CENTER FOR INTERNET SECURITY

CIS Ubuntu 12.04 LTS Server Benchmark

v1.0.0 - 04-02-2014

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

CIS SECURITY BENCHMARKS TERMS OF USE

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

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

UNDER THE FOLLOWING TERMS AND CONDITIONS:

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

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

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Ubuntu 12.04 LTS Server. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This 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 Ubuntu 12.04 LTS Server.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

- **Level 2**

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

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

Acknowledgements

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

Author
Rael Daruszka

Contributor
Timothy Legge RHEL, GSEC, GCWN, GWAPT, GPEN
John Oliver Linux+, Security+, Network+, ACMT, *SAIC*
Paul Sweatman
Matthew Wojcik , *Center for Internet Security*

Recommendations

1 Patching and Software Updates

1.1 Install Updates, Patches and Additional Security Software (Not Scored)

Profile Applicability:

- Level 1

Description:

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Rationale:

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches 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 the following commands to determine if there are packages to be updated:

```
# apt-get update
# apt-get --just-print upgrade
```

Remediation:

Run the following command to update all packages on the system:

```
# apt-get upgrade
```

2 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.

2.1 Create Separate Partition for /tmp (Scored)

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 "[[:space:]]/tmp[[:space:]]" /etc/fstab
```

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/tmp`.

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/

2.2 Set nodev option for /tmp Partition (Scored)

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
```

2.3 Set nosuid option for /tmp Partition (Scored)

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`.

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.

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

2.4 Set noexec option for /tmp Partition (Scored)

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
```

2.5 Create Separate Partition for /var (Scored)

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:

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

Remediation:

For new installations, during installation create a custom partition setup and specify 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/

2.6 Bind Mount the /var/tmp directory to /tmp (Scored)

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 manner `/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 none 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:

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

and edit the `/etc/fstab` file to contain the following line:

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

2.7 Create Separate Partition for /var/log (Scored)

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:

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

Remediation:

For new installations, during installation create a custom partition setup and specify 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/

2.8 Create Separate Partition for /var/log/audit (Scored)

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:

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

Remediation:

For new installations, during installation create a custom partition setup and specify 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/

2.9 Create Separate Partition for /home (Scored)

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:

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

Remediation:

For new installations, during installation create a custom partition setup and specify 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/

2.10 Add nodev Option to /home (Scored)

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 many distributions. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

Audit:

```
# 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
```

2.11 Add nodev Option to Removable Media Partitions (Not Scored)

Profile Applicability:

- Level 1

Description:

Set `nodev` on removable media to prevent character and block special devices that are present on the removable media from being treated as 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:

```
# 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.

2.12 Add noexec Option to Removable Media Partitions (Not Scored)

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 media. This deters users from being able to introduce potentially malicious software on the system.

Audit:

```
# grep <each removable media mountpoint> /etc/fstab
```

Note: 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.

2.13 Add nosuid Option to Removable Media Partitions (Not Scored)

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:

```
# 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.

2.14 Add nodev Option to /run/shm Partition (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# grep /run/shm /etc/fstab | grep nodev
# mount | grep /run/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 `/run/shm`. See the `fstab(5)` manual page for more information.

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

2.15 Add nosuid Option to /run/shm Partition (Scored)

Profile Applicability:

- Level 1

Description:

The `nosuid` mount option specifies that the `/run/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 /run/shm /etc/fstab | grep nosuid
# mount | grep /run/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 `/run/shm`. See the `fstab(5)` manual page for more information.

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

2.16 Add noexec Option to /run/shm Partition (Scored)

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 /run/shm /etc/fstab | grep noexec
# mount | grep /run/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 `/run/shm`. See the `fstab(5)` manual page for more information.

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

2.17 Set Sticky Bit on All World-Writable Directories (Scored)

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:

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

Remediation:

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

2.18 Disable Mounting of cramfs Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.19 Disable Mounting of freevxfs Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.20 Disable Mounting of jffs2 Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.21 Disable Mounting of hfs Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.22 Disable Mounting of hfsplus Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.23 Disable Mounting of squashfs Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.24 Disable Mounting of udf Filesystems (Not Scored)

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:

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

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

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

2.25 Disable Automounting (Scored)

Profile Applicability:

- Level 1

Description:

`autofs` allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have it's contents available in system even if they lacked permissions to mount it themselves.

Audit:

Ensure no start conditions listed for `autofs`:

```
# initctl show-config autofs
autofs
```

Remediation:

Remove or comment out start lines in `/etc/init/autofs.conf`:

```
#start on runlevel [2345]
```

3 Secure Boot Settings

3.1 Set User/Group Owner on bootloader config (Scored)

Profile Applicability:

- Level 1

Description:

Set the owner and group of your boot loaders config file to the root user. These instructions default to GRUB stored at `/boot/grub/grub.cfg`.

Rationale:

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

Audit:

Perform the following to determine if the `/boot/grub/grub.cfg` file has the correct ownership:

```
# stat -c "%u %g" /boot/grub/grub.cfg | egrep "^0 0"
```

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

Remediation:

Run the following to change ownership of `/boot/grub/grub.cfg`:

```
# chown root:root /boot/grub/grub.cfg
```

3.2 Set Permissions on bootloader config (Scored)

Profile Applicability:

- Level 1

Description:

Set permission on the your boot loaders config 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 `/boot/grub/grub.cfg` file permissions are correct:

```
# stat -L -c "%a" /boot/grub/grub.cfg | egrep ".00"
```

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

Remediation:

Run the following to set the permissions fro `/boot/grub/grub.cfg`:

```
# chmod og-rwx /boot/grub/grub.cfg
```

3.3 Set Boot Loader Password (Scored)

Profile Applicability:

- Level 1

Description:

Setting the boot loader password will require that anyone rebooting the 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 "^set superusers" /boot/grub/grub.cfg
set superusers="<user-list>"
```

```
# grep "^password" /boot/grub/grub.cfg
password_pbkdf2 <user> <encrypted password>
```

At least one user must be specified as a super user and have a password assigned.

Remediation:

Create an encrypted password with grub-md5-crypt:

```
# grub-mkpasswd-pbkdf2
Enter password: <password>
Reenter password: <password>
Your PBKDF2 is <encrypted-password>
```

Add the following into `/etc/grub.d/00_header` or a custom `/etc/grub.d` configuration file:

cat <<EOF
set superusers="*<user-list>*"
password_pbkdf2 *<user>* *<encrypted-password>*
EOF

Run the following to update the grub configuration:

```
# update-grub
```

3.4 Require Authentication for Single-User Mode (Scored)

Profile Applicability:

- Level 1

Description:

Setting a password for the `root` user will force authentication in single user mode.

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 if a password is set for the `root` user:

```
# grep ^root:[*\!]: /etc/shadow
```

No results should be returned.

Remediation:

Run the following command and follow the prompts to set a password for the `root` user:

```
# passwd root
```

4 Additional Process Hardening

4.1 Restrict Core Dumps (Scored)

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. The `apport` service if active will override the `fs.suid_dumpable` variable setting and automatically create core dump reports. The `whoopsie` service monitors `apport` core dump reports and transmits them to Canonical.

