` filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands

```
# /sbin/modprobe -n -v freevxfs
install /bin/true
# /sbin/lsmmod | grep freevxfs
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/freevxfs.conf`

Add the following line:

```
install freevxfs /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14457-6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.20 Disable Mounting of jffs2 Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `jffs2` (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v jffs2
install /bin/true
# /sbin/lsmmod | grep jffs2
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/jffs2.conf`

Add the following line:

```
install jffs2 /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14853-6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.21 Disable Mounting of hfs Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `hfs` filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v hfs
install /bin/true
# /sbin/lsmmod | grep hfs
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/hfs.conf`

Add the following line:

```
install hfs /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-15087-0

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.22 Disable Mounting of hfsplus Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `hfsplus` filesystem type is a hierarchical filesystem designed to replace `hfs` that allows you to mount Mac OS filesystems.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v hfsplus
install /bin/true
# /sbin/lsmmod | grep hfsplus
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/hfsplus.conf`

Add the following line:

```
install hfsplus /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14093-9

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.23 Disable Mounting of squashfs Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to `cramfs`). A `squashfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v squashfs
install /bin/true
# /sbin/lsmmod | grep squashfs
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/squashfs.conf`

Add the following line:

```
install squashfs /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14118-4

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.24 Disable Mounting of udf Filesystems (Automated)

Profile Applicability:

- Level 2

Description:

The `udf` filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# /sbin/modprobe -n -v udf
install /bin/true
# /sbin/lsmmod | grep udf
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `/etc/modprobe.d/udf.conf`

Add the following line:

```
install udf /bin/true
```

Default Value:

OS Default: N/A

References:

1. CCE-14871-8

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2 Configure Software Updates

Red Hat uses the yum command line tool to install and update software packages. Updating the `RHEL5` software via the Internet requires a valid Red Hat subscription. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a Red Hat Satellite Update server that can be used in place of Red Hat's servers, whereas a single deployment of a Red Hat system may prefer to get updates from Red Hat's servers. Updates can be performed automatically or manually, depending on the site's policy for patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production. For the purpose of this benchmark, the requirement is to ensure that a patch management system is configured and maintained. The specifics on patch update procedures are left to the organization.

1.2.1 Configure Connection to the RHN RPM Repositories (Manual)

Profile Applicability:

- Level 1

Description:

Systems need to be registered with the Red Hat Network (RHN) to receive patch updates. This is usually configured during initial installation.

Rationale:

It is important to register with the Red Hat Network to make sure that patches are updated on a regular basis. This helps to reduce the exposure time as new vulnerabilities are discovered.

Audit:

Verify that the system is registered by executing the following command:

```
# yum check-update
```

Remediation:

If your system is not listed on the RHN site as a registered system, run the Red Hat Network Registration tool as follows:

```
# rhn register
```

Follow the prompts on the screen. If successful, the system will appear on the RHN web site and be subscribed to one or more software update channels. Additionally, a new daemon, `rhnsd`, will be enabled.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

1.2.2 Verify Red Hat GPG Key is Installed (Automated)

Profile Applicability:

- Level 1

Description:

Red Hat cryptographically signs updates with a GPG key to verify that they are valid.

Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system.

Audit:

Run the following command to ensure that the system has the Red Hat GPG key properly installed:

```
# rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey
```

Remediation:

Compare the GPG fingerprint with the one from Red Hat's web site at <http://www.redhat.com/security/team/key>. The following command can be used to print the installed release key's fingerprint, which is actually contained in the file referenced below:

```
# gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

More information on package signing is also available at <https://access.redhat.com/security/team/key>.

Default Value:

OS Default: N/A

References:

1. <https://access.redhat.com/security/team/key>
2. CCE-14440-2

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

1.2.3 Verify that gpgcheck is Globally Activated (Automated)

Profile Applicability:

- Level 1

Description:

The `gpgcheck` option, found in the main section of the `/etc/yum.conf` file determines if an RPM package's signature is always checked prior to its installation.

Rationale:

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

Audit:

Run the following command to verify that `gpgcheck` is set to 1 in all occurrences of the `/etc/yum.conf` file:

```
# grep gpgcheck /etc/yum.conf
gpgcheck=1
```

Remediation:

Edit the `/etc/yum.conf` file and set the `gpgcheck` to 1 as follows:

```
gpgcheck=1
```

References:

1. CCE-14914-6

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

1.2.4 Disable the rhnsd Daemon (Manual)

Profile Applicability:

- Level 2

Description:

The `rhnsd` daemon polls the Red Hat Network web site for scheduled actions.

Rationale:

Patch management policies may require that organizations test the impact of a patch before it is deployed in a production environment. Having patches automatically deployed could have a negative impact on the environment. It is best to not allow an action by default but only after appropriate consideration has been made. It is recommended that the service be disabled unless the risk is understood and accepted. This is not scorable item since organizations may have addressed the risk.

Audit:

Run the following command:

```
# chkconfig --list rhnsd  
rhnsd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Remediation:

Disable the `rhnsd` daemon by running the following command:

```
# chkconfig rhnsd off
```

Default Value:

OS Default: N/A

References:

1. CCE-3416-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.2.5 Disable yum-updatesd (Automated)

Profile Applicability:

- Level 2

Description:

The `yum-updatesd` utility provides notification of updates that are available for your system.

Rationale:

The `yum-updatesd` service may introduce unnecessary overhead and prevent other programs from running. When possible, replace this service with a `cron` job that calls `yum` directly.

Audit:

Run the following command:

```
# chkconfig --list yum-updatesd
yum-updatesd: 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Remediation:

Disable the `yum-updatesd` daemon by running the following command:

```
# chkconfig yum-updatesd off
```

Default Value:

OS Default: N/A

References:

1. CCE-4218-4

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.2.6 Obtain Software Package Updates with yum (Manual)

Profile Applicability:

- Level 1

Description:

The `yum` update utility performs software updates, including dependency analysis, based on repository metadata and can be run manually from the command line, invoked from one of the provided front-end tools, or configured to run automatically at specified intervals.

Rationale:

The `yum` update utility is the preferred method to update software since it checks for dependencies and ensures that the software is installed correctly. Refer to your local patch management procedures for the method used to perform yum updates.

Audit:

Run the following command to determine if there are any packages that need to be updated:

```
# yum check-update
```

Remediation:

Run the following command to install updates:

```
# yum update
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.2.7 Verify Package Integrity Using RPM (Manual)

Profile Applicability:

- Level 1

Description:

RPM has the capability of verifying installed packages by comparing the installed files against the file information stored in the package.

Rationale:

Verifying packages gives a system administrator the ability to detect if package files were changed, which could indicate that a valid binary was overwritten with a trojaned binary.

Audit:

Perform the following to verify integrity of installed packages:

```
# rpm -qVa | awk '$2 != "c" { print $0}'
```

If any output shows up, you may have an integrity issue with that package

Remediation:

Address unexpected discrepancies identified in the audit step.

Default Value:

OS Default: N/A

References:

1. CCE-14931-0

Additional Information:

Actions in other areas of the benchmark change permissions on some files to make them more secure than the default, which would cause this check to fail. It is important to validate the packages either have the permissions they were intended to have, or have been intentionally altered. It is recommended that any output generated in the audit step be investigated to justify the discrepancy.

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.3 Advanced Intrusion Detection Environment (AIDE)

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

1.3.1 Install AIDE (Automated)

Profile Applicability:

- Level 2

Description:

In some installations, AIDE is not installed automatically.

Rationale:

Install AIDE to make use of the file integrity features to monitor critical files for changes that could affect the security of the system.

Audit:

Run the following command and verify aide is installed:

```
# yum list aide
aide. <hardware platform> <package version> installed
```

Remediation:

Run the following command to install AIDE:

```
# yum install aide
```

Note: The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Set `PRELINKING=no` in `/etc/sysconfig/prelink` and run `/usr/sbin/prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

Default Value:

OS Default: N/A

References:

1. CCE-14081-4

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.3.2 Implement Periodic Execution of File Integrity (Automated)

Profile Applicability:

- Level 2

Description:

Implement periodic file checking, in compliance with site policy.

Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Audit:

Perform the following to determine if there is a `crontab` job scheduled to run the aide check.

```
# crontab -u root -l | grep aide
0 5 * * * /usr/sbin/aide --check
```

Remediation:

Execute the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/sbin/aide --check
```

Note: The checking in this instance occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.4 Configure SELinux

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under SELinux, every process and every object (files, sockets, pipes) on the system is assigned a security context, a label that includes detailed type information about the object. The kernel allows processes to access objects only if that access is explicitly allowed by the policy in effect. The policy defines transitions, so that a user can be allowed to run software, but the software can run under a different context than the user's default. This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation. Three such policies have been designed for use with RHEL5 and are included with the system: `targeted`, `strict`, and `mls`. These are described as follows:

- `targeted`: consists mostly of Type Enforcement (TE) rules, and a small number of Role-Based Access Control (RBAC) rules. Targeted restricts the actions of many types of programs, but leaves interactive users largely unaffected.
- `strict`: also uses TE and RBAC rules, but on more programs and more aggressively.
- `mls`: implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the targeted policy. References: 1. NSA SELinux resources: a. <http://www.nsa.gov/research/selinux> b. <http://www.nsa.gov/research/selinux/list.shtml>

2. Fedora SELinux resources: a. FAQ: <http://docs.fedoraproject.org/selinux-faq> b. User Guide: <http://docs.fedoraproject.org/selinux-user-guide> c. Managing Services Guide: <http://docs.fedoraproject.org/selinux-managing-confined-services-guide>

3. SELinux Project web page and wiki: a. <http://www.selinuxproject.org>

4. Chapters 43-45 of *Red Hat Enterprise Linux 5: Deployment Guide* (Frank Mayer, Karl MacMillan and David Caplan),

5. *SELinux by Example: Using Security Enhanced Linux* (Prentice Hall, August 6, 2006)

1.4.1 Enable SELinux in /etc/grub.conf (Automated)

Profile Applicability:

- Level 2

Description:

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters

Rationale:

SELinux must be enabled at boot time in `/etc/grub.conf` to ensure that the controls it provides are not overwritten.

Audit:

Perform the following to verify that SELinux is enabled at boot time:

```
# grep selinux=0 /etc/grub.conf  
[no output produced]  
# grep enforcing=0 /etc/grub.conf  
[no output produced]
```

Remediation:

Remove all instances of `selinux=0` and `enforcing=0` from `/etc/grub.conf`.

Default Value:

OS Default: No

References:

1. CCE-3977-6

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.4.2 Set the SELinux State (Automated)

Profile Applicability:

- Level 2

Description:

Set SELinux to enable when the system is booted.

Rationale:

SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.

Audit:

Perform the following to determine if SELinux is enabled at boot time.

```
# grep SELINUX=enforcing /etc/selinux/config
SELINUX=enforcing

# /usr/sbin/sestatus

SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
Policy from config file: targeted
```

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUX parameter:

```
SELINUX=enforcing
```

Default Value:

OS Default: No

References:

1. CCE-3999-0

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.4.3 Set the SELinux Policy (Automated)

Profile Applicability:

- Level 2

Description:

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Audit:

Perform the following to determine if the targeted policy is selected in the `/etc/selinux/config` file.

```
# grep SELINUXTYPE=targeted /etc/selinux/config
SELINUXTYPE=targeted
# /usr/sbin/sestatus
SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
Policy from config file: targeted
```

Note: If your organization requires stricter policies, verify that they are selected by using the "grep" command on the `/etc/selinux/config` file.

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

Note: If your organization requires stricter policies, make sure they are added to the `/etc/selinux/config` file.

Default Value:

OS Default: No

References:

1. CCE-3624-4

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.4.4 Remove SETroubleshoot (Automated)

Profile Applicability:

- Level 2

Description:

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

Rationale:

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled or removed.

Audit:

Perform the following to determine if `setroubleshoot` is installed.

```
# rpm -q setroubleshoot
package setroubleshoot is not installed
```

Remediation:

Run the following command to remove `setroubleshoot`

```
# yum erase setroubleshoot
```

Default Value:

OS Default: No

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.4.5 Disable MCS Translation Service (mcstrans) (Automated)

Profile Applicability:

- Level 2

Description:

The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`

Rationale:

Since this service is not used very often, disable it to reduce the amount of potentially vulnerable code running on the system.

Audit:

Run the following command:

```
# chkconfig --list mcstrans
mcstrans 0: off 1: off 2: off 3: off 4: off 5: off 6: off
```

Remediation:

Run the following command to disable mcstrans:

```
# chkconfig mcstrans off
```

Default Value:

OS Default: No

References:

1. CCE-3668-1

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.4.6 Check for Unconfined Daemons (Automated)

Profile Applicability:

- Level 2

Description:

Daemons that are not defined in SELinux policy will inherit the security context of their parent process.

Rationale:

Since daemons are launched and descend from the `init` process, they will inherit the security context label `initrc_t`. This could cause the unintended consequence of giving the process more permission than it requires.

Audit:

Perform the following to determine if unconfined daemons are running on the system.

```
# ps -eZ | egrep "initrc" | egrep -vw "tr|ps|egrep|bash|awk" | tr ':' ' ' |  
awk '{ print $NF }'
```

[no output produced]

Remediation:

Investigate any unconfined daemons found during the audit action.

Default Value:

OS Default: No

References:

1. CCE-14991-4

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.5 Secure Boot Settings

1.5.1 Set User/Group Owner on /etc/grub.conf (Automated)

Profile Applicability:

- Level 1

Description:

Set the owner and group of `/etc/grub.conf` to the root user.

Rationale:

Setting the owner and group to *root* prevents non-root users from changing the file.

Audit:

Perform the following to determine if the `/etc/grub.conf` file has the correct ownership:

```
# stat -L -c "%u %g" /etc/grub.conf | egrep "^0 0$"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following command to assign owner and group of `/etc/grub.conf` to root:

```
# chown root:root /etc/grub.conf
```

Default Value:

OS Default: No

References:

1. CCE-4144-2
2. CCE-4197-0

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.5.2 Set Permissions on /etc/grub.conf (Automated)

Profile Applicability:

- Level 1

Description:

Set permission on the `/etc/grub.conf` file to read and write for root only.

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Audit:

Perform the following to determine if the `/etc/grub.conf` file permissions are correct:

```
# stat -L -c "%a" /etc/grub.conf | egrep ".00"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following command to remove excess permissions from `/etc/grub.conf`

```
# chmod og-rwx /etc/grub.conf
```

Default Value:

OS Default: No

References:

1. CCE-3923-0

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.5.3 Set Boot Loader Password (Automated)

Profile Applicability:

- Level 1

Description:

Setting the boot loader password will require that anyone rebooting system must enter a password before being able to set command line boot parameters

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Audit:

Perform the following to determine if a password is required to set command line boot parameters:

```
# grep "^password" /etc/grub.conf
password --md5 <passwd hash>
```

Remediation:

Run the following:

```
#!/bin/bash
grub-md5-crypt | tee /tmp/$$
x=$(tail -1 /tmp/$$)
/bin/rm -f /tmp/$$
ed /etc/grub.conf << END > /dev/null 2>&1
g/^password/d
$
?^#?
a
password --md5 $x
.
w
q
END
```

Default Value:

OS Default: No

References:

1. CCE-3818-2

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.5.4 Require Authentication for Single-User Mode (Automated)

Profile Applicability:

- Level 1

Description:

Since `/etc/init` determines what run state the system is in, setting the entry in `/etc/inittab` will force single user authentication.

Rationale:

Requiring authentication in single user mode prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Perform the following to determine

```
# grep "sulogin" /etc/inittab
~:S:wait:/sbin/sulogin
```

Remediation:

Add the following to `/etc/inittab`:

```
~:S:wait:/sbin/sulogin
```

Default Value:

OS Default: No

References:

1. CCE-4241-6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.5.5 Disable Interactive Boot (Automated)

Profile Applicability:

- Level 1

Description:

The `PROMPT` option provides console users the ability to interactively boot the system and select which services to start on boot .

Rationale:

Turn off the `PROMPT` option on the console to prevent console users from potentially overriding established security settings.

Audit:

Perform the following to determine if `PROMPT` is disabled:

```
# grep "^PROMPT=" /etc/sysconfig/init  
  
PROMPT=no
```

Remediation:

Set the `PROMPT` parameter in `/etc/sysconfig/init` to `no`.

Default Value:

OS Default: No

References:

1. CCE-4245-7

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.6 Additional Process Hardening

1.6.1 Restrict Core Dumps (Automated)

Profile Applicability:

- Level 1

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Rationale:

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see `limits.conf(5)`). In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

Audit:

Perform the following to determine if core dumps are restricted.

```
# grep "hard core" /etc/security/limits.conf
*      hard core 0
# sysctl fs.suid_dumpable
fs.suid_dumpable = 0
```

Remediation:

Add the following line to the `/etc/security/limits.conf` file.

```
*      hard core 0
```

Add the following line to the `/etc/sysctl.conf` file.

```
fs.suid_dumpable = 0
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.6.2 Configure ExecShield (Automated)

Profile Applicability:

- Level 1

Description:

Execshield is made up of a number of kernel features to provide protection against buffer overflow attacks. These features include prevention of execution in memory data space, and special handling of text buffers.