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
```

Ensure no start conditions are listed for the apport or whoopsie services:

```
# initctl show-config apport
apport
# initctl show-config whoopsie
whoopsie
```

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
```

Uninstall the `apport` and `whoopsie` packages or comment out any start lines in `/etc/init/apport.conf` and `/etc/init/whoopsie.conf` files:

```
#start on runlevel [2345]
```

4.2 Enable XD/NX Support on 32-bit x86 Systems (Not Scored)

Profile Applicability:

- Level 1

Description:

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

Rationale:

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

Audit:

Run the following to see if your kernel has identified and activated NX/XD protection.

```
# dmesg | grep NX
NX (Execute Disable) protection: active
```

Remediation:

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems:

If necessary configure your bootloader to load the new kernel and reboot the system.

You may need to enable NX or XD support in your bios.

4.3 Enable Randomized Virtual Memory Region Placement (Scored)

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 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
```

4.4 Disable Prelink (Scored)

Profile Applicability:

- Level 1

Description:

The prelinking feature changes binaries in an attempt to decrease their startup time.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.

Audit:

Run the following command:

```
# dpkg -s prelink
```

Ensure package status is not-installed or dpkg returns no info is available.

Remediation:

Run the command:

```
# /usr/sbin/prelink -ua
```

to restore binaries to a normal, non-prelinked state, then remove prelink:

```
# apt-get purge prelink
```

4.5 Activate AppArmor (Scored)

Profile Applicability:

- Level 2

Description:

AppArmor provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model.

Rationale:

For an action to occur, both the traditional DAC permissions must be satisfied as well as the AppArmor MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, AppArmor rules can only make a system's permissions more restrictive and secure.

Audit:

Check the status of AppArmor:

```
# apparmor_status
apparmor module is loaded.
18 profiles are loaded.
18 profiles are in enforce mode.
/sbin/dhclient
/usr/bin/evince
/usr/bin/evince-previewer
/usr/bin/evince-previewer//launchpad_integration
/usr/bin/evince-previewer//sanitized_helper
/usr/bin/evince-thumbnailer
/usr/bin/evince-thumbnailer//sanitized_helper
/usr/bin/evince//launchpad_integration
/usr/bin/evince//sanitized_helper
/usr/lib/NetworkManager/nm-dhcp-client.action
/usr/lib/connman/scripts/dhclient-script
/usr/lib/cups/backend/cups-pdf
/usr/lib/lightdm/lightdm/lightdm-guest-session-wrapper
/usr/lib/lightdm/lightdm/lightdm-guest-session-wrapper//chromium_browser
/usr/lib/telepathy/mission-control-5
/usr/lib/telepathy/telepathy-*
/usr/sbin/cupsd
```

```
/usr/sbin/tcpdump
0 profiles are in complain mode.
2 processes have profiles defined.
2 processes are in enforce mode.
/sbin/dhclient (779)
/usr/lib/telepathy/mission-control-5 (2022)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined
```

Ensure profiles are loaded, no profiles are in complain mode, and no processes are unconfined.

Remediation:

Install `apparmor` and `apparmor-utils` if missing (additional profiles can be found in the `apparmor-profiles` package):

```
# apt-get install apparmor apparmor-utils
```

Remove `apparmor=0` from all kernels in `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-3.0.80-0.7-ec2 root=/dev/sda1 xencons=xvc0 console=xvc0
splash=silent showopts
```

Set all profiles to enforce mode:

```
# aa-enforce /etc/apparmor.d/*
```

Any unconfined processes may need to have a profile created or activated for them and then be restarted.

5 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.

5.1 Ensure Legacy Services are Not Enabled

The items in this section are intended to ensure that legacy services are not active on the system. This guidance recommends disabling the software however removal is also an acceptable remediation.

Note: The audit items in the section check to see if the packages are listed in the package management database and installed. 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.

5.1.1 Ensure NIS is not installed (Scored)

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.

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:

Run the following command:

```
# dpkg -s nis
```

Ensure package status is not-installed or dpkg returns no info is available.

Remediation:

Uninstall the `nis` package:

```
# apt-get purge nis
```

5.1.2 Ensure rsh server is not enabled (Scored)

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:

Ensure the `rsh` services are not enabled:

```
# grep ^shell /etc/inetd.conf
# grep ^login /etc/inetd.conf
# grep ^exec /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `shell`, `login`, or `exec` lines in /etc/inetd.conf:

```
#shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
#exec           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
```

5.1.3 Ensure rsh client is not installed (Scored)

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:

Run the following commands:

```
# dpkg -s rsh-client
# dpkg -s rsh-redone-client
```

Ensure package status is not-installed or dpkg returns no info is available for both.

Remediation:

Uninstall the `rsh-client` and `rsh-reload-client` packages:

```
# apt-get purge rsh-client rsh-reload-client
```

5.1.4 Ensure talk server is not enabled (Scored)

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 initiate of talk sessions) is installed by default.

Rationale:

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

Audit:

Ensure the `talk` services are not enabled:

```
# grep ^talk /etc/inetd.conf
# grep ^ntalk /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `talk` or `ntalk` lines in `/etc/inetd.conf`:

```
#talk            dgram   udp     wait    nobody.tty      /usr/sbin/in.talkd      in.ta
lkd
#ntalk           dgram   udp     wait    nobody.tty      /usr/sbin/in.ntalkd     in.nt
alkd
```

5.1.5 Ensure talk client is not installed (Scored)

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:

Run the following command:

```
# dpkg -s talk
```

Ensure package status is not-installed or dpkg returns no info is available.

Remediation:

Uninstall the `talk` package:

```
# apt-get purge talk
```

5.1.6 Ensure telnet server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

The `telnet-server` package contains the `telnet` 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.

Audit:

Ensure the `telnet` services is not enabled:

```
# grep ^telnet /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `telnet` lines in `/etc/inetd.conf`:

```
#telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd
```

5.1.7 Ensure tftp-server is not enabled (Scored)

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 packages `tftp` and `atftp` are both used to define and support a TFTP server.

Rationale:

TFTP does not support authentication nor does it ensure the confidentiality or 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:

Ensure the `tftp` service is not enabled:

```
# grep ^tftp /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `tftp` lines in `/etc/inetd.conf`:

#tftp stream tcp nowait root internal

5.1.8 Ensure xinetd is not enabled (Scored)

Profile Applicability:

- Level 1

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.

Note: Several other services recommended to be disabled in this benchmark have xinetd versions as well, if xinetd is required in your environment ensure they are disabled in xinetd configuration as well.

Rationale:

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

Audit:

Ensure no start conditions listed for `xinetd`:

```
# initctl show-config xinetd
xinetd
```

Remediation:

Remove or comment out start lines in `/etc/init/xinetd.conf`:

```
#start on runlevel [2345]
```

5.2 Ensure chargen is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`chargen` 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:

Ensure the `chargen` services are not enabled:

```
# grep ^chargen /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `chargen` lines in /etc/inetd.conf:

#chargen stream tcp nowait root internal

5.3 Ensure daytime is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`daytime` 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:

Ensure the `daytime` services are not enabled:

```
# grep ^daytime /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `daytime` lines in /etc/inetd.conf:

#daytime stream tcp nowait root internal

5.4 Ensure echo is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`echo` 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:

Ensure the `echo` services are not enabled:

```
# grep ^echo /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `echo` lines in /etc/inetd.conf:

#echo stream tcp nowait root internal

5.5 Ensure discard is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`discard` is a network service that simply discards all data 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:

Ensure the `discard` services are not enabled:

```
# grep ^discard /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `discard` lines in /etc/inetd.conf:

#discard stream tcp nowait root internal

5.6 Ensure time is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`time` is a network service that responds with the server's current date and time as a 32 bit integer. 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:

Ensure the `time` services are not enabled:

```
# grep ^time /etc/inetd.conf
```

No results should be returned.

Remediation:

Remove or comment out any `time` lines in /etc/inetd.conf:

#time stream tcp nowait root internal

6 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.

Note: This section lists common packages for different services however there are alternate packages which provide many of these services which should also be disabled or deleted if not required.

6.1 Ensure the X Window system is not installed (Scored)

Profile Applicability:

- Level 1

Description:

The X Window system provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Window 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:

Run the following command:

```
# dpkg -l xserver-xorg-core*
```

Ensure no matching packages are listed as installed.

Remediation:

Uninstall X Windows:

```
# apt-get purge xserver-xorg-core*
```

6.2 Ensure Avahi Server is not enabled (Scored)

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 3.2.1 - 3.2.5 to secure it.

Audit:

Ensure no start conditions listed for `avahi-daemon`:

```
# initctl show-config avahi-daemon
avahi-daemon
```

Remediation:

Remove or comment out start lines in `/etc/init/avahi-daemon.conf`:

```
#start on (filesystem
#          and started dbus)
```

6.3 Ensure print server is not enabled (Not Scored)

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:

Ensure no start conditions listed for `cups`:

```
# initctl show-config cups
cups
```

Remediation:

Remove or comment out start lines in `/etc/init/cups.conf`:

```
#start on (filesystem
#           and (started dbus or runlevel [2345]))
```

References:

1. More detailed documentation on CUPS is available at the project homepage at http://www.cups.org.

6.4 Ensure DHCP Server is not enabled (Scored)

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:

Ensure no start conditions listed for `isc-dhcp-server` or `isc-dhcp-server6`:

```
# initctl show-config isc-dhcp-server
isc-dhcp-server
# initctl show-config isc-dhcp-server6
isc-dhcp-server6
```

Remediation:

Remove or comment out start lines in `/etc/init/isc-dhcp-server.conf` and `/etc/init/isc-dhcp-server6.conf`:

```
#start on runlevel [2345]
```

References:

1. More detailed documentation on DHCP is available at http://www.isc.org/software/dhcp.

6.5 Configure Network Time Protocol (NTP) (Scored)

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. More information on NTP 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:

Run the following to ensure `ntp` is installed:

```
# dpkg -s ntp
```

Ensure package status is `installed ok installed`.

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

```
# grep "restrict .* default" /etc/ntp.conf
restrict -4 default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer 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
# grep "RUNASUSER=ntp" /etc/init.d/ntp
RUNASUSER=ntp
```

Remediation:

Install `ntp`:

```
# apt-get install ntp
```

Ensure the following lines are in `/etc/ntp.conf`:

```
restrict -4 default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

Also, make sure `/etc/ntp.conf` has at least one NTP server specified:

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

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

References:

1. For more information on configuring NTP servers, go to the NTP homepage at http://www.ntp.org.

6.6 Ensure LDAP is not enabled (Not Scored)

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.

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:

Run the following command:

```
# dpkg -s slapd
```

Ensure package status is not-installed or dpkg returns no info is available.

Remediation:

Uninstall the `slapd` package:

```
# apt-get purge slapd
```

References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at http://www.openldap.org.

6.7 Ensure NFS and RPC are not enabled (Not Scored)

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:

Ensure no start conditions listed for `rpcbind-boot`:

```
# initctl show-config rpcbind-boot
rpcbind-boot
```

Run the following to ensure no start links for `nfs-kernel-server` exist in `/etc/rc*.d`:

```
# ls /etc/rc*.d/S*nfs-kernel-server
```

No results should be returned.

Remediation:

Remove or comment out start lines in /etc/init/rpcbind-boot.conf:

```
#start on virtual-filesystems and net-device-up IFACE=lo
```

Remove any start links for `nfs-kernel-server` from `/etc/rc*.d`:

```
# rm /etc/rc*.d/S*nfs-kernel-server
```

6.8 Ensure DNS Server is not enabled (Not Scored)

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:

Run the following to ensure no start links for `bind9` exist in `/etc/rc*.d`:

```
# ls /etc/rc*.d/S*bind9
```

No results should be returned.

Remediation:

Remove any start links for `bind9` from `/etc/rc*.d`:

```
# rm /etc/rc*.d/S*bind9
```

6.9 Ensure FTP Server is not enabled (Not Scored)

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:

Ensure no start conditions listed for `vsftpd`:

```
# initctl show-config vsftpd
vsftpd
```

Remediation:

Remove or comment out start lines in /etc/init/vsftpd.conf:

```
#start on runlevel [2345] or net-device-up IFACE!=lo
```

6.10 Ensure HTTP Server is not enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

HTTP or web servers provide the ability to host web site content.

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:

Run the following to ensure no start links for `apache2` exist in `/etc/rc*.d`:

```
# ls /etc/rc*.d/S*apache2
```

No results should be returned.

Remediation:

Remove any start links for `apache2` from `/etc/rc*.d`:

```
# rm /etc/rc*.d/S*apache2
```

6.11 Ensure IMAP and POP server is not enabled (Not Scored)

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:

Ensure no start conditions listed for `dovecot`:

```
# initctl show-config dovecot
dovecot
```

Remediation:

Remove or comment out start lines in `/etc/init/dovecot.conf`:

```
#start on runlevel [2345]
```

6.12 Ensure Samba is not enabled (Not Scored)

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:

Ensure no start conditions listed for `smbd`:

```
# initctl show-config smbd
smbd
```

Remediation:

Remove or comment out start lines in `/etc/init/smbd.conf`:

```
#start on (local-filesystems and net-device-up)
```

6.13 Ensure HTTP Proxy Server is not enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Squid is a standard proxy server used in many distributions and environments.

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:

Ensure no start conditions listed for `squid3`:

```
# initctl show-config squid3
squid3
```

Remediation:

Remove or comment out start lines in `/etc/init/squid3.conf`:

```
#start on runlevel [2345]
```

6.14 Ensure SNMP Server is not enabled (Not Scored)

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:

Run the following to ensure no start links for `snmpd` exist in `/etc/rc*.d`:

```
# ls /etc/rc*.d/S*snmpd
```

No results should be returned.

Remediation:

Remove any start links for `snmpd` from `/etc/rc*.d`:

```
# rm /etc/rc*.d/S*snmpd
```

6.15 Configure Mail Transfer Agent for Local-Only Mode (Scored)

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.

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: The remediation given here provides instructions for configuring the postfix mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

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[[:space:]]"
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
```

Remediation:

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below.

```
inet_interfaces = localhost
```

Restart postfix:

```
# service postfix restart
```

6.16 Ensure rsync service is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

The `rsyncd` service can be used to synchronize files between systems over network links.

Rationale:

The `rsyncd` service presents a security risk as it uses unencrypted protocols for communication.