Rationale:

Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Audit:

Perform the following to determine if ExecShield is enabled.

```
# sysctl kernel.exec-shield
kernel.exec-shield = 1
```

Remediation:

Add the following line to the `/etc/sysctl.conf` file.

```
kernel.exec-shield = 1
```

Default Value:

OS Default: Yes

References:

1. CCE-4168-1

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.6.3 Enable Randomized Virtual Memory Region Placement (Automated)

Profile Applicability:

- Level 1

Description:

Set the system flag to force randomized virtual memory region placement.

Rationale:

Randomly placing virtual memory regions will make it difficult for to write memory page exploits as the memory placement will be consistently shifting.

Audit:

Perform the following to determine if virtual memory is randomized.

```
# sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
```

Remediation:

Add the following line to the `/etc/sysctl.conf` file.

```
kernel.randomize_va_space = 2
```

Default Value:

OS Default: Yes

References:

1. CCE-4146-7

CIS Controls:

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

1.6.4 Enable XD/NX Support on 32-bit x86 Systems (Automated)

Profile Applicability:

- Level 1

Description:

Modern versions of 32bit processors of the x86 family support a feature that prevents code execution on a per memory page basis. On AMD processors, this feature is called No Execute (NX) and on Intel processors, it is called Execute Disable (XD).

Rationale:

This feature can help prevent buffer overflow exploits from running on the system. Where possible, this extra protection should be installed. Prior to running the remediation, dump out the cpuinfo by typing `cat /proc/cpuinfo`. In the flags field, verify that the flags `paе` and `nx` exist. If they do, proceed to the remediation section. If they do not, consult the processor guide for the processor you are running to determine if this feature exists and how to turn it on in the BIOS.

Audit:

Perform the following to determine if XD/NX support is enabled.

```
# yum list kernel-PAE
kernel-PAE.<hardware platform> <release> installed
```

Remediation:

Run the following to install kernel-PAE

```
# yum install kernel-PAE
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies

Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

1.6.5 Disable Prelink (Automated)

Profile Applicability:

- Level 1

Description:

Prelinking is a performance enhancing feature that decreases process start up time. It loads shared libraries into addresses for which the linking of required symbols has already been performed. After a binary has been prelinked, the addresses at which shared libraries is not changed, even if `kernel.randomize_va_space` is set to 1.

Rationale:

There is a bug in prelink that interferes with AIDE, the Linux file integrity checker. This has been fixed in RHEL6 (so prelink does not need to be disabled in RHEL6 systems).

Audit:

Perform the following to determine or prelinking is disabled.

```
# grep PRELINKING /etc/sysconfig/prelink
PRELINKING=no
```

Remediation:

Edit `/etc/sysconfig/prelink` and set `PRELINKING=no`:

```
PRELINKING=no
```

Note: If the feature is changed from yes to no, run `/usr/sbin/prelink -ua` to revert binaries and libraries to their original context before prelinking.

Default Value:

OS Default: No

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7 Use the Latest OS Release (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, Red Hat releases updates to the Red Hat operating system to support new hardware platforms, deliver new functionality as well as the bundle together a set of patches that can be tested as a unit.

Rationale:

Newer updates may contain security enhancements that would not be available through the standard patching process. As a result, it is recommended that the latest update of the Red Hat software be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Audit:

Run one of the following commands to determine the current OS level:

```
# uname -r
```

OR

```
# cat /etc/redhat-release
```

Remediation:

Obtain and install the latest update of the `RHEL5` software.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices

Install the latest stable version of any security-related updates on all network devices.

2 OS Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on what services can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system.

2.1 Remove Legacy Services

The items in this section are intended to ensure that legacy services are not installed on the system. Some guidance includes directives to both disable and remove the service. There is no good reason to have these services on the system, even in a disabled state.

Note: The audit items in the section check to see if the packages are listed in the yum database and installed using rpm. It could be argued that someone may have installed them separately. However, this is also true for any other type of rogue software. It is beyond the scope of this benchmark to address software that is installed using non-standard methods and installation directories.

2.1.1 Remove telnet-server (Automated)

Profile Applicability:

- Level 1

Description:

The telnet-server package contains the `telnetd` daemon, which accepts connections from users from other systems via the `telnet` protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Red Hat Linux distributions.

Audit:

Perform the following to determine if the telnet-server package is on the system.

```
# yum list telnet-server
telnet-server. <hard platform> <release> <anything except installed>
```

Remediation:

Run the following to remove telnet-server:

```
# yum erase telnet-server
```

Default Value:

OS Default: Disabled

References:

1. CCE-3390-2
2. CCE-4330-7

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.2 Remove telnet Clients (Automated)

Profile Applicability:

- Level 1

Description:

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an authorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Red Hat Linux distributions.

Audit:

Perform the following to determine if the telnet package is on the system.

```
# yum list telnet  
telnet.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove telnet:

```
# yum erase telnet
```

Default Value:

OS Default: Disabled

References:

1. CCE-3390-2
2. CCE-4330-7

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.3 Remove rsh-server (Automated)

Profile Applicability:

- Level 1

Description:

The Berkeley rsh-server (`rsh`, `rlogin`, `rcp`) package contains legacy services that exchange credentials in clear-text.

Rationale:

These legacy service contain numerous security exposures and have been replaced with the more secure SSH package.

Audit:

Perform the following to determine if rsh-server is installed on the system.

```
# yum list rsh-server  
rsh-server.<hard platform> <release> <anything except installed>
```

Remediation:

Run the following command to remove rsh-server:

```
# yum erase rsh-server
```

Default Value:

OS Default: Not Installed

References:

1. CCE-4308-3

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.4 Remove rsh (Automated)

Profile Applicability:

- Level 1

Description:

The `rsh` package contains the client commands for the `rsh` services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh` package removes the clients for `rsh`, `rcp` and `rlogin`.

Audit:

Perform the following to determine if `rsh` is installed on the system.

```
# yum list rsh  
rsh.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `rsh`:

```
# yum erase rsh
```

Default Value:

OS Default: Not Installed

References:

1. CCE-4141-8 (rsh)
2. CCE- 3974-3 (rcp)
3. CCE- 3537-8 (rlogin)

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.5 Remove NIS Client (Automated)

Profile Applicability:

- Level 1

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`yplibind`) was used to bind a machine to an NIS server and receive the distributed configuration files

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Audit:

Perform the following to determine if `yplibind` is installed on the system.

```
# yum list yplibind
yplibind.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `yplibind`:

```
# yum erase yplibind
```

Default Value:

OS Default: Disabled

References:

1. CCE-3705-1 (disable)
2. CCE-4348-9 (uninstall)

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.6 Remove NIS Server (Automated)

Profile Applicability:

- Level 1

Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used.

Audit:

Perform the following to determine if ypserv is installed on the system.

```
# yum list ypserv  
ypserv.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove ypserv:

```
# yum erase ypserv
```

Default Value:

OS Default: Disabled

References:

1. CCE-3705-1 (disable)
2. CCE-4348-9 (uninstall)

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.7 Remove tftp (Automated)

Profile Applicability:

- Level 1

Description:

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol, typically used to automatically transfer configuration or boot files between machines. TFTP does not support authentication and can be easily hacked. The package `tftp` is a client program that allows for connections to a `tftp` server.

Rationale:

It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server). In that case, use extreme caution when configuring the services.

Audit:

Perform the following to determine if `tftp` is installed on the system.

```
# yum list tftp  
tftp.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `tftp`:

```
# yum erase tftp
```

Default Value:

OS Default: Disabled

References:

1. CCE-4273-9 (disable)
2. CCE-3916-4 (uninstall)

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.8 Remove tftp-server (Automated)

Profile Applicability:

- Level 1

Description:

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol, typically used to automatically transfer configuration or boot machines from a boot server. The package `tftp-server` is the server package used to define and support a TFTP server.

Rationale:

TFTP does not support authentication nor does it ensure the confidentiality of integrity of data. It is recommended that TFTP be removed, unless there is a specific need for TFTP. In that case, extreme caution must be used when configuring the services.

Audit:

Perform the following to determine if `tftp-server` is installed on the system.

```
# yum list tftp-server  
tftp-server.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `tftp-server`:

```
# yum erase tftp-server
```

Default Value:

OS Default: Disabled

References:

1. CCE-4273-9 (disable)
2. CCE-3916-4 (uninstall)

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.9 Remove talk (Automated)

Profile Applicability:

- Level 1

Description:

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client (allows initialization of `talk` sessions) is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

Audit:

Perform the following to determine if `talk` is installed on the system.

```
# yum list talk  
talk.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `talk`:

```
# yum erase talk
```

Default Value:

OS Default: Enabled

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.10 Remove talk-server (Automated)

Profile Applicability:

- Level 1

Description:

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client (allows initialization of `talk` sessions) is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

Audit:

Perform the following to determine if `talk-server` is installed on the system:

```
# yum list talk-server  
talk.<hard platform> <release>    <anything except install>
```

Remediation:

Run the following command to remove `talk-server`:

```
# yum erase talk-server
```

Default Value:

OS Default: Not Installed

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.11 Remove xinetd (Automated)

Profile Applicability:

- Level 2

Description:

The eXtended InterNET Daemon (`xinetd`) is an open source super daemon that replaced the original `inetd` daemon. The `xinetd` daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

Rationale:

If there are no `xinetd` services required, it is recommended that the daemon be deleted from the system.

Audit:

Perform the following to determine if `xinetd` is installed on the system.

```
# yum list xinetd  
xinted.<hard platform> <release>    <anything except installed>
```

Remediation:

Run the following command to remove `xinetd`:

```
# yum erase xinetd
```

Default Value:

OS Default: Not Installed

References:

1. CCE-4234-1
2. CCE-4164-0

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.1.12 Disable chargen-dgram (Automated)

Profile Applicability:

- Level 1

Description:

chargen-dgram is a network service that responds with 0 to 512 ASCII characters for each datagram it receives. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list chargen-dgram
chargen-dgram:      off
```

Remediation:

Disable the chargen-dgram service by running the following command:

```
# chkconfig chargen-dgram off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.13 Disable *chargen-stream* (Automated)

Profile Applicability:

- Level 1

Description:

`chargen-stream` is a network service that responds with 0 to 512 ASCII characters for each connection it receives. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list chargen-stream  
  
chargen-stream:    off
```

Remediation:

Disable the `chargen-stream` service by running the following command:

```
# chkconfig chargen-stream off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.14 Disable daytime-dgram (Automated)

Profile Applicability:

- Level 1

Description:

`daytime-dgram` is a network service that responds with the server's current date and time. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list daytime-dgram
daytime-dgram:    off
```

Remediation:

Disable the `daytime-dgram` service by running the following command:

```
# chkconfig daytime-dgram off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.15 Disable daytime-stream (Automated)

Profile Applicability:

- Level 1

Description:

`daytime-stream` is a network service that responds with the server's current date and time. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list daytime-stream
daytime-stream:    off
```

Remediation:

Disable the `daytime-stream` service by running the following command:

```
# chkconfig daytime-stream off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.16 Disable echo-dgram (Automated)

Profile Applicability:

- Level 1

Description:

echo-dgram is a network service that responds to clients with the data sent to it by the client. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list echo-dgram
echo-dgram: off
```

Remediation:

Disable the echo-dgram service by running the following command:

```
# chkconfig echo-dgram off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.17 Disable echo-stream (Automated)

Profile Applicability:

- Level 1

Description:

`echo-stream` is a network service that responds to clients with the data sent to it by the client. This service is intended for debugging and testing purposes. It is recommended that this service be disabled.

Rationale:

Disabling this service will reduce the remote attack surface of the system.

Audit:

Run the following command:

```
# chkconfig --list echo-stream  
  
echo-stream:          off
```

Remediation:

Disable the echo-stream service by running the following command:

```
# chkconfig echo-stream off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.18 Disable tcpmux-server (Automated)

Profile Applicability:

- Level 1

Description:

`tcpmux-server` is a network service that allows a client to access other network services running on the server. It is recommended that this service be disabled.

Rationale:

`tcpmux-server` can be abused to circumvent the server's host based firewall. Additionally, `tcpmux-server` can be leveraged by an attacker to effectively port scan the server.

Audit:

Run the following command:

```
# chkconfig --list tcpmux-server  
  
tcpmux-server:      off
```

Remediation:

Disable the `tcpmux-server` service by running the following command:

```
# chkconfig tcpmux-server off
```

Default Value:

OS Default: Disabled

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3 Special Purpose Services

This section describes services that are installed on servers that specifically need to run these services. If any of these services are not required, it is recommended that they be disabled or deleted from the system to reduce the potential attack surface.

3.1 Disable Avahi Server

3.1.1 Disable Avahi Server (Automated)

Profile Applicability:

- Level 1

Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

Rationale:

Since servers are not normally used for printing, this service is not needed unless dependencies require it. If this is the case, disable the service to reduce the potential attack surface. If for some reason the service is required on the server, follow the recommendations in sub-sections 3.1.2 - 3.1.5 to secure it.

Audit:

Perform the following to determine if Avahi is disabled.

```
# chkconfig --list avahi-daemon
avahi-daemon:      0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Remediation:

Run the following command to disable avahi-daemon:

```
# chkconfig avahi-daemon off
```

Edit the `/etc/sysconfig/network` file and remove `zeroconf`.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.2 Service Only via Required Protocol (Manual)

Profile Applicability:

- Level 1

Description:

Avahi can support either the IPv4 or IPv6 protocols, depending on what the system is configured to use.

Rationale:

Configure IPv4 or IPv6, depending on which protocol needs to be used. Limiting support to the protocol that is actually reduces the potential attack surface

Audit:

Perform the following to determine which protocol is configured on your system.

```
# grep use-ipv /etc/avahi/avahi-daemon.conf  
  
use-ipv6 = no  
If ipv4 is only used.  
Use-ipv4 = no  
If ipv6 is only used.
```

Remediation:

Edit the `/etc/avahi/avahi-daemon.conf` file to use the appropriate protocol for your environment.

- if only using IPv4, disable IPv6 with this line:

```
use-ipv6=no
```

- if only using IPv6, disable IPv4 with this line:

```
use-ipv4=no
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.3 Check Responses TTL Field (Automated)

Profile Applicability:

- Level 1

Description:

Avahi can be configured to ignore packets unless the TTL field is 255.

Rationale:

Setting this field makes sure that only multicast DNS packets from the local network are processed. Although a properly configured router and firewall should not allow these packets from outside networks, this is an extra check to ensure this does not happen.

Audit:

Perform the following to determine if the TTL setting is correct.

```
# grep "^check-response-ttl=yes" /etc/avahi/avahi-daemon.conf
check-response-ttl=yes
```

Remediation:

Edit the `/etc/avahi/avahi-daemon.conf` file and add the following line to the `[server]` section:

```
check-response-ttl=yes
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.4 Prevent Other Programs from Using Avahi's Port (Manual)

Profile Applicability:

- Level 1

Description:

Avahi can stop other multicast Domain Name Service (mDNS) stacks from running on the host by preventing other processes from binding to port 5353.

Rationale:

Setting this option ensures that only Avahi is processing multicast DNS packets coming into that port on the system.

Audit:

Perform the following to determine if Avahi's port is restricted:

```
# grep "^disallow-other-stacks=yes" /etc/avahi/avahi-daemon.conf  
disallow-other-stacks=yes
```

Remediation:

Edit the `/etc/avahi/avahi-daemon.conf` file and add the following line:

```
disallow-other-stacks=yes
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.5 Disable Publishing (Automated)

Profile Applicability:

- Level 1

Description:

The default setting in the configuration file allows the avahi-daemon to send information about the local host such as its address records and the services it offers, to the local network.

Rationale:

If the system does not need to offer services, disable publishing any information about the system to reduce the potential attack surface.

Audit:

Perform the following to determine if publishing is disabled.

```
# grep "^disable-publishing=yes" /etc/avahi/avahi-daemon.conf
disable-publishing=yes
```

Remediation:

Disable publishing in the `/etc/avahi/avahi-daemon.conf` file as follows:

```
#!/bin/bash
grep "^disable-publishing=yes" /etc/avahi/avahi-daemon.conf
if [ $? -ne 0 ]
then
ed /etc/avahi/avahi-daemon.conf <<END
g/ disable-publishing=yes /d
/^\[publish\]/
a
disable-publishing =yes
.
w
q
END
fi
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.1.6 Restrict Published Information (if publishing is required) (Manual)

Profile Applicability:

- Level 1

Description:

If it is necessary to publish some information to the network, it should not be joined by any extraneous information or by information supplied by a non-trusted source on the system.

Rationale:

This option is most useful on client machines. Setting this option will prevent Avahi from advertising its services. Clients machines typically consume services rather than provide services.

Audit:

Perform the following to determine if publishing is restricted:

```
# grep "^disable-publishing=yes" /etc/avahi/avahi-daemon.conf
disable-publishing=yes
# grep "^publish" /etc/avahi/avahi-daemon.conf
publish-address=no
publish-binfo=no
publish-workstation=no
publish-domain=no
```

Remediation:

Restrict publishing by editing the `/etc/avahi/avahi-daemon.conf` file as follows:

```
#!/bin/bash
grep "^disable-user-service-publishing=yes" /etc/avahi/avahi-daemon.conf
if [ $? -ne 0 ]
then
ed /etc/avahi/avahi-daemon.conf << END
g/ disable-publishing=yes /d
/^\[publish\]/
a
disable-publishing=yes
publish-address=no
publish-binfo=no
publish-workstation=no
publish-domain=no
.
w
q
END
fi
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.2 Set Daemon umask (Automated)

Profile Applicability:

- Level 1

Description:

Set the default `umask` for all processes started at boot time. The settings in `umask` selectively turn off default permission when a file is created by a daemon process.

Rationale:

Setting the `umask` to `027` will make sure that files created by daemons will not be readable, writable or executable by any other than the group and owner of the daemon process and will not be writable by the group of the daemon process. The daemon process can manually override these settings if these files need additional permission.

Audit:

Perform the following to determine if the daemon `umask` is set.

```
# grep umask /etc/sysconfig/init
umask 027
```

Remediation:

Add the following line to the `/etc/sysconfig/init` file.

```
umask 027
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

3.3 Remove X Windows (Automated)

Profile Applicability:

- Level 1

Description:

The X Windows system provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on desktops where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Audit:

Perform the following to determine if X Windows is installed on the system.

```
# grep "^id:" /etc/inittab
id:3:initdefault

# yum grouplist "X Window System"

loaded plugins: rhnplugin, security
Setting up Group Process
Available Groups:
  X Window System
Done
```

Remediation:

Edit `/etc/inittab` set default runlevel as follows:

```
s/:5:/:3:/
```

Uninstall the X Windows System:

```
# yum groupremove "X Window System"
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.4 Disable Print Server - CUPS (Manual)

Profile Applicability:

- Level 1

Description:

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.

Audit:

Perform the following to determine if CUPS is disabled.

```
# chkconfig --list cups
chkconfig: 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Remediation:

Run the following command to disable cups:

```
# chkconfig cups off
```

Default Value:

OS Default: Disabled

References:

1. <http://www.cups.org>.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.5 Remove DHCP Server (Manual)

Profile Applicability:

- Level 1

Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

Rationale:

Unless a server is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if DHCP is disabled.

```
# yum list dhcp  
  
dhcp.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove dhcp:

```
# yum erase dhcp
```

Default Value:

OS Default: Not Installed

References:

1. <http://www.isc.org/software/dhcp>

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.6 Configure Network Time Protocol (NTP) (Automated)

Profile Applicability:

- Level 1

Description:

The Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. The version of NTP delivered with Red Hat can be found at <http://www.ntp.org>. NTP can be configured to be a client and/or a server.

Rationale:

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured as NTP clients to synchronize their clocks (especially to support time sensitive security mechanisms like Kerberos). This also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

The following script checks for the correct parameters on restrict default and restrict -6 default:

```
# grep "restrict default" /etc/ntp.conf
restrict default kod nomodify nopeer notrap noquery
# grep "restrict -6 default" /etc/ntp.conf
restrict -6 default kod nomodify nopeer notrap noquery
```

Perform the following to determine if the system is configured to use an NTP Server and that the ntp daemon is running as an unprivileged user.

```
# grep "^server" /etc/ntp.conf
server <ntp-server>
# grep "ntp:ntp" /etc/sysconfig/ntpd
OPTIONS="-u ntp:ntp -p /var/run/ntpd.pid"
```

Remediation:

Add the following lines to `/etc/ntp.conf`:

```
# Script to fix /etc/ntp.conf
cp /etc/ntp.conf /tmp/ntp.conf.$$
egrep -v '(restrict default|restrict -6 default)' /tmp/ntp.conf.$$ >
/etc/ntp.conf
ed /etc/ntp.conf << END
0a
restrict default kod nomodify nopeer notrap noquery
restrict -6 default kod nomodify nopeer notrap noquery
.
w
q
END
```

Ensure `/etc/ntp.conf` has an NTP server specified:

```
server <ntp-server>
```

Note: is the IP address or hostname of a trusted time server. Configuring an NTP server is outside the scope of this benchmark.

Default Value:

OS Default: N/A

References:

1. <http://www.ntp.org>

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

3.7 Remove LDAP (Automated)

Profile Applicability:

- Level 1

Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database. The default client/server LDAP application for Red Hat is OpenLDAP.

Rationale:

If the server will not need to act as an LDAP client or server, it is recommended that the software be disabled to reduce the potential attack surface.

Audit:

Perform the following to determine if LDAP is running.

```
# yum list openldap-servers  
openldap-servers.<hardware platform> <release> <anything but installed>
```

Remediation:

If LDAP is running on the system and is not needed, remove it as follows:

```
# yum erase openldap-servers
```

Default Value:

OS Default: No

References:

1. <http://www.openldap.org>

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.8 Disable NFS and RPC (Automated)

Profile Applicability:

- Level 1

Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the server does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.

Audit:

Perform the following to determine if NFS is disabled.

```
# chkconfig --list nfslock
nfslock:    0:off 1:off 2:off 3:off 4:off 5:off 6:off

# chkconfig --list rpcgssd
rpcgssd:    0:off 1:off 2:off 3:off 4:off 5:off 6:off

# chkconfig --list rpcidmapd
rpcidmapd:  0:off 1:off 2:off 3:off 4:off 5:off 6:off

# chkconfig --list portmap
portmap:    0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Remediation:

Run the following commands:

```
# chkconfig nfslock off
# chkconfig rpcgssd off
# chkconfig rpcidmapd off
# chkconfig portmap off
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.9 Remove DNS Server (Automated)

Profile Applicability:

- Level 1

Description:

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

Rationale:

Unless a server is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if DNS is disabled on the system.

```
# yum list bind  
bind. <hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove bind:

```
# yum erase bind
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.10 Remove FTP Server (Automated)

Profile Applicability:

- Level 1

Description:

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if FTP is disabled.

```
# yum list vsftpd  
vsftpd.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove vsftpd

```
# yum erase vsftpd
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.11 Remove HTTP Server (Automated)

Profile Applicability:

- Level 1

Description:

HTTP or web servers provide the ability to host web site content. The default HTTP server shipped with Red Hat Linux is Apache.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if apache is disabled.

```
# yum list httpd  
httpd. <hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove httpd:

```
# yum erase httpd
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.12 Remove Dovecot (IMAP and POP3 services) (Automated)

Profile Applicability:

- Level 1

Description:

Dovecot is an open source IMAP and POP3 server for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided to this server, it is recommended that the service be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if dovecot is installed on the system.

```
# yum list dovecot  
dovecot.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove dovecot:

```
# yum erase dovecot
```

Default Value:

OS Default: N/A

References:

1. <http://www.dovecot.org>

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.13 Remove Samba (Automated)

Profile Applicability:

- Level 1

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Small Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if samba is installed on the system.

```
# yum list samba  
samba.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove samba:

```
# yum erase samba
```

Default Value:

OS Default: Not Installed

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.14 Remove HTTP Proxy Server (Automated)

Profile Applicability:

- Level 1

Description:

The default HTTP proxy package shipped with Red Hat Linux is squid.

Rationale:

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

Audit:

Perform the following to determine if squid is installed on the system.

```
# yum list squid  
squid.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove squid:

```
# yum erase squid
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.15 Remove SNMP Server (Automated)

Profile Applicability:

- Level 1

Description:

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.

Audit:

Perform the following to determine if net-snmp is installed on the system.

```
# yum list net-snmp  
net.snmp.<hardware platform> <release> <anything but installed>
```

Remediation:

Run the following command to remove net-snmp:

```
# yum erase net-snmp
```

Default Value:

OS Default: Not Installed

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

3.16 Configure Mail Transfer Agent for Local-Only Mode (Automated)

Profile Applicability:

- Level 1

Description:

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail. By default, the MTA is set to loopback mode on RHEL5 and RHEL6.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

Note: RHEL5 uses sendmail as the default MTA while RHEL6 uses Postfix. The recommendation to set the default MTA to local-only mode applies regardless of the MTA that is used.

Audit:

Perform the following command and make sure that the MTA is listening on the loopback address (127.0.0.1):

```
# netstat -an | grep LIST | grep 25  
tcp    0      0  127.0.0.1:25          0.0.0.0:*             LISTEN
```

Remediation:

Edit `/etc/mail/sendmail.cf` and add or edit the following line to the Options section.

```
O DaemonPortOptions=Port=smtp, Addr=127.0.0.1, Name=MTA
```

Run the following command to restart sendmail:

```
# service sendmail restart
```

Default Value:

OS Default: Yes

CIS Controls:

Version 7

9 Limitation and Control of Network Ports, Protocols, and Services

Limitation and Control of Network Ports, Protocols, and Services

4 Network Configuration and Firewalls

This section provides guidance for secure network and firewall configuration.

4.1 Modify Network Parameters (Host Only)

The following network parameters determine if the system is to act as a *host only*. A system is considered *host only* if the system has a single interface, or has multiple interfaces but will not be configured as a router.

4.1.1 Disable IP Forwarding (Automated)

Profile Applicability:

- Level 1

Description:

The `net.ipv4.ip_forward` flag is used to tell the server whether it can forward packets or not. If the server is not to be used as a router, set the flag to 0.

Rationale:

Setting the flag to 0 ensures that a server with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Audit:

Run the following command and verify output matches:

```
# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

Remediation:

Set the `net.ipv4.ip_forward` parameter to 0 in `/etc/sysctl.conf`:

```
net.ipv4.ip_forward = 0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.ip_forward=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: N/A

References:

1. CCE-3561-8

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.1.2 Disable Send Packet Redirects (Automated)

Profile Applicability:

- Level 1

Description:

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0
# sysctl net.ipv4.conf.default.send_redirects
net.ipv4.conf.default.send_redirects = 0
```

Remediation:

Set the `net.ipv4.conf.all.send_redirects` and `net.ipv4.conf.default.send_redirects` parameters to 0 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.send_redirects=0
# sysctl -w net.ipv4.conf.default.send_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: N/A

References:

1. CCE-4151-7
2. CCE-4155-8

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2 Modify Network Parameters (Host and Router)

The following network parameters determine if the system is to act as a router. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

4.2.1 Disable Source Routed Packet Acceptance (Automated)

Profile Applicability:

- Level 1

Description:

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to 0 disables the system from accepting source routed packets. Assume this server was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the server as a way to reach the private address servers. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Audit:

Run the following commands and verify output matches:

```
# /sbin/sysctl net.ipv4.conf.all.accept_source_route
net.ipv4.conf.all.accept_source_route = 0

# /sbin/sysctl net.ipv4.conf.default.accept_source_route
net.ipv4.conf.default.accept_source_route = 0
```

Remediation:

Set the `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` parameters to 0 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.conf.all.accept_source_route=0
# /sbin/sysctl -w net.ipv4.conf.default.accept_source_route=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: Yes

References:

1. CCE-4236-6
2. CCE-4091-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.2 Disable ICMP Redirect Acceptance (Automated)

Profile Applicability:

- Level 1

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects`, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Audit:

Run the following commands and verify output matches:

```
# /sbin/sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 0
# /sbin/sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 0
```

Remediation:

Set the `net.ipv4.conf.all.accept_redirects` and `net.ipv4.conf.default.accept_redirects` parameters to 0 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0
# /sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: No

References:

1. CCE-4217-6
2. CCE-4186-3

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.3 Disable Secure ICMP Redirect Acceptance (Automated)

Profile Applicability:

- Level 2

Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.

Audit:

Perform the following to determine if ICMP redirect messages will be rejected from known gateways.

```
# /sbin/sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 0
# /sbin/sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 0
```

Remediation:

Set the `net.ipv4.conf.all.secure_redirects` and `net.ipv4.conf.default.secure_redirects` parameters to 0 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.secure_redirects=0
net.ipv4.conf.default.secure_redirects=0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.conf.all.secure_redirects=0
# /sbin/sysctl -w net.ipv4.conf.default.secure_redirects=0
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: No

References:

1. CCE-3472-8
2. CCE-3339-9

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.4 Log Suspicious Packets (Automated)

Profile Applicability:

- Level 1

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their server.

Audit:

Perform the following to determine if suspicious packets are logged.

```
# /sbin/sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 1
```

Remediation:

Set the `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians` parameters to 1 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.conf.all.log_martians=1
# /sbin/sysctl -w net.ipv4.conf.default.log_martians=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: No

References:

1. CCE-4320-8

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.5 Enable Ignore Broadcast Requests (Automated)

Profile Applicability:

- Level 1

Description:

Setting `net.ipv4.icmp_echo_ignore_broadcasts` to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Audit:

Perform the following to determine if all ICMP echo and timestamp requests to broadcast and multicast addresses will be ignored.

```
# /sbin/sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Remediation:

Set the `net.ipv4.icmp_echo_ignore_broadcasts` parameter to 1 in `/etc/sysctl.conf`:

```
net.ipv4.icmp_echo_ignore_broadcasts=1
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: Yes

References:

1. CCE-3644-2

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.6 Enable Bad Error Message Protection (Automated)

Profile Applicability:

- Level 1

Description:

Setting `icmp_ignore_bogus_error_responses` to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Audit:

Perform the following to determine if bogus messages will be ignored.

```
# /sbin/sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remediation:

Set the `net.ipv4.icmp_ignore_bogus_error_responses` parameter to 1 in `/etc/sysctl.conf`:

```
net.ipv4.icmp_ignore_bogus_error_responses=1
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: Yes

References:

1. CCE-4133-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.7 Enable RFC-recommended Source Route Validation (Automated)

Profile Applicability:

- Level 2

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting these flags is a good way to deter attackers from sending your server bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your server, you will not be able to enable this feature without breaking the routing.

Audit:

Perform the following to determine if RFC-recommended source route validation is enabled.

```
# /sbin/sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1
# /sbin/sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1
```

Remediation:

Set the `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` parameters to 1 in `/etc/sysctl.conf`:

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.conf.all.rp_filter=1
# /sbin/sysctl -w net.ipv4.conf.default.rp_filter=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: Yes

References:

1. CCE-4080-8
2. CCE-3840-6

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.8 Enable TCP SYN Cookies (Automated)

Profile Applicability:

- Level 1

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the server to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a server by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the server to keep accepting valid connections, even if under a denial of service attack.

Audit:

Perform the following to determine if TCP SYN Cookies is enabled.

```
# /sbin/sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
```

Remediation:

Set the `net.ipv4.tcp_syncookies` parameter to 1 in `/etc/sysctl.conf`:

```
net.ipv4.tcp_syncookies=1
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv4.tcp_syncookies=1
# /sbin/sysctl -w net.ipv4.route.flush=1
```

Default Value:

OS Default: N/A

References:

1. CCE-4265-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.3 Wireless Networking

4.3.1 Deactivate Wireless Interfaces (Manual)

Profile Applicability:

- Level 1

Description:

Wireless networking is used when wired networks are unavailable. Red Hat contains a wireless tool kit to allow system administrators to configure and use wireless networks.

Rationale:

If wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Audit:

Perform the following to determine if wireless interfaces are active.

```
# ifconfig -a  
Validate that all interfaces using wireless are down.
```

Remediation:

Use the following commands to list all interfaces and identify devices with wireless interfaces. Once identified, shutdown the interface and remove it.

```
# ifconfig -a.  
# iwconfig  
# ifdown interface  
# rm /etc/sysconfig/network-scripts/ifcfg-
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.4 Disable IPv6

IPv6 is a networking protocol that supersedes IPv4. It has more routable addresses and has built in security

4.4.1 Configure IPv6

If IPv6 is to be used, follow this section of the benchmark to configure IPv6.

4.4.1.1 Disable IPv6 Router Advertisements (Automated)

Profile Applicability:

- Level 1

Description:

This setting disables the systems ability to accept router advertisements

Rationale:

It is recommended that systems not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Audit:

Perform the following to determine if the system is disabled from accepting router advertisements:

```
# /sbin/sysctl net.ipv6.conf.all.accept_ra
net.ipv6.conf.all.accept_ra = 0
# /sbin/sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0
```

Remediation:

Set the `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` parameter to 0 in `/etc/sysctl.conf`:

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
# /sbin/sysctl -w net.ipv6.conf.default.accept_ra=0
# /sbin/sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.4.1.2 Disable IPv6 Redirect Acceptance (Automated)

Profile Applicability:

- Level 1

Description:

This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic.

Rationale:

It is recommended that systems not accept ICMP redirects as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Audit:

Perform the following to determine if IPv6 redirects are disabled.

```
# /sbin/sysctl net.ipv6.conf.all.accept_redirects
net.ipv6.conf.all.accept_redirect = 0
# /sbin/sysctl net.ipv6.conf.default.accept_redirects
net.ipv6.conf.default.accept_redirect = 0
```

Remediation:

Set the `net.ipv6.conf.all.accept_redirects` and `net.ipv6.conf.default.accept_redirects` parameters to 0 in `/etc/sysctl.conf`:

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

Run the following commands to set the active kernel parameters:

```
# /sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0
# /sbin/sysctl -w net.ipv6.conf.default.accept_redirects=0
# /sbin/sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.4.2 Disable IPv6 (Manual)

Profile Applicability:

- Level 1

Description:

Although IPv6 has many advantages over IPv4, few organizations have implemented IPv6.

Rationale:

If IPv6 is not to be used, it is recommended that the driver not be installed. While use of IPv6 is not a security issue, it will cause operational slowness as packets are tried via IPv6, when there are no recipients. In addition, disabling unneeded functionality reduces the potential attack surface.