Audit:

Ensure that the `rsync` service is not enabled:

```
# grep ^RSYNC_ENABLE /etc/default/rsync
RSYNC_ENABLE=false
```

Remediation:

Set `RSYNC_ENABLE` to `false` in `/etc/default/rsync`:

```
RSYNC_ENABLE=false
```

6.17 Ensure Biosdevname is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

`biosdevname` is an external tool that works with the udev framework for naming devices.

`biosdevname` uses three methods to determine NIC names：

1. PCI firmware spec.3.1
2. smbios (matches # after "em" to OEM # printed on board or housing)
3. PCI IRQ Routing Table (uses # of NIC position in the device history). If the BIOS does not support `biosdevname`, no NICs' are re-named.

Rationale:

`biosdevname` is an external tool that works with the `udev` framework for custom re-naming of system hardware connections made by the kernel and BIOS. As allowing the re-naming

of devices can severely disrupt network communications by creating resource conflicts and provide an attack vector for denial of service exploits, this capability should be disabled or restricted according to the needs of the organization.

Audit:

Run the following command:

```
# dpkg -s biosdevname
```

Ensure package status is not-installed or dpkg returns no info is available.

Remediation:

Uninstall the `biosdevname` package:

```
# apt-get purge biosdevname
```

7 Network Configuration and Firewalls

This section provides guidance for secure network and firewall configuration.

7.1 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.

7.1.1 Disable IP Forwarding (Scored)

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:

Perform the following to determine if `net.ipv4.ip_forward` is enabled on the system.

```
# /sbin/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
```

Modify active kernel parameters to match:

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

7.1.2 Disable Send Packet Redirects (Scored)

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:

Perform the following to determine if send packet redirects is disabled.

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

Modify active kernel parameters to match:

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

7.2 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.

7.2.1 Disable Source Routed Packet Acceptance (Scored)

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:

Perform the following to determine if accepting source routed packets is disabled.

```
# /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
```

Modify active kernel parameters to match:

```
# /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
```

7.2.2 Disable ICMP Redirect Acceptance (Scored)

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` to 0, 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:

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

```
# /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
```

Modify active kernel parameters to match:

```
# /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
```

7.2.3 Disable Secure ICMP Redirect Acceptance (Scored)

Profile Applicability:

- Level 1

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
```

Modify active kernel parameters to match:

```
# /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
```

7.2.4 Log Suspicious Packets (Scored)

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
# /sbin/sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.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
```

Modify active kernel parameters to match:

```
# /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
```

7.2.5 Enable Ignore Broadcast Requests (Scored)

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
```

Modify active kernel parameters to match:

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

7.2.6 Enable Bad Error Message Protection (Scored)

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
```

Modify active kernel parameters to match:

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

7.2.7 Enable RFC-recommended Source Route Validation (Scored)

Profile Applicability:

- Level 1

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
```

Modify active kernel parameters to match:

```
# /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
```

7.2.8 Enable TCP SYN Cookies (Scored)

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
```

Modify active kernel parameters to match:

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

7.3 Configure IPv6

IPv6 is a networking protocol that supersedes IPv4. It has more routable addresses and has built in security. If IPv6 is to be used, follow this section of the benchmark to configure IPv6, otherwise disable IPv6.

7.3.1 Disable IPv6 Router Advertisements (Not Scored)

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.ipv4. net.ipv6.conf.all.accept_ra = 0
# /sbin/sysctl net.ipv6.conf.default.accept_ra
net.ipv4. 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
```

Modify active kernel parameters to match:

```
# /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
```

7.3.2 Disable IPv6 Redirect Acceptance (Not Scored)

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.ipv4. net.ipv6.conf.all.accept_redirect = 0
# /sbin/sysctl net.ipv6.conf.default.accept_redirects
net.ipv4. 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
```

Modify active kernel parameters to match:

```
# /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
```

7.3.3 Disable IPv6 (Not Scored)

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 it be disabled to reduce the attack surface of the system.

Audit:

Run the following command to determine if IPv6 is enabled:

```
# ip addr | grep inet6
```

No results should be returned.

Remediation:

Create or edit the file `/etc/sysctl.conf` and add the following lines:

```
net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=1
```

Run the following command or reboot to apply the changes:

```
# sysctl -p
```

7.4 Install TCP Wrappers

7.4.1 Install TCP Wrappers (Scored)

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:

Run the following to ensure `tcpd` is installed:

```
# dpkg -s tcpd
```

Ensure package status is `installed ok installed`.

Remediation:

Install `tcpd`:

```
# apt-get install tcpd
```

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

```
# ldd <path-to-daemon> | grep libwrap.so
```

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

7.4.2 Create /etc/hosts.allow (Not Scored)

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:

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.

7.4.3 Verify Permissions on /etc/hosts.allow (Scored)

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:

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

```
# /bin/chmod 644 /etc/hosts.allow
```

7.4.4 Create /etc/hosts.deny (Not Scored)

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`:

```
# grep "ALL: ALL" /etc/hosts.deny
ALL: ALL
```

Remediation:

Create `/etc/hosts.deny`:

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

7.4.5 Verify Permissions on /etc/hosts.deny (Scored)

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 644 /etc/hosts.deny
```

7.5 Uncommon Network Protocols

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

7.5.1 Disable DCCP (Not Scored)

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 "install dccp /bin/true" /etc/modprobe.d/CIS.conf
install dccp /bin/true
```

Remediation:

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

7.5.2 Disable SCTP (Not Scored)

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 "install sctp /bin/true" /etc/modprobe.d/CIS.conf
install sctp /bin/true
```

Remediation:

```
# echo "install sctp /bin/true" >> /etc/modprobe.d/CIS.conf
```

7.5.3 Disable RDS (Not Scored)

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 "install rds /bin/true" /etc/modprobe.d/CIS.conf
install rds /bin/true
```

Remediation:

```
# echo "install rds /bin/true" >> /etc/modprobe.d/CIS.conf
```

7.5.4 Disable TIPC (Not Scored)

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 "install tipc /bin/true" /etc/modprobe.d/CIS.conf
install tipc /bin/true
```

Remediation:

```
# echo "install tipc /bin/true" >> /etc/modprobe.d/CIS.conf
```

7.6 Deactivate Wireless Interfaces (Not Scored)

Profile Applicability:

- Level 1

Description:

Wireless networking is used when wired networks are unavailable. Ubuntu provides the nmcli interface which allows 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 command to disable wireless:

```
# nmcli nm wifi off
```

7.7 Ensure Firewall is active (Scored)

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. `ufw` was developed to ease IPtables firewall configuration.

Rationale:

IPtables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv4 addresses and ports. Ubuntu provides UFW to ease firewall configuration.

Audit:

Ensure `ufw` is active:

```
# ufw status
Status: active
```

Remediation:

Activate `ufw`:

```
# ufw enable
```

Ensure that any needed ports, such as ssh access, are configured properly first.

8 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

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.

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`).

8.1 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.

8.1.1 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.

Note: Items in this section configure auditd, ensure it is installed per 8.1.2 Install and Enable auditd Service.

8.1.1.1 Configure Audit Log Storage Size (Not Scored)

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.

8.1.1.2 Disable System on Audit Log Full (Not Scored)

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 the following lines to the `/etc/audit/auditd.conf` file.