Audit:

Perform the following to determine if IPv6 is enabled

```
# grep ipv6 /etc/modprobe.conf
options ipv6 "disable=1"
```

Remediation:

Run the following command:

```
# echo "options ipv6 \"disable=1\"" >> /etc/modprobe.conf
```

Default Value:

OS Default: N/A

References:

1. CCE-3562-6

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.5 Install TCP Wrappers

4.5.1 Install TCP Wrappers (Automated)

Profile Applicability:

- Level 1

Description:

TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. In the past, services that were called from `inetd` and `xinetd` supported the use of tcp wrappers. As `inetd` and `xinetd` have been falling in disuse, any service that can support tcp wrappers will have the `libwrap.so` library attached to it.

Rationale:

TCP Wrappers provide a good simple access list mechanism to services that may not have that support built in. It is recommended that all services that can support TCP Wrappers, use it.

Audit:

Perform the following to determine if TCP Wrappers is enabled.

```
# yum list tcp-wrappers
tcp_wrappers.
```

Remediation:

Run the following command to install `tcp_wrappers`:

```
# yum install tcp_wrappers
```

To verify if a service supports TCP Wrappers, run the following command:

```
# ldd | grep libwrap.so
```

If there is any output, then the service supports TCP Wrappers.

Default Value:

OS Default: Not installed

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.5.2 Create `/etc/hosts.allow` (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/hosts.allow` file specifies which IP addresses are permitted to connect to the host. It is intended to be used in conjunction with the `etc/hosts.deny` file.

Rationale:

The `/etc/hosts.allow` file supports access control by IP and helps ensure that only authorized systems can connect to the server.

Audit:

Run the following command to verify the contents of the `/etc/hosts.allow` file.

```
# cat /etc/hosts.allow  
  
[contents will vary, depending on your network configuration]
```

Remediation:

Run the following command to create `/etc/hosts.allow`:

```
# echo "ALL: <net>/<mask>, <net>/<mask>, ..." >/etc/hosts.allow
```

where each `<net>/<mask>` combination (for example, "192.168.1.0/255.255.255.0") represents one network block in use by your organization that requires access to this system.

Default Value:

OS Default: Installed

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.5.3 Verify Permissions on /etc/hosts.allow (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/hosts.allow` file contains networking information that is used by many applications and therefore must be readable for these applications to operate.

Rationale:

It is critical to ensure that the `/etc/hosts.allow` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to determine the permissions on the `/etc/hosts.allow` file.

```
# /bin/ls -l /etc/hosts.allow
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.allow
```

Remediation:

Run the following command to remove excess permissions from the `/etc/hosts.allow` file:

```
# /bin/chmod u-x,go-wx /etc/hosts.allow
```

Default Value:

OS Default: Installed

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.5.4 Create `/etc/hosts.deny` (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/hosts.deny` file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the `/etc/hosts.allow` file.

Rationale:

The `/etc/hosts.deny` file serves as a failsafe so that any host not specified in `/etc/hosts.allow` is denied access to the server.

Audit:

Verify that `/etc/hosts.deny` exists and is configured to deny all hosts not explicitly listed in `/etc/hosts.allow`:

```
# cat /etc/hosts.deny
ALL: ALL
```

Remediation:

Run the following command to create `/etc/hosts.deny`:

```
# echo "ALL: ALL" >> /etc/hosts.deny
```

Default Value:

OS Default: Installed

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.5.5 Verify Permissions on /etc/hosts.deny (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/hosts.deny` file contains network information that is used by many system applications and therefore must be readable for these applications to operate.

Rationale:

It is critical to ensure that the `/etc/hosts.deny` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to determine the permissions on the `/etc/hosts.deny` file.

```
# /bin/ls -l /etc/hosts.deny
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/hosts.deny
```

Remediation:

If the permissions of the `/etc/hosts.deny` file are incorrect, run the following command to correct them:

```
# /bin/chmod u-x,go-wx /etc/hosts.deny
```

Default Value:

OS Default: Installed

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.6 Uncommon Network Protocols

Red Hat Linux supports several network protocols that are not commonly used. While vulnerabilities in network coding is rare (a vulnerability was discovered in RDS in October 2010), it can have devastating effects on the security of the system. If these protocols are not needed, it is recommended that they be disabled in the kernel.

4.6.1 Disable DCCP (Automated)

Profile Applicability:

- Level 1

Description:

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

Rationale:

If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Audit:

Perform the following to determine if DCCP is disabled.

```
# grep -e "^\s*install\s+dccp\s+\s+/bin\/(true|false)" /etc/modprobe.conf
install dccp /bin/true
```

Remediation:

Run the following command:

```
# echo "install dccp /bin/true" >> /etc/modprobe.conf
```

Default Value:

OS Default: N/A

References:

1. CCE-14268-7

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.6.2 Disable SCTP (Automated)

Profile Applicability:

- Level 1

Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Perform the following to determine if SCTP is disabled.

```
# grep -e "^s*install\s+sctp\s+\s+/bin\/(true|false)" /etc/modprobe.conf
install sctp /bin/true
```

Remediation:

Run the following command:

```
# echo "install sctp /bin/true" >> /etc/modprobe.conf
```

Default Value:

OS Default: N/A

References:

1. CCE-14132-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.6.3 Disable RDS (Automated)

Profile Applicability:

- Level 1

Description:

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Perform the following to determine if RDS is disabled.

```
# grep -e "^s*install\s+rds\s+\s+/bin\/(true|false)" /etc/modprobe.conf
install rds /bin/true
```

Remediation:

```
# echo "install rds /bin/true" >> /etc/modprobe.conf
```

Default Value:

OS Default: N/A

References:

1. CCE-14027-7

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.6.4 Disable TIPC (Automated)

Profile Applicability:

- Level 1

Description:

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

Perform the following to determine if TIPC is disabled.

```
# grep -e "^s*install\s+tipc\s+\/bin\/(true|false)" /etc/modprobe.conf
install tipc /bin/true
```

Remediation:

Run the following command:

```
# echo "install tipc /bin/true" >> /etc/modprobe.conf
```

Default Value:

OS Default: N/A

References:

1. CCE-14911-2

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.7 Enable IPtables (Automated)

Profile Applicability:

- Level 1

Description:

IPtables is an application that allows a system administrator to configure the IPv4 tables, chains and rules provided by the Linux kernel firewall.

Rationale:

IPtables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv4 addresses and ports.

Audit:

Perform the following to determine if IPtables is enabled.

```
# chkconfig --list iptables
iptables    0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Remediation:

Run the following commands:

```
# service iptables restart
# chkconfig iptables on
```

References:

1. CCE-4189-7

Additional Information:

OS Default: N/A

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.8 Enable IP6tables (Automated)

Profile Applicability:

- Level 1

Description:

IP6tables is an application that allows a system administrator to configure the IPv6 tables, chains and rules provided by the Linux kernel firewall.

Rationale:

Rationale: IP6tables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv6 addresses and ports.

Note: IP6Tables should only be enabled if IPv6 has been enabled on your system.

Audit:

Perform the following to determine if IP6Tables is enabled:

```
# chkconfig --list ip6tables  
  
ip6tables 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Remediation:

Run the following commands:

```
# service ip6tables restart  
# chkconfig ip6tables on
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

5 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included with RHEL5.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the `ntpd(8)` manual page for more information on configuring NTP.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log. Although it is recommended that `rsyslog` be used for logging, guidance for configuring `syslog` is provided in for sites where `rsyslog` does not meet the requirements.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run `setuid` to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

5.1 Configure Syslog

The `syslogd` logging daemon is the default for RHEL and is used by many applications to log activity in accordance with settings in the `/etc/syslog.conf` file. There are some limitations to syslog, such as lack of authentication for client or servers, lack of encryption, or reliable network transportation.

Rationale: Despite the limitations of `syslog`, it is better to configure it properly than to have no or limited logging. If possible, it is recommended that `rsyslog` be used instead.

5.1.1 Configure `/etc/syslog.conf` (Manual)

Profile Applicability:

- Level 1

Description:

The `/etc/syslog.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `syslog` (e.g., successful and failed `su` attempts, failed login attempts, `root` login attempts, etc.).

Audit:

Review the contents of the `/etc/syslog.conf` file to ensure appropriate logging is set. In addition, perform the following command and ensure that the log files are logging information:

```
# ls -l /var/log
```

Remediation:

Edit the following lines in the `/etc/syslog.conf` file as appropriate for your environment:

```
auth,user.* /var/log/messages
kern.* /var/log/kern.log
daemon.* /var/log/daemon.log
syslog.* /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.*
/var/log/unused.log
```

Execute the following command to restart `syslogd`:

```
# pkill -HUP syslogd
```

Default Value:

OS Default: N/A

References:

1. See the `syslog(2)` man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.1.2 Create and Set Permissions on syslog Log Files (Automated)

Profile Applicability:

- Level 1

Description:

A log file must already exist for syslog to be able to write to it.

Rationale:

It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `syslog` data is archived and protected.

Audit:

For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands and verify that the `owner:group` is `root:root` and the permissions are `0600` (for sites that do not use a security group) and `root:<securegrp>` with permissions of `0640` (for sites that use a secure group):

```
# ls -l LOGFILE
```

Remediation:

For sites that have **not** implemented a secure admin group: For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands:

```
# touch <LOGFILE>
# chown root:root <LOGFILE>
# chmod og-rwx <LOGFILE>
```

For sites that **have** implemented a secure admin group: For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands (where is the name of the security group):

```
# touch <LOGFILE>
# chown root:<securegrp> <LOGFILE>
# chmod g-wx,o-rwx <LOGFILE>
```

Default Value:

OS Default: N/A

References:

1. See the `syslog.conf(5)` man page for more information.

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

5.1.3 Configure syslog to Send Logs to a Remote Log Host (Automated)

Profile Applicability:

- Level 1

Description:

The `syslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Audit:

Review the `/etc/syslog.conf` file and verify that logs are sent to a central host (where `logfile.example.com` is the name of your central log host).

```
# grep "^*.*[^I][^I]*@" /etc/syslog.conf
*.* @loghost.example.com
```

Remediation:

Edit the `/etc/syslog.conf` file and add the following line (where `logfile.example.com` is the name of your central log host).

```
*.* @loghost.example.com
```

Execute the following command to restart `syslogd`

```
# pkill -HUP syslogd
```

Default Value:

OS Default: N/A

References:

1. See the `syslog.conf(5)` man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.1.4 Accept Remote syslog Messages Only on Designated Log Hosts (Manual)

Profile Applicability:

- Level 1

Description:

By default, `syslog` on RHEL5 does not listen for log messages coming in from remote systems. The `-r` flag can be used to enable this ability and the `-s` option can be used to strip the domain name from incoming messages to reduce redundant information in log files.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept syslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `syslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

****NOTE:****Since syslog uses UDP to send messages to a remote host, there is no guarantee that the remote host will actually receive all the data. Log messages may be lost, especially on busy sites.

Audit:

Run the following command:

```
# grep SYSLOGD_OPTIONS /etc/sysconfig/syslog
-m 0 -r -s example.com (if designated as a log host)
-m 0 (if not designated as a log host)
```

Remediation:

For each host designated as a log host, edit the `/etc/sysconfig/syslog` file and add the following line:

```
SYSLOGD_OPTIONS="-m 0 -r -s <LOGHOST>"
```

Execute the following command to restart syslogd

```
# pkill -HUP syslogd
```

For hosts that are **not** designated log hosts, edit the `/etc/sysconfig/syslog` file and add the following line:

```
SYSLOGD_OPTIONS="-m 0"
```

Execute the following command to restart syslogd

```
# pkill -HUP syslogd
```

Default Value:

OS Default: No

References:

1. See the `syslog(8)` man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2 Configure rsyslog

The rsyslog software is recommended as a replacement for the default syslogd daemon and provides improvements over syslogd, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

5.2.1 Install the rsyslog package (Automated)

Profile Applicability:

- Level 1

Description:

The `rsyslog` package is a third party package that provides many enhancements to `syslog`, such as multi-threading, TCP communication, message filtering and data base support. As of RHEL 5.2, `rsyslog` is available as part of the core distribution.

Rationale:

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit:

Perform the following command to verify that `rsyslog` is installed.

```
# yum list rsyslog
rsyslog.<hardware platform> <release&> <installed>
```

Remediation:

Run the following command to install `rsyslog`:

```
# yum install rsyslog
```

Default Value:

OS Default: No

References:

1. <http://www.rsyslog.com/docs>

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.2 Activate the rsyslog Service (Automated)

Profile Applicability:

- Level 1

Description:

The `chkconfig` command can be used to ensure that the `syslog` service is turned off and that the `rsyslog` service is turned on.

Rationale:

It is important to ensure that `syslog` is turned off so that it does not interfere with the `rsyslog` service.

Audit:

Run the following commands:

```
# chkconfig --list syslog
syslog 0:off 1:off 2:off 3:off 4:off 5:off 6:off

# chkconfig --list rsyslog
rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Remediation:

Run the following commands:

```
# chkconfig syslog off
# chkconfig rsyslog on
```

Default Value:

OS Default: No

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.3 Configure `/etc/rsyslog.conf` (Manual)

Profile Applicability:

- Level 1

Description:

The `/etc/rsyslog.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed `su` attempts, failed login attempts, `root` login attempts, etc.).

Audit:

Review the contents of the `/etc/rsyslog.conf` file to ensure appropriate logging is set. In addition, perform the following command and ensure that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the following lines in the `/etc/rsyslog.conf` file as appropriate for your environment:

```
auth,user.* /var/log/messages
kern.* /var/log/kern.log
daemon.* /var/log/daemon.log
syslog.* /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.*
/var/log/unused.log
```

Run the following commands:

```
# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

Default Value:

OS Default: No

References:

1. See the `rsyslog.conf(5)` man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.4 Create and Set Permissions on rsyslog Log Files (Automated)

Profile Applicability:

- Level 1

Description:

A log file must already exist for `rsyslog` to be able to write to it.

Rationale:

It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `rsyslog` data is archived and protected.

Audit:

For each listed in the `/etc/rsyslog.conf` file, perform the following command and verify that the `_<owner>_:_<group>_` is `root:root` and the permissions are `0600` (for sites that have not implemented a secure group) and `root:securegrp` with permissions of `0640` (for sites that have implemented a secure group):

```
# ls -l <logfile>
```

Remediation:

For sites that have **not** implemented a secure admin group:

Create the `/var/log/` directory and for each listed in the `/etc/rsyslog.conf` file, perform the following commands:

```
# touch <logfile>
# chown root:root <logfile>
# chmod og-rwx <logfile>
```

For sites that **have** implemented a secure admin group:

Create the `/var/log/` directory and for each listed in the `/etc/rsyslog.conf` file, perform the following commands (where is the name of the security group):

```
# touch <logfile>
# chown root:<securegrp> <logfile>
# chmod g-wx,o-rwx <logfile>
```

Default Value:

OS Default: No

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.5 Configure rsyslog to Send Logs to a Remote Log Host (Automated)

Profile Applicability:

- Level 1

Description:

The `rsyslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Audit:

Review the `/etc/rsyslog.conf` file and verify that logs are sent to a central host (where `logfile.example.com` is the name of your central log host).

```
# grep "^*.*[^\I][^\I]*@" /etc/rsyslog.conf
*.* @@loghost.example.com
```

Remediation:

Edit the `/etc/rsyslog.conf` file and add the following line (where `logfile.example.com` is the name of your central log host).

```
*.* @@loghost.example.com
```

Execute the following command to restart `rsyslogd`

```
# pkill -HUP rsyslogd
```

Note: The double "at" sign (`@@`) directs `rsyslog` to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

Default Value:

OS Default: No

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.6 Accept Remote rsyslog Messages Only on Designated Log Hosts (Manual)

Profile Applicability:

- Level 1

Description:

By default, `rsyslog` does not listen for log messages coming in from remote systems. The `ModLoad` tells `rsyslog` to load the `imtcp.so` module so it can listen over a network via TCP. The `InputTCPServerRun` option instructs `rsyslogd` to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `rsyslog` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `rsyslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Run the following commands:

```
# grep '$ModLoad' /etc/rsyslog.conf
$ModLoad imtcp.so
# grep '$InputTCPServerRun' /etc/rsyslog.conf
$InputTCPServerRun 514
```

Remediation:

For hosts that are designated as log hosts, edit the `/etc/rsyslog.conf` file and add or modify the following lines:

```
$ModLoad imtcp.so
$InputTCPServerRun 514
```

Execute the following command to restart `rsyslogd`:

```
# pkill -HUP rsyslogd
```

Default Value:

OS Default: No

References:

1. See the rsyslog(8) man page for more information.

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.3 Configure System Accounting (*auditd*)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, `auditd` will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

Note: For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems. For 32 bit systems, only one rule is needed.

5.3.1 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

5.3.1.1 Configure Audit Log Storage Size (Manual)

Profile Applicability:

- Level 2

Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:

Perform the following to determine the maximum size of the audit log files.

```
# grep max_log_file /etc/audit/auditd.conf  
max_log_file = <MB>
```

Remediation:

Set the `max_log_file` parameter in `/etc/audit/auditd.conf`

```
max_log_file = <MB>
```

Note: MB is the number of Megabytes the file can be.

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

5.3.1.2 Disable System on Audit Log Full (Manual)

Profile Applicability:

- Level 2

Description:

The `auditd` daemon can be configured to halt the system when the audit logs are full.

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Audit:

Perform the following to determine if `auditd` is configured to notify the administrator and halt the system when audit logs are full.

```
# grep space_left_action /etc/audit/auditd.conf
space_left_action = email
# grep action_mail_acct /etc/audit/auditd.conf
action_mail_acct = root
# grep admin_space_left_action /etc/audit/auditd.conf
admin_space_left_action = halt
```

Remediation:

Add or edit the following lines in the `/etc/audit/auditd.conf` file.

```
space_left_action = email
action_mail_acct = root
admin_space_left_action = halt
```

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

5.3.1.3 Keep All Auditing Information (Automated)

Profile Applicability:

- Level 2

Description:

Normally, `auditd` will hold 4 logs of maximum log file size before deleting older log files.

Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Audit:

Perform the following to determine if audit logs are retained.

```
# grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

Remediation:

Add the following line to the `/etc/audit/auditd.conf` file.

```
max_log_file_action = keep_logs
```

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

5.3.2 Enable auditd Service (Automated)

Profile Applicability:

- Level 2

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Perform the following to determine if `auditd` is enabled.

```
# chkconfig --list auditd
auditd: 0: off 1: off 2: on 3: on 4: on 5: on 6: off
```

Remediation:

Run the following command to enable `auditd`:

```
# chkconfig auditd on
```

Default Value:

OS Default: N/A

References:

1. CCE-4292-9

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.3.3 Keep All Auditing Information (Automated)

Profile Applicability:

- Level 2

Description:

Normally, `auditd` will hold 4 logs of maximum log file size before deleting older log files.

Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Audit:

Perform the following to determine if audit logs are retained.

```
# grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

Remediation:

Add the following line to the `/etc/audit/auditd.conf` file.

```
max_log_file_action = keep_logs
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.3.4 Enable Auditing for Processes That Start Prior to auditd (Automated)

Profile Applicability:

- Level 2

Description:

Configure `grub` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

Perform the following to determine if `/etc/grub.conf` is configured to log processes that start prior to `auditd`.

```
# grep "audit=1" /etc/grub.conf
```

Make sure each line that starts with `kernel` has the `audit=1` parameter set.

Remediation:

Run the following:

```
# ed /etc/grub.conf << END
g/kernel/s/$/ audit=1/
w
q
END
```

Default Value:

OS Default: N/A

References:

1. CCE-15026-8

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.3.5 Record Events That Modify Date and Time Information (Automated)

Profile Applicability:

- Level 2

Description:

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the `adjtimex` (tune kernel clock), `settimeofday` (Set time, using `timeval` and `timezone` structures) `stime` (using seconds since 1/1/1970) or `clock_settime` (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the `/var/log/audit.log` file upon exit, tagging the records with the identifier "time-change"

Rationale:

Unexpected changes in system data and/or time could be a sign of malicious activity on the system.

Audit:

Perform the following to determine if events where the system date and/or time has been modified are captured.

On a 64 bit system, perform the following command and ensure the output is as shown.

```
# grep time_change /etc/audit/audit.rules

-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

On a 32 bit system, perform the following command and ensure the output is as shown.

```
# grep time_change /etc/audit/audit.rules

-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.6 Record Events That Modify User/Group Information (Automated)

Profile Applicability:

- Level 2

Description:

Record events affecting the `group`, `passwd` (user IDs), `shadow` and `gshadow` (passwords) or `/etc/security/opasswd` (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit:

Perform the following to determine if events that modify user/group information are recorded.

```
# grep identity /etc/audit/audit.rules

-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14829-6

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.7 Record Events That Modify the System's Network Environment (Automated)

Profile Applicability:

- Level 2

Description:

Record changes to network environment files or system calls. The below parameters monitor the `sethostname` (set the systems host name) or `setdomainname` (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the `/etc/issue` and `/etc/issue.net` files (messages displayed pre-login), `/etc/hosts` (file containing host names and associated IP addresses) and `/etc/sysconfig/network` (directory containing network interface scripts and configurations) files.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Audit:

On a 64 bit system, perform the following command and ensure the output is as shown to determine if events that modify the system's environment are recorded.

```
# grep system-locale /etc/audit/audit.rules

-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if events that modify the system's environment are recorded.

```
# grep system-locale /etc/audit/audit.rules

-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14816-3

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.8 Record Events That Modify the System's Mandatory Access Controls (Automated)

Profile Applicability:

- Level 2

Description:

Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the `/etc/selinux` directory.

Rationale:

Changes to files in this directory could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit:

Perform the following to determine if events that modify the system's mandatory access controls are recorded

```
# grep MAC_policy /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
```

Remediation:

Add the following line to the `/etc/audit/audit.rules` file.

```
-w /etc/selinux/ -p wa -k MAC-policy
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14821-3

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.9 Collect Login and Logout Events (Automated)

Profile Applicability:

- Level 2

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file `/var/log/faillog` tracks failed events from login. The file `/var/log/lastlog` maintain records of the last time a user successfully logged in. The file `/var/log/tallylog` maintains a tally of failed logins associated with programs that use pam for authentication and have the `pam_tally2.so` module configured. The file `/var/log/btmp` keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`. All audit records will be tagged with the identifier "logins."

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

Perform the following to determine if login and logout events are recorded.

```
# grep logins /etc/audit/audit.rules  
  
-w /var/log/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -p wa -k logins  
-w /var/log/btmp -p wa -k session
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /var/log/faillog -p wa -k logins  
-w /var/log/lastlog -p wa -k logins  
-w /var/log/tallylog -p wa -k logins  
-w /var/log/btmp -p wa -k session
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14904-7

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.13 Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

5.3.10 Collect Session Initiation Information (Automated)

Profile Applicability:

- Level 2

Description:

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file `/var/run/utmp` file tracks all currently logged in users. The `/var/log/wtmp` file tracks logins, logouts, shutdown and reboot events. All audit records will be tagged with the identifier "session."

Rationale:

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Audit:

Perform the following to determine if session initiation information is collected.

```
# grep session /etc/audit/audit.rules  
  
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k session
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k session
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Note: Use the last command to read `/var/log/wtmp` (last with no parameters) and `/var/run/utmp` (last `-f /var/run/utmp`)

Default Value:

OS Default: N/A

References:

1. CCE-14679-5

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login

Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.13 Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

5.3.11 Collect Discretionary Access Control Permission Modification Events (Automated)

Profile Applicability:

- Level 2

Description:

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The `chmod`, `fchmod` and `fchmodat` system calls affect the permissions associated with a file. The `chown`, `fchown`, `fchownat` and `lchown` system calls affect owner and group attributes on a file. The `setxattr`, `lsetxattr`, `fsetxattr` (set extended file attributes) and `removexattr`, `lremovexattr`, `fremovexattr` (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system userids (`auid >= 500`) and will ignore Daemon events (`auid = 4294967295`). All audit records will be tagged with the identifier "perm_mod."

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

For 64 bit systems, perform the following command and ensure the output is as shown to determine if permission modifications are being recorded.

```
# grep perm_mod /etc/audit/audit.rules

-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if permission modifications are being recorded.

```
# grep perm_mod /etc/audit/audit.rules

-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14058-2

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.12 Collect Unsuccessful Unauthorized Access Attempts to Files (Automated)

Profile Applicability:

- Level 2

Description:

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (`creat`), opening (`open`, `openat`) and truncation (`truncate`, `ftruncate`) of files. An audit log record will only be written if the user is a non-privileged user (`auid > = 500`), is not a Daemon event (`auid=4294967295`) and if the system call returned `EACCES` (permission denied to the file) or `EPERM` (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access."

Rationale:

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Audit:

On 64 bit systems, perform the following command and ensure the output is as shown to determine if there are unsuccessful attempts to access files.

```
# grep access /etc/audit/audit.rules

-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

On 32 bit systems, perform the following command and ensure the output is as shown to determine if there are unsuccessful attempts to access files.

```
# grep access /etc/audit/audit.rules

-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14917-9

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data

Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

5.3.13 Collect Use of Privileged Commands (Automated)

Profile Applicability:

- Level 2

Description:

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing `<partition>` with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=" $(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs) "' -F auid!=4294967295 -k
privileged" }'
```

Verify all resulting lines are the `/etc/audit/audit.rules` file

Remediation:

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them.

The audit parameters associated with this are as follows:

- -F path=" \$1 "-" will populate each file name found through the find command and processed by awk.
- -F perm=x - will write an audit record if the file is executed.
- -F auid>=500 - will write a record if the user executing the command is not a privileged user.
- -F auid!= 4294967295 - will ignore Daemon events

All audit records should be tagged with the identifier "privileged".

Run the following command replacing with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>="$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"}' -F auid!=4294967295 -k
privileged" }'
```

Edit the `/etc/audit/audit.rules` file.

Example:

```
# find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a
always,exit -F path=" $1 " -F perm=x -F auid>="$(awk '/^\s*UID_MIN/{print
$2}' /etc/login.defs)"}' -F auid!=4294967295 -k privileged" }' >>
/etc/audit/audit.rules
```

Default Value:

OS Default: N/A

References:

1. CCE-14296-8

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.14 Collect Successful File System Mounts (Automated)

Profile Applicability:

- Level 2

Description:

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user

Rationale:

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

****Note:****This tracks successful and unsuccessful `mount` commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS)

Audit:

For 64 bit systems perform the following command and ensure the output is as shown to determine if filesystem mounts are recorded.

```
# grep mounts /etc/audit/audit.rules  
  
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts  
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts
```

For 32 bit systems perform the following command and ensure the output is as shown to determine if filesystem mounts are recorded.

```
# grep mounts /etc/audit/audit.rules  
  
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts  
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k  
mounts
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-4024-6

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.3.15 Collect File Deletion Events by User (Automated)

Profile Applicability:

- Level 2

Description:

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the `unlink` (remove a file), `unlinkat` (remove a file attribute), `rename` (rename a file) and `renameat` (rename a file attribute) system calls and tags them with the identifier "delete".

Rationale:

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Audit:

For 64 bit systems, perform the following command and ensure the output is as shown to determine if file deletion events by user are recorded.

```
# grep delete /etc/audit/audit.rules

-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
aid>=500 -F aid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
aid>=500 -F aid!=4294967295 -k delete
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if file deletion events by user are recorded.

```
# grep delete /etc/audit/audit.rules

-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
aid>=500 -F aid!=4294967295 -k delete
```

Remediation:

At a minimum, configure the audit system to collect file deletion events for all users and root.

For 64 bit systems, add the following to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
aid>=500 -F aid!=4294967295 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
aid>=500 -F aid!=4294967295 -k delete
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

For 32 bit systems, add the following to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
aid>=500 -F aid!=4294967295 -k delete
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14820-5

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.3.16 Collect Changes to System Administration Scope (sudoers) (Automated)

Profile Applicability:

- Level 2

Description:

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers` will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier "scope."

Rationale:

Changes in the `/etc/sudoers` file can indicate that an unauthorized change has been made to scope of system administrator activity.

Audit:

Perform the following to determine if changes to `/etc/sudoers` are recorded.

```
# grep scope /etc/audit/audit.rules  
-w /etc/sudoers -p wa -k scope
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /etc/sudoers -p wa -k scope
```

Execute the following command to restart auditd

```
# pkill -P 1-HUP auditd
```

Default Value:

OS Default: N/A

References:

1. CCE-14824-7

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.17 Collect System Administrator Actions (sudolog) (Automated)

Profile Applicability:

- Level 2

Description:

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale:

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Audit:

Perform the following to determine if administrator activity is recorded.

```
# grep actions /etc/audit/audit.rules  
-w /var/log/sudo.log -p wa -k actions
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /var/log/sudo.log -p wa -k actions
```

Execute the following command to restart `auditd`

```
# pkill -P 1-HUP auditd
```

Note: The system must be configured with `su` disabled (See Item 7.6 Restrict Access to the `su` Command) to force all command execution through `sudo`. This will not be effective on the console, as administrators can log in as root.

Default Value:

OS Default: N/A

References:

1. CCE-14824-7

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.18 Collect Kernel Module Loading and Unloading (Automated)

Profile Applicability:

- Level 2

Description:

Monitor the loading and unloading of kernel modules. The programs `insmod` (install a kernel module), `rmmod` (remove a kernel module), and `modprobe` (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The `init_module` (load a module) and `delete_module` (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules".

Rationale:

Monitoring the use of `insmod`, `rmmod` and `modprobe` could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the `init_module` and `delete_module` system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Audit:

Perform the following to determine if kernel module loading and unloading is recorded.

```
# grep modules /etc/audit/audit.rules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -S init_module -S delete_module -k modules
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -S init_module -S delete_module -k modules
```

Default Value:

OS Default: N/A

References:

1. CCE-14688-6

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems

Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

5.3.19 Make the Audit Configuration Immutable (Automated)

Profile Applicability:

- Level 2

Description:

Set system audit so that audit rules cannot be modified with `auditctl`. Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

Rationale:

In immutable mode, unauthorized users cannot execute changes to the audit system to potential hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Audit:

Perform the following to determine if the audit configuration is immutable.

```
# grep "^-e 2" /etc/audit/audit.rules  
-e 2
```

Remediation:

Add the following lines to the `/etc/audit/audit.rules` file.

```
-e 2
```

Note: This must be the last entry in the `/etc/audit/audit.rules` file

Default Value:

OS Default: N/A

References:

1. CCE-14692-8

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.4 Configure logrotate (Manual)

Profile Applicability:

- Level 1

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageable large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`. These files are rotated on a weekly basis via a cron job and the last 4 weeks are kept.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Perform the following to determine if the appropriate system logs are rotated.

```
# grep '{' /etc/logrotate.d/syslog  
  
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler  
/var/log/boot.log /var/log/cron {
```

Remediation:

Edit the `/etc/logrotate.d/syslog` file to include appropriate system logs:

```
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler  
/var/log/boot.log /var/log/cron {
```

Default Value:

OS Default: Yes

References:

1. CCE-4182-2

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6 System Access, Authentication and Authorization

6.1 Configure cron and anacron

6.1.1 Enable anacron Daemon (Automated)

Profile Applicability:

- Level 2

Description:

The `anacron` daemon is used on systems that are not up 24x7. The `anacron` daemon will execute jobs that would have normally been run had the system not been down

Rationale:

Cron jobs may include critical security or administrative functions that need to run on a regular basis. Use this daemon on machines that are not up 24x7, or if there are jobs that need to be executed after the system has been brought back up after a maintenance window.

Audit:

Perform the following to determine if `anacron` is enabled.

```
# chkconfig --list anacron
anacron: 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Remediation:

Run the following command:

```
# chkconfig anacron on
```

Note: NSA Guidance recommends disabling `anacron` for systems that are intended to be up 24X7, with the rationale that unnecessary software should be disabled to reduce risk. However, even systems that are designed to be up at all times can experience downtime that could prevent important system maintenance jobs from running. Review the requirements for your site to determine your appropriate risk level.

Default Value:

OS Default: Enabled

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.1.2 Enable cron Daemon (Automated)

Profile Applicability:

- Level 1

Description:

The `cron` daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run and `cron` is used to execute them.

Audit:

Perform the following to determine if `cron` is enabled.

```
# chkconfig --list crond  
  
cron: 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

Remediation:

Run the following command to enable `cron`:

```
# chkconfig crond on
```

Default Value:

OS Default: Enabled

References:

1. CCE-4324-0

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.1.3 Set User/Group Owner and Permission on /etc/anacrontab (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/anacrontab` file is used by `anacron` to control its own jobs. The commands in this item make sure that `root` is the user and group owner of the file and is the only user that can read and write the file.

Rationale:

This file contains information on what system jobs are run by `anacron`. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

Perform the following to determine if the `/etc/anacrontab` file has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/anacrontab | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on `/etc/anacrontab`:

```
# chown root:root /etc/anacrontab
# chmod og-rwx /etc/anacrontab
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.4 Set User/Group Owner and Permission on /etc/crontab (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make here sure that root is the user and group owner of the file and is the only user that can read and write the file.

Rationale:

This file contains information on what system jobs are run by `cron`. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

Perform the following to determine if the `/etc/crontab` file has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/crontab | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

Default Value:

OS Default: N/A

References:

1. CCE-3626-9
2. CCE-3851-3
3. CCE-4388-5

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.5 Set User/Group Owner and Permission on /etc/cron.hourly (Automated)

Profile Applicability:

- Level 1

Description:

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Perform the following to determine if the `/etc/cron.hourly` directory has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/cron.hourly | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on the `/etc/cron.hourly` directory:

```
# chown root:root /etc/cron.hourly
# chmod og-rwx /etc/cron.hourly
```

Default Value:

OS Default: N/A

References:

1. CCE-4054-3
2. CCE-3983-4
3. CCE-4106-1

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.6 Set User/Group Owner and Permission on /etc/cron.daily (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.daily` directory contains system `cron` jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Perform the following to determine if the `/etc/cron.daily` directory has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/cron.daily | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

Default Value:

OS Default: N/A

References:

1. CCE-3481-9
2. CCE-4022-0
3. CCE-4450-3

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.7 Set User/Group Owner and Permission on /etc/cron.weekly (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.weekly` directory contains system `cron` jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Perform the following to determine if the `/etc/cron.weekly` directory has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/cron.weekly | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly
# chmod og-rwx /etc/cron.weekly
```

Default Value:

OS Default: N/A

References:

1. CCE-4331-5
2. CCE-3833-1
3. CCE-4203-6

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.8 Set User/Group Owner and Permission on /etc/cron.monthly (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.monthly` directory contains system `cron` jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Perform the following to determine if the `/etc/cron.monthly` directory has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/cron.monthly | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

Default Value:

OS Default: N/A

References:

1. CCE-4322-4
2. CCE-4441-2
3. CCE-4251-5

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.9 Set User/Group Owner and Permission on /etc/cron.d (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily, weekly, and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

Perform the following to determine if the `/etc/cron.d` directory has the correct permissions.

```
# stat -L -c "%a %u %g" /etc/cron.d | egrep ".00 0 0"
```

If the above command emits no output then the system is not configured as recommended.