```
space_left_action = email
action_mail_acct = root
admin_space_left_action = halt
```

8.1.1.3 Keep All Auditing Information (Scored)

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
```

8.1.2 Install and Enable auditd Service (Scored)

Profile Applicability:

- Level 2

Description:

Install and 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:

Run the following to ensure `auditd` is installed:

```
# dpkg -s auditd
```
Ensure package status is `installed ok installed`.

Run the following to ensure proper start links for `auditd` exist in `/etc/rc*.d`:

```
# ls /etc/rc*.d/S*auditd
/etc/rc2.d/S37auditd  /etc/rc3.d/S37auditd  /etc/rc4.d/S37auditd  /etc/rc5.d/S37auditd
```
Start links should exist for run levels 2, 3, 4, and 5.

Remediation:

Install auditd:

```
# apt-get install auditd
```

If needed create proper start links for `auditd` in `/etc/rc*.d` by running the following command from each of the relevant directories:

```
# ln -s ../init.d/auditd S37auditd
```
Start links should be created for run levels 2, 3, 4, and 5.

8.1.3 Enable Auditing for Processes That Start Prior to auditd (Scored)

Profile Applicability:

- Level 2

Description:

Configure `grub` or `lilo` 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 `/boot/grub/grub.cfg` is configured to log processes that start prior to `auditd`.

```
# grep "linux" /boot/grub/grub.cfg
```
Make sure each line that starts with linux has the audit=1 parameter set.

Remediation:

Edit `/etc/default/grub` to include `audit=1` as part of `GRUB_CMDLINE_LINUX`:

```
GRUB_CMDLINE_LINUX="audit=1"
```

And run the following command to update the grub configuration:

```
# update-grub
```

8.1.4 Record Events That Modify Date and Time Information (Scored)

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 date 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
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

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
```

```
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

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
```

8.1.5 Record Events That Modify User/Group Information (Scored)

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
```

8.1.6 Record Events That Modify the System's Network Environment (Scored)

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/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/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 exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -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/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 exit,always -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/network -p wa -k system-locale
```

Remediation:

For 64 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -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/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 exit,always -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/network -p wa -k system-locale
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

8.1.7 Record Events That Modify the System's Mandatory Access Controls (Scored)

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 lines to the /etc/audit/audit.rules file.

```
Add the following lines to /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

8.1.8 Collect Login and Logout Events (Scored)

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 records of failures via the `pam_tally2` module

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
```

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
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

8.1.9 Collect Session Initiation Information (Scored)

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." 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 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
-w /var/log/btmp -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
-w /var/log/btmp -p wa -k session
# Execute the following command to restart auditd
# pkill -HUP -P 1 auditd
```

Note: Use the last command to read /var/log/wtmp (last with no parameters) and /var/run/utmp (last -f /var/run/utmp)

8.1.10 Collect Discretionary Access Control Permission Modification Events (Scored)

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 -HUP -P 1 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 -HUP -P 1 auditd
```

8.1.11 Collect Unsuccessful Unauthorized Access Attempts to Files (Scored)

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 -HUP -P 1 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 -HUP -P 1 auditd
```

8.1.12 Collect Use of Privileged Commands (Scored)

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:

Verify that an audit line for each setuid/setgid program identified in the `find` command appears in the audit file with the above attributes.

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 will be tagged with the identifier "privileged."

```
# find PART -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print \
"-a always,exit -F path=" $1 " -F perm=x -F auid>=500 -F auid!=4294967295 \
-k privileged" }'
```

Next, add those lines to the `/etc/audit/audit.rules` file.

8.1.13 Collect Successful File System Mounts (Scored)

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 -HUP -P 1 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 -HUP -P 1 auditd
```

8.1.14 Collect File Deletion Events by User (Scored)

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 auid>=500 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 \
-F auid!=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 auid>=500 \
-F auid!=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 auid>=500 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=500 \
-F auid!=4294967295 -k delete
# Execute the following command to restart auditd
# pkill -HUP -P 1 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 auid>=500 \
-F auid!=4294967295 -k delete
# Execute the following command to restart auditd
# pkill -P 1-HUP auditd
```

8.1.15 Collect Changes to System Administration Scope (sudoers) (Scored)

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 -HUP -P 1 auditd
```

8.1.16 Collect System Administrator Actions (sudolog) (Scored)

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 -HUP -P 1 auditd
```

Note: The system must be configured with `su` disabled (See Item 9.5 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.

8.1.17 Collect Kernel Module Loading and Unloading (Scored)

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
For 32 bit systems
-a always,exit arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems
-a always,exit arch=b64 -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
For 32 bit systems, add
-a always,exit arch=b32 -S init_module -S delete_module -k modules
For 64 bit systems, add
-a always,exit arch=b64 -S init_module -S delete_module -k modules
```

8.1.18 Make the Audit Configuration Immutable (Scored)

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 potentially 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

8.2 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.

8.2.1 Install the rsyslog package (Scored)

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.

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:

Ensure `rsyslog` is installed:

```
# dpkg -s rsyslog
```

Ensure package status is `installed ok installed`.

Remediation:

Install the `rsyslog` package:

```
# apt-get install rsyslog
```

8.2.2 Ensure the rsyslog Service is activated (Scored)

Profile Applicability:

- Level 1

Description:

Once the rsyslog package is installed it needs to be activated.

Rationale:

If the rsyslog service is not activated the system will not have a syslog service running.

Audit:

Ensure that the `rsyslog` service is active:

```
# initctl show-config rsyslog
rsyslog
start on filesystem
stop on runlevel [06]
```

Remediation:

Set the proper start conditions in `/etc/init/rsyslog.conf`:

```
start on filesystem
```

8.2.3 Configure /etc/rsyslog.conf (Not Scored)

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` and `/etc/rsyslog.d/*` files 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` or `/etc/rsyslog.d/*` file as appropriate for your
environment:

```
*.emerg :omusrmsg:*
mail.* -/var/log/mail
mail.info -/var/log/mail.info
mail.warning -/var/log/mail.warn
mail.err /var/log/mail.err
news.crit -/var/log/news/news.crit
```

```
news.err -/var/log/news/news.err
news.notice -/var/log/news/news.notice
*.=warning;*.=err -/var/log/warn
*.crit /var/log/warn
*.*;mail.none;news.none -/var/log/messages
local0,local1.* -/var/log/localmessages
local2,local3.* -/var/log/localmessages
local4,local5.* -/var/log/localmessages
local6,local7.* -/var/log/localmessages
```

Execute the following command to restart rsyslogd

```
# pkill -HUP rsyslogd
```

References:

1. See the rsyslog.conf(5) man page for more information.

8.2.4 Create and Set Permissions on rsyslog Log Files (Scored)

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 *<logfile>* 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 *<logfile>* listed in the `/etc/rsyslog.conf` or `/etc/rsyslog.d/*` files, 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 *<logfile>* 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>
```

References:

1. See the rsyslog.conf(5) man page for more information.

8.2.5 Configure rsyslog to Send Logs to a Remote Log Host (Scored)

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.

References:

1. See the rsyslog.conf(5) man page for more information.

8.2.6 Accept Remote rsyslog Messages Only on Designated Log Hosts (Not Scored)

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:

```
# grep '$ModLoad imtcp.so' /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 un-comment the following lines:

```
$ModLoad imtcp.so
$InputTCPServerRun 514
```

Execute the following command to restart `rsyslogd`:

```
# pkill -HUP rsyslogd
```

References:

1. See the rsyslog(8) man page for more information.

8.3 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.

8.3.1 Install AIDE (Scored)

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 to ensure `aide` is installed:

```
# dpkg -s aide
```

Ensure package status is `installed ok installed`.

Remediation:

Install AIDE:

```
# apt-get install aide
```

Initialize AIDE:

```
# aideinit
# cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

Note: The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run `/usr/sbin/prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

8.3.2 Implement Periodic Execution of File Integrity (Scored)

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 `cron` 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.

8.4 Configure logrotate (Not Scored)

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/rsyslog` is the configuration file used to rotate log files created by `rsyslog`.

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:

Review the `/etc/logrotate.d/rsyslog` file to determine if the appropriate system logs are rotated according to your site policy.

Remediation:

Edit the `/etc/logrotate.d/rsyslog` file to include appropriate system logs according to your site policy.

9 System Access, Authentication and Authorization

9.1 Configure cron

9.1.1 Enable cron Daemon (Scored)

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:

Ensure proper start conditions listed for `cron`:

```
# /sbin/initctl show-config cron
cron
  start on runlevel [2345]
  stop on runlevel [!2345]
```

Remediation:

Edit start lines in `/etc/init/cron.conf` to match the following:

```
start on runlevel [2345]
```

9.1.2 Set User/Group Owner and Permission on /etc/crontab (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access 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 -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:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

9.1.3 Set User/Group Owner and Permission on /etc/cron.hourly (Scored)

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` file has the correct permissions.

```
# stat -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:

```
# chown root:root /etc/cron.hourly
# chmod og-rwx /etc/cron.hourly
```

9.1.4 Set User/Group Owner and Permission on /etc/cron.daily (Scored)

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 -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:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

9.1.5 Set User/Group Owner and Permission on /etc/cron.weekly (Scored)

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 -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:

```
# chown root:root /etc/cron.weekly
# chmod og-rwx /etc/cron.weekly
```

9.1.6 Set User/Group Owner and Permission on /etc/cron.monthly (Scored)

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 -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:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

9.1.7 Set User/Group Owner and Permission on /etc/cron.d (Scored)

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 -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:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

9.1.8 Restrict at/cron to Authorized Users (Scored)

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 /etc/cron.allow
# ls -l /etc/at.allow
-rw------- 1 root root /etc/at.allow
```

Remediation:

```
# /bin/rm /etc/cron.deny
# /bin/rm /etc/at.deny
# touch /etc/cron.allow
# touch /etc/at.allow
# chmod og-rwx /etc/cron.allow
# chmod og-rwx /etc/at.allow
# chown root:root /etc/cron.allow
# chown root:root /etc/at.allow
```

9.2 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.

9.2.1 Set Password Creation Requirement Parameters Using pam_cracklib (Scored)

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.

- `retry=3` - Allow 3 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 `/etc/pam.d/common-password` file.

```
# grep pam_cracklib.so /etc/pam.d/common-password
password required pam_cracklib.so 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/common-password`:

```
password required pam_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1
lcredit=-1
```

9.2.2 Set Lockout for Failed Password Attempts (Not Scored)

Profile Applicability:

- Level 1

Description:

Lock out users after *n* unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration file `/etc/pam.d/login`. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM.

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 user lockout.

```
# grep "pam_tally2" /etc/pam.d/login
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
```

Remediation:

Edit the `/etc/pam.d/login` file and add the auth line below:

```
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
```

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 `/sbin/pam_tally2 -u` *<username>* `--reset`. This command sets the failed count to 0, effectively unlocking the user.

9.2.3 Limit Password Reuse (Scored)

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.

Note that these change only apply to accounts configured on the local system.

Audit:

Perform the following to determine the current setting for reuse of older passwords:

```
# grep "remember" /etc/pam.d/common-password
password [success=1 default=ignore] pam_unix.so obscure sha512 remember=5
```

Remediation:

Set the `pam_unix.so remember` parameter to `5` in `/etc/pam.d/common-password`:

```
password sufficient pam_unix.so remember=5
```

Note: The default password setting in this document is the last 5 passwords. Change this number to conform to your site's password policy.

9.3 Configure SSH

Description: 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.

If the ssh server is not installed the contents of this section are not required. You can check the install status of the ssh server with the following command:

```
# dpkg -s openssh-server
```

9.3.1 Set SSH Protocol to 2 (Scored)

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
```

9.3.2 Set LogLevel to INFO (Scored)

Profile Applicability:

- Level 1

Description:

The `INFO` parameter specifices that record login and logout activity will be logged.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `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. `INFO` level is the basic level that only records login activity of SSH users. 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
```

9.3.3 Set Permissions on /etc/ssh/sshd_config (Scored)

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-priliveged 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------- 1 root root 762 Sep 23 002 /etc/ssh/sshd_config
```

Remediation:

If the user and group ownership of the `/etc/ssh/sshd_config` file are incorrect, run the following command to correct them:

```
# chown root:root /etc/ssh/sshd_config
```

If the permissions are incorrect, run the following command to correct them:

```
# chmod 600 /etc/ssh/sshd_config
```

9.3.4 Disable SSH X11 Forwarding (Scored)

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
```

9.3.5 Set SSH MaxAuthTries to 4 or Less (Scored)

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
```

9.3.6 Set SSH IgnoreRhosts to Yes (Scored)

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
```

9.3.7 Set SSH HostbasedAuthentication to No (Scored)

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
```

9.3.8 Disable SSH Root Login (Scored)

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
```

9.3.9 Set SSH PermitEmptyPasswords to No (Scored)

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
```

9.3.10 Do Not Allow Users to Set Environment Options (Scored)

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
```

9.3.11 Use Only Approved Cipher in Counter Mode (Scored)

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 (CBD) 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
```

References:

1. For more information on the Counter mode algorithms, read RFC4344 at http://www.ietf.org/rfc/rfc4344.txt.

9.3.12 Set Idle Timeout Interval for User Login (Scored)

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 command 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 parameter as follows:

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

9.3.13 Limit Access via SSH (Scored)

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:

`AllowUsers`

The `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.

`AllowGroups`

The `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.

`DenyUsers`

The `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.

`DenyGroups`

The `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 command and verify that the 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 one or more of the parameter as follows:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

9.3.14 Set SSH Banner (Scored)

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
```

9.4 Restrict root Login to System Console (Not Scored)

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:

```
# cat /etc/securetty
```

Remediation:

Remove entries for any consoles that are not in a physically secure location.

9.5 Restrict Access to the su Command (Scored)

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:

```
# 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:

add the following line to the `/etc/pam.d/su` file.

```
auth required pam_wheel.so use_uid
```

Once this is done, create a comma separated list of users in the wheel statement in the `/etc/group` file.

10 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 10 System Maintenance.

10.1 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.