Remediation:

Run the following commands to update the owner, group, and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

Default Value:

OS Default: N/A

References:

1. CCE-4212-7
2. CCE-4380-2
3. CCE-4250-7

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.10 Restrict at/cron to Authorized Users (Automated)

Profile Applicability:

- Level 1

Description:

Configure `/etc/cron.allow` and `/etc/at.allow` to allow specific users to use these services. If `/etc/cron.allow` or `/etc/at.allow` do not exist, then `/etc/at.deny` and `/etc/cron.deny` are checked. Any user not specifically defined in those files is allowed to use `at` and `cron`. By removing the files, only users in `/etc/cron.allow` and `/etc/at.allow` are allowed to use `at` and `cron`. Note that even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user. The `cron.allow` file only controls administrative access to the `crontab` command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule `cron` jobs. Using the `cron.allow` file to control who can run `cron` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

Perform the following to determine if the remediation in the section has been performed:

```
# ls -l /etc/cron.deny
[no output returned]
# ls -l /etc/at.deny
[no output returned]
# ls -l /etc/cron.allow
-rw----- 1 root root <date> /etc/cron.allow
# ls -l /etc/at.allow
-rw----- 1 root root <date> /etc/at.allow
```

Remediation:

Run the following command to remove `/etc/cron.deny`:

```
# /bin/rm /etc/cron.deny
```

Run the following command to remove `/etc/at.deny`:

```
# /bin/rm /etc/at.deny
```

Run the following command to create `/etc/cron.allow`

```
# touch /etc/cron.allow
```

Run the following command to create `/etc/at.allow`:

```
# touch /etc/at.allow
```

Run the following commands to update the owner, group, and permissions on `/etc/cron.allow`

```
# chmod og-rwx /etc/cron.allow  
# chown root:root /etc/cron.allow
```

Run the following commands to update the owner, group, and permissions on `/etc/at.allow`

Run the following command to create `/etc/at.allow`:

```
# chmod og-rwx /etc/at.allow  
# chown root:root /etc/at.allow
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2 Configure SSH

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`.

Rationale: It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

6.2.1 Set SSH Protocol to 2 (Automated)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^Protocol" /etc/ssh/sshd_config  
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

Default Value:

OS Default: Yes

References:

1. CCE-4245-7
2. <http://www.ssh.com/company/newsroom/article/210/>

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2.2 Set LogLevel to INFO (Automated)

Profile Applicability:

- Level 1

Description:

The `INFO` parameter specifies that record login and logout activity will be logged.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. The "`DEBUG`" is specifically *not* recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information. The "`INFO`" level is the basic level that only records login activity of SSH users. The `VERBOSE` level records both login and logout activity. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^LogLevel" /etc/ssh/sshd_config
LogLevel INFO
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel INFO
```

Default Value:

OS Default: No

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6.2.3 Set Permissions on /etc/ssh/sshd_config (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to root.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to determine the user and group ownership on the `/etc/ssh/sshd_config` file.

```
# /bin/ls -l /etc/ssh/sshd_config
-rw-r--r-- 1 root root 762 Sep 23 002 /etc/ssh/sshd_config
```

Remediation:

Run the following command to change the user and group ownership of `/etc/ssh/sshd_config` to the root user:

```
# chown root:root /etc/ssh/sshd_config
```

Run the following command to remove excess permissions from `/etc/ssh/sshd_config`:

```
# chmod u-x,go-wx 644 /etc/ssh/sshd_config
```

Default Value:

OS Default: Yes

References:

1. CCE-3958-6
2. CCE-3495-9

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2.4 Disable SSH X11 Forwarding (Automated)

Profile Applicability:

- Level 1

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^X11Forwarding" /etc/ssh/sshd_config
X11Forwarding no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

Default Value:

OS Default: No

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2.5 Set SSH MaxAuthTries to 4 or Less (Automated)

Profile Applicability:

- Level 1

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, it is set the number based on site policy.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^MaxAuthTries" /etc/ssh/sshd_config  
MaxAuthTries 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

OS Default: No

CIS Controls:

Version 7

16.13 Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

6.2.6 Set SSH IgnoreRhosts to Yes (Automated)

Profile Applicability:

- Level 1

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` OR `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with `ssh`.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^IgnoreRhosts" /etc/ssh/sshd_config
IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

OS Default: No

References:

1. CCE-4250-7

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2.7 Set SSH HostbasedAuthentication to No (Automated)

Profile Applicability:

- Level 1

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

OS Default: No

References:

1. CCE-4251-5

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2.8 Disable SSH Root Login (Automated)

Profile Applicability:

- Level 1

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using `ssh(1)`. The default is `no`.

Rationale:

Disallowing root logins over SSH requires server admins to authenticate using their own individual account, then escalating to root via `sudo` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^PermitRootLogin" /etc/ssh/sshd_config
PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

OS Default: No

References:

1. CCE-4252-3

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

6.2.9 Set SSH PermitEmptyPasswords to No (Automated)

Profile Applicability:

- Level 1

Description:

The `PermitEmptyPasswords` parameter specifies if the server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^PermitEmptyPasswords" /etc/ssh/sshd_config
PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

OS Default: No

References:

1. CCE-4256-4

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

6.2.10 Do Not Allow Users to Set Environment Options (Automated)

Profile Applicability:

- Level 1

Description:

The `PermitUserEnvironment` option allows users to present environment options to the `ssh` daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has `ssh` executing trojan'd programs)

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep PermitUserEnvironment /etc/ssh/sshd_config
PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

OS Default: No

References:

1. CCE-4265-5

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2.11 Use Only Approved Ciphers in Counter Mode (Automated)

Profile Applicability:

- Level 1

Description:

This variable limits the types of ciphers that SSH can use during communication.

Rationale:

Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBC) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "Ciphers" /etc/ssh/sshd_config  
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

Default Value:

OS Default: No

References:

1. CCE-4269-7
2. For more information on the Counter mode algorithms, read RFC4344 at <http://www.ietf.org/rfc4344.txt>.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.2.12 Set Idle Timeout Interval for User Login (Manual)

Profile Applicability:

- Level 1

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of `ssh` sessions. When the `ClientAliveInterval` variable is set, `ssh` sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, `sshd` will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response from the client, the `ssh` session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client `ssh` session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's `ssh` session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Audit:

To verify the correct SSH setting, run the following commands and verify that the output is as shown:

```
# grep "^ClientAliveInterval" /etc/ssh/sshd_config
ClientAliveInterval 300
# grep "^ClientAliveCountMax" /etc/ssh/sshd_config
ClientAliveCountMax 0
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters as follows:

```
ClientAliveInterval 300  
ClientAliveCountMax 0
```

Default Value:

OS Default: N/A

References:

1. CCE-4247-3

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

6.2.13 Limit Access via SSH (Automated)

Profile Applicability:

- Level 1

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

AllowUsersThe `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.

AllowGroupsThe `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of comma separated user names. Numeric groupIDs are not recognized with this variable.

DenyUsersThe `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.

DenyGroupsThe `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

To verify the correct SSH setting, run the following commands and verify that at least one commands' output is as shown:

```
# grep "^AllowUsers" /etc/ssh/sshd_config
AllowUsers <userlist>

# grep "^AllowGroups" /etc/ssh/sshd_config
AllowGroups <grouplist>

# grep "^DenyUsers" /etc/ssh/sshd_config
DenyUsers <userlist>

# grep "^DenyGroups" /etc/ssh/sshd_config
DenyGroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set at least one of the parameters as follows:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

Default Value:

OS Default: No

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

6.2.14 Set SSH Banner (Automated)

Profile Applicability:

- Level 1

Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Consult with your legal department for the appropriate warning banner for your site.

Audit:

To verify the correct SSH setting, run the following command and verify that `<bannerfile>` is either `/etc/issue` or `/etc/issue.net`:

```
# grep "^Banner" /etc/ssh/sshd_config
Banner <bannerfile>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

Default Value:

OS Default: No

References:

1. CCE-4260-6

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2.15 Enable SSH UsePrivilegeSeparation (Automated)

Profile Applicability:

- Level 1

Description:

The `UsePrivilegeSeparation` parameter causes `sshd` to use a non-root process for pre-authorization work, then launch a new process under the context of the authenticated user.

Rationale:

Separating pre and post authorization processes reduces the probability of a pre-authorization vulnerability in SSHD resulting in root access.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "UsePrivilegeSeparation" /etc/ssh/sshd_config
UsePrivilegeSeparation yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
UsePrivilegeSeparation yes
```

Note: `UsePrivilegeSeparation` defaults to `yes` if not present in configuration.

Default Value:

`yes`

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

6.3 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

6.3.1 Set Password Creation Requirement Parameters Using *pam_cracklib* (Automated)

Profile Applicability:

- Level 1

Description:

The `pam_cracklib` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the `pam_cracklib.so` options.

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - allow three tries before sending back a failure.
- `minlen=14` - password must be 14 characters or more
- `dcredit=-1` - provide at least one digit
- `ucredit=-1` - provide at least one uppercase character
- `ocredit=-1` - provide at least one special character
- `lcredit=-1` - provide at least one lowercase character

The setting shown above is one possible policy. Alter these values to conform to your own organization's password policies.

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Perform the following to determine the current settings in the `pam_cracklib.so` file.

```
# grep pam_cracklib.so /etc/pam.d/system-auth
password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Remediation:

Set the `pam_cracklib.so` parameters as follows in `/etc/pam.d/system-auth`:

```
password required pam_cracklib.so try_first_pass retry=3 minlen=14 dcredit=-1
ucredit=-1 ocredit=-1 lcredit=-1
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.3.2 Set Lockout for Failed Password Attempts (Manual)

Profile Applicability:

- Level 1

Description:

Lock out userIDs after n unsuccessful consecutive login attempts. The first set of changes are made to the main PAM configuration file `/etc/pam.d/system-auth`. The second set of changes are applied to the program specific PAM configuration file (in this case, the `ssh` daemon). The second set of changes must be applied to each program that will lock out userIDs's.

Set the lockout number to the policy in effect at your site.

Rationale:

Locking out userIDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Perform the following to determine the current settings for userID lockout.

```
# grep "pam_tally2" /etc/pam.d/system-auth
auth required pam_tally2.so deny=5 onerr=fail
```

Remediation:

```
# sed -i "5i\auth\required\pam_tally2.so deny=5 onerr=fail"
/etc/pam.d/system-auth
```

Note:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` module, the user can be unlocked by issuing the command:

```
# /usr/sbin/pam\_tally2 -u --reset=0
```

This command sets the failed tally count to 0, effectively unlocking the userid.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16.7 Establish Process for Revoking Access

Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

6.3.3 Use `pam_deny.so` to Deny Services (Manual)

Profile Applicability:

- Level 1

Description:

Adding `pam_deny.so` as a requisite to a PAM aware service allows you to quickly disable the service. The requisite tag on the `auth` line tells PAM that authentication must fail if the name module returns a failure. Since `pam_deny.so` always returns failure, authentication will always fail for this service. This mechanism can be applied to any other PAM aware service on the system.

Rationale:

While there are other ways to disable a service, adding `pam_deny.so` allows you to disable the service for new users without affecting current users of the service.

Audit:

Perform the following to determine if `pam_deny.so` is a requisite in the service. Perform this command for each PAM-aware authentication service.

```
# grep "^auth" /etc/pam.d/sshd
auth requisite pam_deny.so
```

Remediation:

Edit PAM aware services as shown below. For example the `sshd` service would be modified by editing the `/etc/pam.d/sshd` file as shown:

```
auth requisite pam_deny.so
```

Note: Perform this action for every service that provides authentication and supports PAM.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16.7 Establish Process for Revoking Access

Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

6.3.4 Upgrade Password Hashing Algorithm to SHA-512 (Automated)

Profile Applicability:

- Level 1

Description:

The SHA-512 encryption has been available since Red Hat release 5.2,. The commands below change password encryption from `md5` to `sha512` (a much stronger encryption algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Audit:

Perform the following to determine if the password-hashing algorithm is set to SHA-512:

```
# authconfig --test | grep hashing | grep sha512
```

If the above command emits no output then the system is not configured as recommended

Remediation:

Perform the following to configure the system as recommended:

```
# authconfig --passalgo=sha512 --update
```

Note: If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all userID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '( $3 >=500 && $1 != "nfsnobody" ) { print $1 }' /etc/passwd |  
xargs -n 1 chage -d 0
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

6.3.5 Limit Password Reuse (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Audit:

Perform the following to determine the current setting for reuse of older passwords:

```
# grep "remember" /etc/pam.d/system-auth
password sufficient pam_unix.so remember=5
```

Remediation:

Set the `pam_unix.so remember` parameter to 5 or more in `/etc/pam.d/system_auth`:

```
password sufficient pam_unix.so remember=5
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.3.6 Remove the pam_ccreds Package (Automated)

Profile Applicability:

- Level 2

Description:

The `pam_ccreds` module provides the ability for Linux users to locally authenticate using an enterprise identity when the network is unavailable.

Rationale:

While cached credentials provide flexibility in allowing enterprise users to authenticate when not attached to the network, it provides attackers with the ability of compromising those credentials if they've compromised the system.

Audit:

Perform the following to determine if users are not permitted to use cached credentials:

```
# yum list pam_ccreds  
pam_ccreds.<platform> <other items> <anything but installed>
```

Remediation:

Run the following command to remove `pam_ccreds`:

```
# yum erase pam_ccreds
```

Default Value:

OS Default: N/A

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

6.4 Restrict root Login to System Console (Manual)

Profile Applicability:

- Level 1

Description:

The file `/etc/securetty` contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Audit:

Check the `/etc/securetty` for any insecure terminals:

```
# cat /etc/securetty
```

Remediation:

Remove entries for any consoles that are not in a physically secure location.

Default Value:

OS Default: N/A

References:

1. CCE-3485-0

CIS Controls:

Version 7

4 [Controlled Use of Administrative Privileges](#)
Controlled Use of Administrative Privileges

6.5 Restrict Access to the su Command (Automated)

Profile Applicability:

- Level 1

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in the `wheel` group to execute `su`.

Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The `sudo` utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following commands and verify similar output:

```
# grep pam_wheel.so /etc/pam.d/su
auth required pam_wheel.so use_uid
# grep wheel /etc/group
wheel:x:10:root, <user list>
```

Remediation:

Set the `pam_wheel.so` parameters as follows in `/etc/pam.d/su`:

```
auth required pam_wheel.so use_uid
```

Set the proper list of users to be included in the `wheel` group in `/etc/groups`.

Default Value:

OS Default: No

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges

Controlled Use of Administrative Privileges

7 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment. Guidance for monitoring these settings and others that may change over time is provided in Section 9 System Maintenance.

7.1 Set Shadow Password Suite Parameters (/etc/login.defs)

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If userIDs are added a different way, use the `chage` command to effect changes to individual userIDs.

7.1.1 Set Password Expiration Days (Automated)

Profile Applicability:

- Level 1

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 90 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following commands and verify output matches:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 90
# chage --list <user>
Maximum number of days between password change: 90
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to 90 in `/etc/login.defs`:

```
PASS_MAX_DAYS 90
```

Modify active user parameters to match:

```
# chage --maxdays 90 <user>
```

Default Value:

OS Default: No

CIS Controls:

Version 7

16.10 Ensure All Accounts Have An Expiration Date

Ensure that all accounts have an expiration date that is monitored and enforced.

7.1.2 Set Password Change Minimum Number of Days (Automated)

Profile Applicability:

- Level 1

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following commands and verify the output

```
# grep PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 7
# chage --list <user>
Minimum number of days between password change: 7
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 7 in `/etc/login.defs`:

```
PASS_MIN_DAYS 7
```

Modify active user parameters to match:

```
# chage --mindays 7 <user>
```

Default Value:

OS Default: No

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

7.1.3 Set Password Expiring Warning Days (Automated)

Profile Applicability:

- Level 1

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following commands and verify the output

```
# grep PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
# chage --list <user>
Number of days of warning before password expires: 7
```

Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs`:

```
PASS_WARN_AGE 7
```

Modify active user parameters to match:

```
# chage --warndays 7 <user>
```

Default Value:

OS Default: No

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

7.2 Disable System Accounts (Automated)

Profile Applicability:

- Level 1

Description:

There are a number of accounts provided with the Red Hat that are used to manage applications and are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are locked to prevent them from being used to provide an interactive shell. By default, Red Hat sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to `/sbin/nologin`. This prevents the account from potentially being used to run any commands.