10.1.1 Set Password Expiration Days (Scored)

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:

```
# 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>
```

10.1.2 Set Password Change Minimum Number of Days (Scored)

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:

```
# 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>
```

10.1.3 Set Password Expiring Warning Days (Scored)

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:

```
# 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>
```

10.2 Disable System Accounts (Scored)

Profile Applicability:

- Level 1

Description:

There are a number of accounts provided with Ubuntu 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 Ubuntu set 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 `/usr/sbin/nologin`. This prevents the account from potentially being used to run any commands.

Audit:

Run the following script to determine if any system accounts can be accessed:

```
egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" &&
$1!="halt" && $3<500 && $7!="/usr/sbin/nologin" && $7!="/bin/false") {print}'
```

There should be no results returned.

Remediation:

Accounts that have been locked are prohibited from running commands on the system. Such accounts are not able to login to the system nor are they able to use scheduled execution facilities such as cron. To make sure system accounts cannot be accessed, using the following script:

```
#!/bin/bash
for user in `awk -F: '($3 < 500) {print $1 }' /etc/passwd`; do
   if [ $user != "root" ]
   then
      /usr/sbin/usermod -L $user
      if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ]
      then
         /usr/sbin/usermod -s /usr/sbin/nologin $user
      fi
   fi
done
```

10.3 Set Default Group for root Account (Scored)

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:

```
# grep "^root:" /etc/passwd | cut -f4 -d:
0
```

Remediation:

```
# usermod -g 0 root
```

10.4 Set Default umask for Users (Scored)

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`, `.bashrc`, 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:

```
# grep "^UMASK" /etc/login.defs
UMASK 077
```

Remediation:

Edit the **/etc/login.defs** file (and the appropriate files for any other shell supported on your system as necessary) and set the UMASK parameter as shown:

```
UMASK 077
```

10.5 Lock Inactive User Accounts (Scored)

Profile Applicability:

- Level 1

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 35 or more days be disabled.

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:

```
# useradd -D | grep INACTIVE
INACTIVE=35
```

Remediation:

```
# useradd -D -f 35
```

11 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.

11.1 Set Warning Banner for Standard Login Services (Scored)

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:

```
# touch /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
# chown root:root /etc/motd
# chmod 644 /etc/motd
# chown root:root /etc/issue
# chmod 644 /etc/issue
# chown root:root /etc/issue.net
# chmod 644 /etc/issue.net
```

11.2 Remove OS Information from Login Warning Banners (Scored)

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:

```
# egrep '(\\v|\\r|\\m|\\s)' /etc/issue
# egrep '(\\v|\\r|\\m|\\s)' /etc/motd
# egrep '(\\v|\\r|\\m|\\s)' /etc/issue.net
```

Remediation:

Edit the `/etc/motd`, `/etc/issue` and `/etc/issue.net` files and remove any lines containing `\m`, `\r`, `\s` or `\v`.

11.3 Set Graphical Warning Banner (Not Scored)

Profile Applicability:

- Level 1

Description:

Ubuntu defaults to using lightdm for graphical login session management which provides no built in banner setting. The GNOME Display Manager and KDM are both available but must be manually installed.

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:

If the X Window system is in use ensure that a warning banner consistent with your organizations policy is in place.

Remediation:

Set a banner for the display manager in use consistent with your organizations policy. This process depends on the specific Display Manager and theme in use, consult your documentation for more details.

12 Verify System File Permissions

12.1 Verify Permissions on /etc/passwd (Scored)

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:

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

```
# /bin/chmod 644 /etc/passwd
```

12.2 Verify Permissions on /etc/shadow (Scored)

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. Ensure world has no access, group has no write or execute access.

```
# /bin/ls -l /etc/shadow
-rw-r----- 1 root shadow 712 Jul 22 21:33 shadow
```

Remediation:

If the permissions of the `/etc/shadow` file are incorrect, run the following commands to correct them:

```
# /bin/chmod o-rwx,g-rw /etc/shadow
```

12.3 Verify Permissions on /etc/group (Scored)

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/chmod 644 /etc/group
```

12.4 Verify User/Group Ownership on /etc/passwd (Scored)

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-priliveged 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
```

12.5 Verify User/Group Ownership on /etc/shadow (Scored)

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 ownership of the `/etc/shadow` file. Ensure it is owned by user root, and group root or shadow.

```
# /bin/ls -l /etc/shadow
-rw-r----- 1 root shadow 712 Jul 22 21:33 shadow
```

Remediation:

If the ownership of the `/etc/shadow` file are incorrect, run the following command to correct them:

```
# /bin/chown root:shadow /etc/shadow
```

12.6 Verify User/Group Ownership on /etc/group (Scored)

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-priliveged 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 ownership of the `/etc/group` file are incorrect, run the following command to correct them:

```
# /bin/chown root:root /etc/group
```

12.7 Find World Writable Files (Not Scored)

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:

```
#!/bin/bash
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -
perm -0002 -print
```

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.

12.8 Find Un-owned Files and Directories (Scored)

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:

```
#!/bin/bash
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser -
ls
```

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.

12.9 Find Un-grouped Files and Directories (Scored)

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:

```
#!/bin/bash
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -group -ls
```

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.

12.10 Find SUID System Executables (Not Scored)

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:

```
#!/bin/bash
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -
perm -4000 -print
```

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 integrity of these binaries.

12.11 Find SGID System Executables (Not Scored)

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.

Audit:

```
#!/bin/bash
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -
perm -2000 -print
```

Remediation:

Ensure that no rogue set-GID 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.

13 Review User and Group Settings

This section provides guidance on securing aspects of the users and groups.

13.1 Ensure Password Fields are Not Empty (Scored)

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:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Audit:

Run the following command and verify that no output is returned:

```
# /bin/cat /etc/shadow | /usr/bin/awk -F: '($2 == "" ) { print $1 " does not have a
password "}'
```

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:

```
# /usr/bin/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.

13.2 Verify No Legacy "+" Entries Exist in /etc/passwd File (Scored)

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 most 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:

Delete these entries if they exist.

13.3 Verify No Legacy "+" Entries Exist in /etc/shadow File (Scored)

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 most 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:

Delete these entries if they exist.

13.4 Verify No Legacy "+" Entries Exist in /etc/group File (Scored)

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 most 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:

Delete these entries if they exist.

13.5 Verify No UID 0 Accounts Exist Other Than root (Scored)

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 9.4 Restrict root Login to System Console.

Audit:

Run the following command and verify that only the word "root" is returned:

```
# /bin/cat /etc/passwd | /usr/bin/awk -F: '($3 == 0) { print $1 }'
root
```

Remediation:

Delete any other entries that are displayed.

13.6 Ensure root PATH Integrity (Scored)

Profile Applicability:

- Level 1

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unemotionally 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:

```
#!/bin/bash
if [ "`echo $PATH | grep :: `" != "" ]; then
echo "Empty Directory in PATH (::)"
fi
if [ "`echo $PATH | bin/grep :$`" != "" ]; then
echo "Trailing : in PATH"
fi
p=`echo $PATH | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
if [ "$1" = "." ]; then
echo "PATH contains ."
shift
continue
fi
if [ -d $1 ]; then
```