Audit:

Run the following commands and verify no results are returned:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="$(which nologin)"' && $7!="/bin/false") {print}' /etc/passwd
```

Remediation:

The following command will set all system accounts to a non login shell:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="$(which nologin)"' && $7!="/bin/false" && $7!="/usr/bin/false") {print $1}' /etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user"; done
```

Default Value:

OS Default: No

References:

1. CCE-4060-0

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

7.3 Set Default Group for root Account (Automated)

Profile Applicability:

- Level 1

Description:

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the `_root_` account helps prevent `root`-owned files from accidentally becoming accessible to non-privileged users.

Audit:

Run the following command and verify the output.

```
# grep root /etc/passwd | cut -f4 -d:  
0
```

Remediation:

Run the following command to assign gid 0 to root:

```
# usermod -g 0 root
```

Default Value:

OS Default: No

References:

1. CCE-4060-0

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

7.4 Set Default umask for Users (Automated)

Profile Applicability:

- Level 1

Description:

The default `umask` determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the `chmod` command. Users who wish to allow their files and directories to be readable by others by default may choose a different default `umask` by inserting the `umask` command into the standard shell configuration files (`.profile`, `.cshrc`, etc.) in their home directories.

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Note: The directives in this section apply to `bash` and `shell`. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Audit:

Run the following commands and verify output

```
# grep "^umask 077" /etc/bashrc
umask 077
# grep "^umask 077" /etc/profile.d/*
umask 077
```

Remediation:

Edit the `/etc/bashrc` and `/etc/profile.d/cis.sh` files (and the appropriate files for any other shell supported on your system) and add the following the `UMASK` parameter as shown:

```
umask 077
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

7.5 Lock Inactive User Accounts (Automated)

Profile Applicability:

- Level 1

Description:

Guidelines published by the U.S. Department of Defense specify that user accounts must be locked out after 35 days of inactivity. This number may vary based on the particular site's policy.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify INACTIVE conforms to site policy (no greater than 35 days):

```
# useradd -D | grep INACTIVE
```

Remediation:

Run the following command to set the default password inactivity period to 35 days:

```
# useradd -D -f 35
```

Default Value:

OS Default: No

References:

1. CCE-4060-0

CIS Controls:

Version 7

16.9 Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

8 Warning Banners

Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system. Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at <http://www.justice.gov/criminal/cybercrime/>

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

8.1 Set Warning Banner for Standard Login Services

8.1.1 Set Warning Banner for Standard Login Services (Automated)

Profile Applicability:

- Level 1

Description:

The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices, and also prior to logins via telnet. The contents of the `/etc/motd` file is generally displayed after all successful logins, no matter where the user is logging in from, but is thought to be less useful because it only provides notification to the user after the machine has been accessed.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Audit:

Run the following commands and ensure that the files exist and have the correct permissions.

```
# /bin/ls -l /etc/motd
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/motd

# ls /etc/issue
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue

# ls /etc/issue.net
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue.net
```

The commands above simply validate the presence of the `/etc/motd`, `/etc/issue` and `/etc/issue.net` files. Review the contents of these files with the "cat" command and ensure that it is appropriate for your organization.

Remediation:

Run the following commands to update the files:

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/motd
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net
```

Run the following commands to update owner, group and remove excess permissions:

```
# chown root:root /etc/motd
# chmod u-x,go-wx /etc/motd
# chown root:root /etc/issue
# chmod u-x,go-wx /etc/issue
# chown root:root /etc/issue.net
# chmod u-x,go-wx /etc/issue.net
```

Default Value:

OS Default: No

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

8.1.2 Remove OS Information from Login Warning Banners (Automated)

Profile Applicability:

- Level 1

Description:

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information:

`\m` - machine architecture (`uname -m`) `\r` - operating system release (`uname -r`) `\s` - operating system name `\v` - operating system version (`uname -v`)

Rationale:

Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

Audit:

Perform the following commands to check if OS information is set to be displayed in the system login banners:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's//g'))" /etc/issue
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's//g'))" /etc/motd
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's//g'))" /etc/issue.net
```

Remediation:

Edit the `/etc/issue`, `/etc/motd`, and `/etc/issue.net` files with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v`, or references to the OS platform

Default Value:

OS Default: No

References:

1. N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

8.2 Set GNOME Warning Banner (Manual)

Profile Applicability:

- Level 1

Description:

The GNOME Display Manager is used for login session management. See the manual page `gdm(1)` for more information. The remediation action for this item sets a warning message for GDM users before they log in.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Audit:

```
# grep "<Text of Warning banner>" /usr/share/gdm/themes/RHEL/RHEL.xml
<Text of Warning banner>
```

Remediation:

Edit the file `/usr/share/gdm/themes/RHEL/RHEL.xml` and add the following statements after the two (2) pixmap blocks.

```
<item type="rect" id="custom-banner">
Insert the text of your warning banner here.
```

Default Value:

OS Default: No

References:

1. CCE-4188-9

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9 System Maintenance

No matter how securely a system has been installed and hardened, administrator and user activity over time can introduce security exposures. The section describes tasks to be performed on a regular, ongoing basis - perhaps in an automated fashion via the cron utility.

Note: unlike other sections, the items in this section specify an Audit action followed by a Remediation action since it is necessary to determine what the current setting is before determining remediation measures, which will vary depending on the site's policy.

9.1 Verify System File Permissions

9.1.1 Verify System File Permissions (Manual)

Profile Applicability:

- Level 2

Description:

The RPM package manager has a number of useful options. One of these, the `-v` (or `-verify`) option, can be used to verify that system packages are correctly installed. The `-v` option can be used to verify a particular package or to verify all system packages (`-va`). If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

Code Meaning

- S - File size differs.
- M - File mode differs (includes permissions and file type).
- 5 - The MD5 checksum differs.
- D - The major and minor version numbers differ on a device file.
- L - A mismatch occurs in a link.
- U - The file ownership differs.
- G - The file group owner differs.
- T - The file time (mtime) differs.

The `rpm -qf` command can be used to determine which package a particular file belongs to. For example the following command determines which package the `/etc/passwd` file belongs to:

```
# rpm -qf /etc/passwd  
  
setup-2.5.58-7.e15
```

To verify the settings for the package that controls the `/etc/passwd` file, run the following:

```
# rpm -V setup-2.5.58-7.e15  
  
.M..... c /etc/passwd  
S.5....T c /etc/printcap
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -v` command:

```
# rpm -V $(rpm -qf /etc/passwd)
.M..... c /etc/passwd
S.5....T c /etc/printcap
```

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Note: Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and is therefore not a scorable benchmark item, but is provided for those interested in additional security measures.

Audit:

Run the following command to review all installed packages.

Note: this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename> | grep -vw c
```

Remediation:

Correct any discrepancies found and rerun the command until output is clean or risk is mitigated or accepted.

Default Value:

OS Default: N/A

References:

1. N/A
2. http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.2 Verify Permissions on /etc/passwd (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to determine the permissions on the `/etc/passwd` file.

```
# /bin/ls -l /etc/passwd
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/passwd
```

Remediation:

Run the following command to remove excess permissions:

```
# /bin/chmod u-x,go-wx /etc/passwd
```

Default Value:

OS Default: Yes

References:

1. CCE-3566-7

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.3 Verify Permissions on /etc/shadow (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:

Run the following command to determine the permissions on the `/etc/shadow` file.

```
# /bin/ls -l /etc/shadow
-r----- 1 root root 633 Sep 23 2002 /etc/shadow
```

Remediation:

Run the following command to remove excess permissions:

```
# /bin/chmod u-wx,go-rwx /etc/shadow
```

Default Value:

OS Default: Yes

References:

1. CCE-4130-1

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.4 Verify Permissions on /etc/gshadow (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/gshadow` file contains information about group accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as expiration) could also be useful to subvert the group accounts.

Audit:

Run the following command to determine the permissions on the `/etc/gshadow` file.

```
# /bin/ls -l /etc/gshadow
-r----- 1 root root 633 Sep 23 2002 /etc/gshadow
```

Remediation:

Run the following command to remove excess permissions:

```
# /bin/chmod u-wx,go-rwx /etc/gshadow
```

Default Value:

OS Default: Yes

References:

1. CCE-3932-1

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.5 Verify Permissions on /etc/group (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to determine the permissions on the `/etc/group` file.

```
# /bin/ls -l /etc/group
-rw-r--r-- 1 root root 762 Sep 23 002 /etc/group
```

Remediation:

Run the following command to remove excess permissions:

```
# /bin/chmod u-x,go-wx /etc/group
```

Default Value:

OS Default: Yes

References:

1. CCE-3967-7

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.6 Verify User/Group Ownership on /etc/passwd (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains a list of all the valid userIDs defined in the system, but not the passwords. The command below sets the owner and group of the file to root.

Rationale:

The `/etc/passwd` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to determine the user and group ownership on the `/etc/passwd` file.

```
# /bin/ls -l /etc/passwd
-rw-r--r-- 1 root root 762 Sep 23 002 /etc/passwd
```

Remediation:

If the user and group ownership of the `/etc/passwd` file are incorrect, run the following command to correct them:

```
# /bin/chown root:root /etc/passwd
```

Default Value:

OS Default: Yes

References:

1. CCE-3958-6
2. CCE-3495-9

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.7 Verify User/Group Ownership on /etc/shadow (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/shadow` file contains the one-way cipher text passwords for each user defined in the `/etc/passwd` file. The command below sets the user and group ownership of the file to root.

Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:

Run the following command to determine the permissions on the `/etc/shadow` file.

```
# /bin/ls -l /etc/shadow
-r----- 1 root root 762 Sep 23 2002 /etc/shadow
```

Remediation:

If the permissions of the `/etc/shadow` file are incorrect, run the following command to correct them:

```
# /bin/chown root:root /etc/shadow
```

Default Value:

OS Default: Yes

References:

1. CCE-3918-0
2. CCE-3988-3

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.8 Verify User/Group Ownership on /etc/gshadow (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/gshadow` file contains information about group accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as expiration) could also be useful to subvert the group accounts.

Audit:

Run the following command to determine the permissions on the `/etc/gshadow` file.

```
# /bin/ls -l /etc/gshadow
-r----- 1 root root 633 Sep 23 2002 /etc/gshadow
```

Remediation:

If the permissions of the `/etc/gshadow` file are incorrect, run the following command to correct them:

```
# /bin/chown root:root /etc/gshadow
```

Default Value:

OS Default: Yes

References:

1. CCE-4210-1
2. CCE-4064-2

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.9 Verify User/Group Ownership on /etc/group (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to determine the permissions on the `/etc/group` file.

```
# /bin/ls -l /etc/group
-rw-r--r-- 1 root root 762 Sep 23 002 /etc/group
```

Remediation:

If the permissions of the `/etc/group` file are incorrect, run the following command to correct them:

```
# /bin/chown root:root /etc/group
```

Default Value:

OS Default: Yes

References:

1. CCE-3276-3
2. CCE-3883-6

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.10 Find World Writable Files (Automated)

Profile Applicability:

- Level 1

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

Run the following commands and verify no files are returned:

```
df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -0002
```

Remediation:

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

Default Value:

OS Default: N/A

References:

1. CCE-3795-2
2. CCE-14794-2

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.11 Find Un-owned Files and Directories (Automated)

Profile Applicability:

- Level 1

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Default Value:

OS Default: N/A

References:

1. CCE-4223-4

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.12 Find Un-grouped Files and Directories (Automated)

Profile Applicability:

- Level 1

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nogroup
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nogroup
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Default Value:

OS Default: N/A

References:

1. CCE-3573-3

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.13 Find SUID System Executables (Manual)

Profile Applicability:

- Level 1

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

Run the following command to list SUID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation:

Ensure that no rogue set-UID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the the integrity of these binaries as described below:

Example:

```
# rpm -V `rpm -qf /usr/bin/sudo`  
.....T /usr/bin/sudo  
SM5....T /usr/bin/sudoedit
```

Default Value:

OS Default: N/A

References:

1. CCE-14340-4

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.1.14 Find SGID System Executables (Manual)

Profile Applicability:

- Level 1

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced. The following is an example of checking the "sudo" executable:

```
# rpm -V `rpm -qf /usr/bin/sudo`  
.....T /usr/bin/sudo  
SM5....T /usr/bin/sudoedit
```

Audit:

Run the following command to list SUID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev  
-type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation:

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

Example:

```
# /bin/rpm -V `/bin/rpm -qf sudo`
```

Default Value:

OS Default: N/A

References:

1. CCE-14340-4

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.2 Review User and Group Settings

This section provides guidance on securing aspects of the users and groups.

9.2.1 Ensure Password Fields are Not Empty (Automated)

Profile Applicability:

- Level 1

Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

An account with an empty password field means that anybody may log in as that user without providing a password.

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow
```

Remediation:

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

Default Value:

OS Default: Yes

References:

1. CCE-4238-2

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

9.2.2 Verify No Legacy "+" Entries Exist in /etc/passwd File (Automated)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# /bin/grep '^+:' /etc/passwd
```

Remediation:

Remove any legacy '+' entries from /etc/passwd if they exist.

Default Value:

OS Default: Yes

References:

1. CCE-4114-5

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

9.2.3 Verify No Legacy "+" Entries Exist in /etc/shadow File (Automated)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# /bin/grep '^+:' /etc/shadow
```

Remediation:

Remove any legacy OS Default: Yes '+' entries from /etc/shadow if they exist.

Default Value:

OS Default: Yes

References:

1. CCE-14071-5

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.9 Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

9.2.4 Verify No Legacy "+" Entries Exist in /etc/group File (Automated)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# /bin/grep '^+:' /etc/group
```

Remediation:

Remove any legacy '+' entries from /etc/group if they exist.

References:

1. CCE-14675-3

Additional Information:

OS Default: Yes

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

16.9 Disable Dormant Accounts

Automatically disable dormant accounts after a set period of inactivity.

9.2.5 Verify No UID 0 Accounts Exist Other Than root (Automated)

Profile Applicability:

- Level 1

Description:

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 7.5 Restrict root Login to System Console.

Audit:

Run the following command and verify that only `root` is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd  
root
```

Remediation:

Delete any other entries that are displayed.

References:

1. CCE-4009-7

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.6 Ensure root PATH Integrity (Automated)

Profile Applicability:

- Level 1

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

Rationale:

Including the current working directory (`.`) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

if echo "$PATH" | grep -q ":@" ; then
    echo "Empty Directory in PATH (:@")"
fi
if echo "$PATH" | grep -q ":@" ; then
    echo "Trailing : in PATH"
fi
for x in $(echo "$PATH" | tr ":" " ") ; do
    if [ -d "$x" ] ; then
        ls -ldH "$x" | awk '
$9 == "." {print "PATH contains current working directory (.")}
$3 != "root" {print $9, "is not owned by root"}
substr($1,6,1) != "-" {print $9, "is group writable"}
substr($1,9,1) != "-" {print $9, "is world writable"}'
        else
            echo "$x is not a directory"
        fi
    done
```

Remediation:

Correct or justify any items discovered in the Audit step.

Default Value:

OS Default: Yes

References:

1. CCE-3301-9

CIS Controls:

Version 7

2.6 Address unapproved software

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

9.2.7 Check Permissions on User Home Directories (Automated)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != ""$(which nologin)"" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
    if [ ! -d "$dir" ]; then
        echo "The home directory ($dir) of user $user does not exist."
    else
        dirperm=$(ls -ld $dir | cut -f1 -d" ")
        if [ $(echo $dirperm | cut -c6) != "-" ]; then
            echo "Group Write permission set on the home directory ($dir) of user
$user"
        fi
        if [ $(echo $dirperm | cut -c8) != "-" ]; then
            echo "Other Read permission set on the home directory ($dir) of user
$user"
        fi
        if [ $(echo $dirperm | cut -c9) != "-" ]; then
            echo "Other Write permission set on the home directory ($dir) of user
$user"
        fi
        if [ $(echo $dirperm | cut -c10) != "-" ]; then
            echo "Other Execute permission set on the home directory ($dir) of user
$user"
        fi
    fi
done
```

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

References:

1. CCE-4090-7

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.2.8 Check User Dot File Permissions (Automated)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != ""$(which nologin)"" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
    if [ ! -d "$dir" ]; then
        echo "The home directory ($dir) of user $user does not exist."
    else
        for file in $dir/.[A-Za-z0-9]*; do
            if [ ! -h "$file" -a -f "$file" ]; then
                fileperm=$(ls -ld $file | cut -f1 -d" ")

                if [ $(echo $fileperm | cut -c6) != "-" ]; then
                    echo "Group Write permission set on file $file"
                fi
                if [ $(echo $fileperm | cut -c9) != "-" ]; then
                    echo "Other Write permission set on file $file"
                fi
            fi
        done
    fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

References:

1. N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.2.9 Check Permissions on User .netrc Files (Automated)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.