```
dirperm=`ls -ldH $1 | cut -f1 -d" "`
if [ `echo $dirperm | cut -c6 ` != "-" ]; then
echo "Group Write permission set on directory $1"
fi
if [ `echo $dirperm | cut -c9 ` != "-" ]; then
echo "Other Write permission set on directory $1"
fi
dirown=`ls -ldH $1 | awk '{print $3}'`
if [ "$dirown" != "root" ] ; then
echo $1 is not owned by root
fi
else
echo $1 is not a directory
fi
shift
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

13.7 Check Permissions on User Home Directories (Scored)

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:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd  | /bin/egrep -v '(root|halt|sync|shutdown)' |\
    /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
        dirperm=`/bin/ls -ld $dir | /usr/bin/cut -f1 -d" "`
        if [ `echo $dirperm | /usr/bin/cut -c6 ` != "-" ]; then
            echo "Group Write permission set on directory $dir"
        fi
        if [ `echo $dirperm | /usr/bin/cut -c8 ` != "-" ]; then
            echo "Other Read permission set on directory $dir"
        fi
        if [ `echo $dirperm | /usr/bin/cut -c9 ` != "-" ]; then
            echo "Other Write permission set on directory $dir"
        fi
        if [ `echo $dirperm | /usr/bin/cut -c10 ` != "-" ]; then
            echo "Other Execute permission set on directory $dir"
```

```
        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.

13.8 Check User Dot File Permissions (Scored)

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:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|sync|halt|shutdown)' |
/usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
    for file in $dir/.[A-Za-z0-9]*; do
        if [ ! -h "$file" -a -f "$file" ]; then
            fileperm=`/bin/ls -ld $file | /usr/bin/cut -f1 -d" "`
            if [ `echo $fileperm | /usr/bin/cut -c6 ` != "-" ]; then
                echo "Group Write permission set on file $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c9 ` != "-" ]; then
                echo "Other Write permission set on file $file"
            fi
        fi
    done
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.

13.9 Check Permissions on User .netrc Files (Scored)

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:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|sync|halt|shutdown)' |\
    /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
    for file in $dir/.netrc; do
        if [ ! -h "$file" -a -f "$file" ]; then
            fileperm=`/bin/ls -ld $file | /usr/bin/cut -f1 -d" "`
            if [ `echo $fileperm | /usr/bin/cut -c5 ` != "-" ]
            then
                echo "Group Read set on $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c6 ` != "-" ]
            then
                echo "Group Write set on $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c7 ` != "-" ]
            then
                echo "Group Execute set on $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c8 ` != "-" ]
            then
                echo "Other Read  set on $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c9 ` != "-" ]
            then
                echo "Other Write set on $file"
            fi
            if [ `echo $fileperm | /usr/bin/cut -c10 ` != "-" ]
            then
                echo "Other Execute set on $file"
            fi
        fi
    done
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.

13.10 Check for Presence of User .rhosts Files (Scored)

Profile Applicability:

- Level 1

Description:

While no `.rhosts` files are shipped by default, 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:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)' |\
    /usr/bin/awk -F: '($7 != "/sbin/nologin") { print $6 }'`; do
    for file in $dir/.rhosts; do
        if [ ! -h "$file" -a -f "$file" ]; then
            echo ".rhosts file in $dir"
        fi    done
done
```

Remediation:

If any users have `.rhosts` files determine why they have them.

13.11 Check Groups in /etc/passwd (Scored)

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:

Create a script as shown below and run it:

```
#!/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.

13.12 Check That Users Are Assigned Valid Home Directories (Scored)

Profile Applicability:

- Level 1

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that 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:

This script checks to make sure that home directories assigned in the `/etc/passwd` file exist.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a ! -d "$dir" -a $user != "nfsnobody" ]; then
echo "The home directory ($dir) of user $user does not exist."
fi
done
```

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.

13.13 Check User Home Directory Ownership (Scored)

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:

This script checks to make sure users own the home directory they are assigned to in the `/etc/passwd` file.

```
#!/bin/bash
cat /etc/passwd | awk -F: '{ print $1 " " $3 " " $6 }' | while read user uid dir; do
if [ $uid -ge 500 -a -d "$dir" -a $user != "nfsnobody" ]; then
owner=$(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 of any home directories that are not owned by the defined user to the correct user.

13.14 Check for Duplicate UIDs (Scored)

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:

This script checks to make sure all UIDs in the `/etc/passwd` file are unique.

```
#!/bin/bash
/bin/cat /etc/passwd | /usr/bin/cut -f3 -d":" | /usr/bin/sort -n | /usr/bin/uniq -c |\
    while read x ; do
    [ -z "${x}" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
        users=`/usr/bin/awk -F: '($3 == n) { print $1 }' n=$2 \
            /etc/passwd | /usr/bin/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.

13.15 Check for Duplicate GIDs (Scored)

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:

This script checks to make sure all UIDs in the `/etc/group` file are unique. You can also use the `/usr/sbin/grpck` command to check for other inconsistencies in the `/etc/group` file.

```
#!/bin/bash
/bin/cat /etc/group | /usr/bin/cut -f3 -d":" | /usr/bin/sort -n | /usr/bin/uniq -c |\
    while read x ; do
    [ -z "${x}" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
        grps=`/usr/bin/awk -F: '($3 == n) { print $1 }' n=$2 \
            /etc/group | xargs`
        echo "Duplicate GID ($2): ${grps}"
    fi
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.

13.16 Check for Duplicate User Names (Scored)

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:

This script checks to make sure all user names in the `/etc/passwd` file are unique.

```
#!/bin/bash
cat /etc/passwd | /usr/bin/cut -f1 -d":" | /usr/bin/sort -n | /usr/bin/uniq -c |\
    while read x ; do
    [ -z "${x}" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
        uids=`/usr/bin/awk -F: '($1 == n) { print $3 }' n=$2 \
            /etc/passwd | xargs`
        echo "Duplicate User Name ($2): ${uids}"
```

```
    fi
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.

13.17 Check for Duplicate Group Names (Scored)

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:

This script checks to make sure all group names in the `/etc/group` file are unique.

```
#!/bin/bash
cat /etc/group | /usr/bin/cut -f1 -d":" | /usr/bin/sort -n | /usr/bin/uniq -c |\
    while read x ; do
    [ -z "${x}" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
        gids=`/usr/bin/awk -F: '($1 == n) { print $3 }' n=$2 \
            /etc/group | xargs`
        echo "Duplicate Group Name ($2): ${gids}"
    fi
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.

13.18 Check for Presence of User .netrc Files (Scored)

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:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
    /usr/bin/awk -F: '{ print $6 }'`; do
    if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
        echo ".netrc file $dir/.netrc exists"
    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.

13.19 Check for Presence of User .forward Files (Scored)

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:

This script checks for the presence of `.forward` files that may be in violation of the site security policy.

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd |\
    /usr/bin/awk -F: '{ print $6 }'`; do
    if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
        echo ".forward file $dir/.forward exists"
    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.

13.20 Ensure shadow group is empty (Scored)

Profile Applicability:

- Level 1

Description:

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert additional user accounts.

Audit:

Ensure there are no user in the shadow group:

```
grep ^shadow /etc/group
```

Ensure no users have shadow as their primary group:

```
awk -F: '($4 == "<shadow-gid>") { print }' /etc/passwd
```

Remediation:

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

Appendix: Change History

Date	Version	Changes for this version
04-02-2014	1.0.0	Initial Public Release