Rationale:

.netrc files may contain unencrypted passwords that may be used to attack other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
""${which nologin}"" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.netrc; do
      if [ ! -h "$file" -a -f "$file" ]; then
        fileperm=$(ls -ld $file | cut -f1 -d" ")
        if [ $(echo $fileperm | cut -c5) != "-" ]; then
          echo "Group Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c6) != "-" ]; then
          echo "Group Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c7) != "-" ]; then
          echo "Group Execute set on $file"
        fi
        if [ $(echo $fileperm | cut -c8) != "-" ]; then
          echo "Other Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c9) != "-" ]; then
          echo "Other Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c10) != "-" ]; then
          echo "Other Execute set on $file"
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` file permissions and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.2.10 Check for Presence of User .rhosts Files (Automated)

Profile Applicability:

- Level 1

Description:

While no `.rhosts` files are shipped with RHEL5, users can easily create them.

Rationale:

This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"$$(which nologin)" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.rhosts; do
      if [ ! -h "$file" -a -f "$file" ]; then
        echo ".rhosts file in $dir"
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.rhosts` files and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

References:

1. N/A

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

9.2.11 Check Groups in /etc/passwd (Automated)

Profile Applicability:

- Level 1

Description:

Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group.

Rationale:

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
  grep -q -P "^..*?:[^:]*:$i:" /etc/group
  if [ $? -ne 0 ]; then
    echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
  fi
done
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

Default Value:

OS Default: N/A

References:

1. N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.12 Check That Users Are Assigned Valid Home Directories (Automated)

Profile Applicability:

- Level 1

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in `/` and will not be able to write any files or have local environment variables set.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "" || $(which nologin) != "" && $7 != "/bin/false") { print $1 " " $6 }' | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "The home directory ($dir) of user $user does not exist."
    fi
done
```

Note: The audit script checks all users with interactive shells except `halt`, `sync`, `shutdown`, and `nfsnobody`.

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.13 Check User Home Directory Ownership (Automated)

Profile Applicability:

- Level 1

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != ""$(which nologin)"" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
    if [ ! -d "$dir" ]; then
        echo "The home directory ($dir) of user $user does not exist."
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            echo "The home directory ($dir) of user $user is owned by $owner."
        fi
    fi
done
```

Remediation:

Change the ownership any home directories that are not owned by the defined user to the correct user.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

9.2.14 Check for Duplicate UIDs (Automated)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    users=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs)
    echo "Duplicate UID ($2): $users"
  fi
done
```

Remediation:

Based on the results of the script, establish unique UIDs and review all files owned by the shared UID to determine which UID they are supposed to belong to.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.15 Check for Duplicate GIDs (Automated)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

Remediation:

Based on the results of the script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Default Value:

OS Default: N/A

References:

1. N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.16 Check That Reserved UIDs Are Assigned to System Accounts (Automated)

Profile Applicability:

- Level 1

Description:

Traditionally, UNIX systems establish "reserved" UIDs (0-499 range) that are intended for system accounts.

Rationale:

If a user is assigned a UID that is in the reserved range, even if it is not presently in use, security exposures can arise if a subsequently installed application uses the same UID.

Audit:

Run the following command:

```
# awk -F: '($1!="root" && $1!="bin" && $1!="daemon" && $1!="adm" && $1!="lp" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!="mail" && $1!="news" && $1!="uucp" && $1!="operator" && $1!="games" && $1!="gopher" && $1!="ftp" && $1!="nobody" && $1!="nscd" && $1!="vcsa" && $1!="rpc" && $1!="mailnull" && $1!="smmsp" && $1!="pcap" && $1!="ntp" && $1!="dbus" && $1!="avahi" && $1!="ssh" && $1!="rpcuser" && $1!="nfsnobody" && $1!="haldaemon" && $1!="avahi-autoipd" && $1!="distcache" && $1!="apache" && $1!="oprofile" && $1!="webalizer" && $1!="dovecot" && $1!="squid" && $1!="named" && $1!="xfs" && $1!="gdm" && $1!="sabayon" && $1!="exim" && $3<'$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)''') { print $1" "$3 }' /etc/passwd
```

Investigate any returned accounts.

Remediation:

If it's determined that these accounts should not be within the reserved UID range, change the UIDs that are in the reserved range to one that is in the user range. Review all files owned by the reserved UID to determine which UID they are supposed to belong to.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

9.2.17 Check for Duplicate User Names (Automated)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
cut -d: -f1 /etc/passwd | sort | uniq -d | while read -r x; do
    echo "Duplicate login name ${x} in /etc/passwd"
done
```

Remediation:

Based on the results of the script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

9.2.18 Check for Duplicate Group Names (Automated)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group`. Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate group name ${x} in /etc/group"
done
```

Remediation:

Based on the results of the script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

9.2.19 Check for Presence of User .netrc Files (Automated)

Profile Applicability:

- Level 1

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
""$(which nologin)"" && $7 != "/bin/false") { print $1 " " $6 }' | while
read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "The home directory ($dir) of user $user does not exist."
    else
        if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
            echo ".netrc file $dir/.netrc exists"
        fi
    fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials

Encrypt or hash with a salt all authentication credentials when stored.

9.2.20 Check for Presence of User .forward Files (Automated)

Profile Applicability:

- Level 1

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($7 != "/sbin/nologin" && $7 != "/bin/false" && $1 !~
/^(root|halt|sync|shutdown)$/) { print $1 " " $6 }' /etc/passwd | while read
-r user dir; do
    if [ ! -d "$dir" ] ; then
        echo "The home directory ($dir) of user $user does not exist."
    else
        if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ] ; then
            echo ".forward file $dir/.forward exists"
        fi
    fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

Default Value:

OS Default: N/A

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	Install Updates, Patches and Additional Security Software		
1.1	Filesystem Configuration		
1.1.1	Create Separate Partition for /tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Set nodev option for /tmp Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Set nosuid option for /tmp Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Set noexec option for /tmp Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Create Separate Partition for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	Bind Mount the /var/tmp directory to /tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	Create Separate Partition for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.8	Create Separate Partition for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.9	Create Separate Partition for /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.10	Add nodev Option to /home (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.11	Add nodev Option to Removable Media Partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.12	Add noexec Option to Removable Media Partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.13	Add nosuid Option to Removable Media Partitions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.14	Add nodev Option to /dev/shm Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.15	Add nosuid Option to /dev/shm Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.16	Add noexec Option to /dev/shm Partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.17	Set Sticky Bit on All World-Writable Directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.18	Disable Mounting of cramfs Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.19	Disable Mounting of freevxfs Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.20	Disable Mounting of jffs2 Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.21	Disable Mounting of hfs Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.22	Disable Mounting of hfsplus Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.23	Disable Mounting of squashfs Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.24	Disable Mounting of udf Filesystems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Configure Software Updates		
1.2.1	Configure Connection to the RHN RPM Repositories (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Verify Red Hat GPG Key is Installed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Verify that gpgcheck is Globally Activated (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Disable the rhnsd Daemon (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.5	Disable yum-updatesd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.6	Obtain Software Package Updates with yum (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.7	Verify Package Integrity Using RPM (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Advanced Intrusion Detection Environment (AIDE)		

1.3.1	Install AIDE (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Implement Periodic Execution of File Integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Configure SELinux		
1.4.1	Enable SELinux in /etc/grub.conf (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Set the SELinux State (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Set the SELinux Policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Remove SETroubleshoot (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.5	Disable MCS Translation Service (mcstrans) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.6	Check for Unconfined Daemons (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Secure Boot Settings		
1.5.1	Set User/Group Owner on /etc/grub.conf (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Set Permissions on /etc/grub.conf (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.3	Set Boot Loader Password (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.4	Require Authentication for Single-User Mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.5	Disable Interactive Boot (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Additional Process Hardening		
1.6.1	Restrict Core Dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.2	Configure ExecShield (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.3	Enable Randomized Virtual Memory Region Placement (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.4	Enable XD/NX Support on 32-bit x86 Systems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6.5	Disable Prelink (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Use the Latest OS Release (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	OS Services		
2.1	Remove Legacy Services		
2.1.1	Remove telnet-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Remove telnet Clients (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Remove rsh-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Remove rsh (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Remove NIS Client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Remove NIS Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Remove tftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Remove tftp-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Remove talk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Remove talk-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Remove xinetd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Disable chargen-dgram (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Disable chargen-stream (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Disable daytime-dgram (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Disable daytime-stream (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Disable echo-dgram (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Disable echo-stream (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Disable tcpmux-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3	Special Purpose Services		
3.1	Disable Avahi Server		
3.1.1	Disable Avahi Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Service Only via Required Protocol (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3	Check Responses TTL Field (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	Prevent Other Programs from Using Avahi's Port (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.5	Disable Publishing (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.6	Restrict Published Information (if publishing is required) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Set Daemon umask (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Remove X Windows (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Disable Print Server - CUPS (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Remove DHCP Server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Configure Network Time Protocol (NTP) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Remove LDAP (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Disable NFS and RPC (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Remove DNS Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Remove FTP Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.11	Remove HTTP Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.12	Remove Dovecot (IMAP and POP3 services) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.13	Remove Samba (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.14	Remove HTTP Proxy Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.15	Remove SNMP Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.16	Configure Mail Transfer Agent for Local-Only Mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4	Network Configuration and Firewalls		
4.1	Modify Network Parameters (Host Only)		
4.1.1	Disable IP Forwarding (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Disable Send Packet Redirects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Modify Network Parameters (Host and Router)		
4.2.1	Disable Source Routed Packet Acceptance (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Disable ICMP Redirect Acceptance (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Disable Secure ICMP Redirect Acceptance (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Log Suspicious Packets (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Enable Ignore Broadcast Requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	Enable Bad Error Message Protection (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	Enable RFC-recommended Source Route Validation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	Enable TCP SYN Cookies (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Wireless Networking		
4.3.1	Deactivate Wireless Interfaces (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Disable IPv6		
4.4.1	Configure IPv6		

4.4.1.1	Disable IPv6 Router Advertisements (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.2	Disable IPv6 Redirect Acceptance (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.2	Disable IPv6 (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Install TCP Wrappers		
4.5.1	Install TCP Wrappers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2	Create /etc/hosts.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3	Verify Permissions on /etc/hosts.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4	Create /etc/hosts.deny (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5	Verify Permissions on /etc/hosts.deny (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Uncommon Network Protocols		
4.6.1	Disable DCCP (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.2	Disable SCTP (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.3	Disable RDS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.4	Disable TIPC (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Enable IPtables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.8	Enable IP6tables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Logging and Auditing		
5.1	Configure Syslog		
5.1.1	Configure /etc/syslog.conf (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Create and Set Permissions on syslog Log Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Configure syslog to Send Logs to a Remote Log Host (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Accept Remote syslog Messages Only on Designated Log Hosts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Configure rsyslog		
5.2.1	Install the rsyslog package (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Activate the rsyslog Service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Configure /etc/rsyslog.conf (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Create and Set Permissions on rsyslog Log Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Configure rsyslog to Send Logs to a Remote Log Host (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Accept Remote rsyslog Messages Only on Designated Log Hosts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	Configure System Accounting (auditd)		
5.3.1	Configure Data Retention		
5.3.1.1	Configure Audit Log Storage Size (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.2	Disable System on Audit Log Full (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1.3	Keep All Auditing Information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	Enable auditd Service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	Keep All Auditing Information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	Enable Auditing for Processes That Start Prior to auditd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

5.3.5	Record Events That Modify Date and Time Information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	Record Events That Modify User/Group Information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	Record Events That Modify the System's Network Environment (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	Record Events That Modify the System's Mandatory Access Controls (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	Collect Login and Logout Events (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.10	Collect Session Initiation Information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.11	Collect Discretionary Access Control Permission Modification Events (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.12	Collect Unsuccessful Unauthorized Access Attempts to Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.13	Collect Use of Privileged Commands (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.14	Collect Successful File System Mounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.15	Collect File Deletion Events by User (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.16	Collect Changes to System Administration Scope (sudoers) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.17	Collect System Administrator Actions (sudolog) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.18	Collect Kernel Module Loading and Unloading (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.19	Make the Audit Configuration Immutable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Configure logrotate (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6	System Access, Authentication and Authorization		
6.1	Configure cron and anacron		
6.1.1	Enable anacron Daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Enable cron Daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Set User/Group Owner and Permission on /etc/anacrontab (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.4	Set User/Group Owner and Permission on /etc/crontab (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.5	Set User/Group Owner and Permission on /etc/cron.hourly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.6	Set User/Group Owner and Permission on /etc/cron.daily (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.7	Set User/Group Owner and Permission on /etc/cron.weekly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.8	Set User/Group Owner and Permission on /etc/cron.monthly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.9	Set User/Group Owner and Permission on /etc/cron.d (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.10	Restrict at/cron to Authorized Users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

6.2	Configure SSH		
6.2.1	Set SSH Protocol to 2 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Set LogLevel to INFO (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Set Permissions on /etc/ssh/sshd_config (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Disable SSH X11 Forwarding (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Set SSH MaxAuthTries to 4 or Less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Set SSH IgnoreRhosts to Yes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Set SSH HostbasedAuthentication to No (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Disable SSH Root Login (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.9	Set SSH PermitEmptyPasswords to No (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.10	Do Not Allow Users to Set Environment Options (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.11	Use Only Approved Ciphers in Counter Mode (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.12	Set Idle Timeout Interval for User Login (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.13	Limit Access via SSH (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.14	Set SSH Banner (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.15	Enable SSH UsePrivilegeSeparation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Configure PAM		
6.3.1	Set Password Creation Requirement Parameters Using pam_cracklib (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Set Lockout for Failed Password Attempts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Use pam_deny.so to Deny Services (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Upgrade Password Hashing Algorithm to SHA-512 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.5	Limit Password Reuse (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Remove the pam_ccreds Package (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Restrict root Login to System Console (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Restrict Access to the su Command (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7	User Accounts and Environment		
7.1	Set Shadow Password Suite Parameters (/etc/login.defs)		
7.1.1	Set Password Expiration Days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.2	Set Password Change Minimum Number of Days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	Set Password Expiring Warning Days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Disable System Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Set Default Group for root Account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Set Default umask for Users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Lock Inactive User Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8	Warning Banners		
8.1	Set Warning Banner for Standard Login Services		
8.1.1	Set Warning Banner for Standard Login Services (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

8.1.2	Remove OS Information from Login Warning Banners (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Set GNOME Warning Banner (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9	System Maintenance		
9.1	Verify System File Permissions		
9.1.1	Verify System File Permissions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.2	Verify Permissions on /etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.3	Verify Permissions on /etc/shadow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.4	Verify Permissions on /etc/gshadow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.5	Verify Permissions on /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.6	Verify User/Group Ownership on /etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.7	Verify User/Group Ownership on /etc/shadow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.8	Verify User/Group Ownership on /etc/gshadow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.9	Verify User/Group Ownership on /etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.10	Find World Writable Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.11	Find Un-owned Files and Directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.12	Find Un-grouped Files and Directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.13	Find SUID System Executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.1.14	Find SGID System Executables (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.2	Review User and Group Settings		
9.2.1	Ensure Password Fields are Not Empty (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.2	Verify No Legacy "+" Entries Exist in /etc/passwd File (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.3	Verify No Legacy "+" Entries Exist in /etc/shadow File (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.4	Verify No Legacy "+" Entries Exist in /etc/group File (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.5	Verify No UID 0 Accounts Exist Other Than root (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.6	Ensure root PATH Integrity (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.7	Check Permissions on User Home Directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.8	Check User Dot File Permissions (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.9	Check Permissions on User .netrc Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.10	Check for Presence of User .rhosts Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.11	Check Groups in /etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.12	Check That Users Are Assigned Valid Home Directories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.13	Check User Home Directory Ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.14	Check for Duplicate UIDs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.15	Check for Duplicate GIDs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.16	Check That Reserved UIDs Are Assigned to System Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

9.2.17	Check for Duplicate User Names (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.18	Check for Duplicate Group Names (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.19	Check for Presence of User .netrc Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2.20	Check for Presence of User .forward Files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Dec 3, 2020	2.2.1	#538 Improper Remediation in 1.4.4 Remove SETroubleshoot - CIS_Red_Hat_Enterprise_Linux_5_Benchmark_v2.2.0 (Ticket 1778)
Dec 3, 2020	2.2.1	Incorrect Audit and Remediation Procedure (Ticket 11213)
Dec 3, 2020	2.2.1	#550 5.3.3 Configure Audit Log Storage Size (Ticket 1779)
Dec 3, 2020	2.2.1	#551 5.3.4 Disable System on Audit Log Full (Ticket 1780)
Dec 3, 2020	2.2.1	Incorrect Audit and Remediation Procedure (Ticket 11214)
Dec 9, 2020	2.2.1	DELETE - Restrict at Daemon - redundant. covered by restrict at/cron (Ticket 11898)
Dec 21, 2020	2.2.1	UPDATE - add/update AAC throughout the benchmark (Ticket 11850)
Dec 21, 2020	2.2.1	UPDATE - Clean up formatting (Ticket 11849)
Dec 21, 2020	2.2.1	UPDATE - Map to CIS Controls v7 (Ticket 11848)
Dec 21, 2020	2.2.1	UPDATE - Review User and Group Settings (Ticket 11942)
Dec 21, 2020	2.2.1	#496 Section 1.5.3 updates between 2.1.0 and 2.2.0 still need to be fixed (Ticket 1777)
Dec 21, 2020	2.2.1	#557 5.3.5 duplicates 5.3.1.3 in RHEL 5 v2.2.0 (Ticket 1781)