Center for Internet Security®

CIS Distribution Independent Linux

v1.0.1 - 01-31-2017

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Linux systems running on x86 and x64 platforms.

Commands and scripts are provided which should work on most distributions however some translation to local styles may be required in places. Where possible Red Hat, Debian, and SUSE derivative styles are provided.

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

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

To obtain the latest version of this guide, please visit <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 Linux on a x86 platform.

Consensus Guidance

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

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until

consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://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 - Server**

  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.

  This profile is intended for servers.

- **Level 2 - Server**

  This profile extends the "Level 1 - Server" 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.

  This profile is intended for servers.

- **Level 1 - Workstation**

  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.

  This profile is intended for workstations.

- **Level 2 - Workstation**

  This profile extends the "Level 1 - Workstation" 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.

This profile is intended for workstations.

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:

Editor
Rael Daruszka , *Center for Internet Security*
Ron Colvin
Jonathan Lewis Christopherson

This benchmark is based upon previous Linux benchmarks published and would not be possible without the contributions provided over the history of all of these benchmarks. The CIS community thanks everyone who has contributed to the Linux benchmarks.

Recommendations

1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' 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 recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

Note: If you are repartitioning a system that has already been installed, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the `/tmp` directory, this data will still consume space in `/` once the `/tmp` filesystem is mounted unless it is removed first.

1.1.1 Disable unused filesystems

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

Note: This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment.

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v cramfs
install /bin/true
```

```
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

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

Remediation:

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

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

Critical Controls:

13 Data Protection
Data Protection

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

```
# modprobe -n -v jffs2
install /bin/true
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.4 Ensure mounting of hfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

```
# modprobe -n -v hfs
install /bin/true
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

```
# modprobe -n -v hfsplus
install /bin/true
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.6 Ensure mounting of squashfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

```
# modprobe -n -v squashfs
install /bin/true
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.7 Ensure mounting of udf filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system. If this filesystem type is not needed, disable it.

Audit:

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

```
# modprobe -n -v udf
install /bin/true
# 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
```

Critical Controls:

13 Data Protection
Data Protection

1.1.1.8 Ensure mounting of FAT filesystems is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

The `FAT` filesystem format is primarily used on older windows systems and portable USB drives or flash modules. It comes in three types `FAT12` , `FAT16` , and `FAT32` all of which are supported by the `vfat` kernel module.

Rationale:

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

Audit:

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

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

Remediation:

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

```
install vfat /bin/true
```

Impact:

FAT filesystems are often used on portable USB sticks and other flash media are commonly used to transfer files between workstations, removing VFAT support may prevent the ability to transfer files in this way.

Critical Controls:

13 Data Protection
Data Protection

1.1.2 Ensure separate partition exists for /tmp (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output shows `/tmp` is mounted:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional

tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

Notes:

systemd includes the `tmp.mount` service which should be used instead of configuring `/etc/fstab`.

1.1.3 Ensure nodev option set on /tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

If a `/tmp` partition exists run the following command and verify that the `nodev` option is set on `/tmp`:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/tmp` :

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

Notes:

systemd includes the `tmp.mount` service which should be used instead of configuring `/etc/fstab`. Mounting options are configured in the `Options` setting in `/etc/systemd/system/tmp.mount`.

1.1.4 Ensure nosuid option set on /tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

If a `/tmp` partition exists run the following command and verify that the `nosuid` option is set on `/tmp`:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/tmp` :

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

Notes:

systemd includes the `tmp.mount` service which should be used instead of configuring `/etc/fstab`. Mounting options are configured in the `Options` setting in `/etc/systemd/system/tmp.mount`.

1.1.5 Ensure noexec option set on /tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

If a `/tmp` partition exists run the following command and verify that the `noexec` option is set on `/tmp`:

```
# mount | grep /tmp
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/tmp` :

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

Notes:

systemd includes the `tmp.mount` service which should be used instead of configuring `/etc/fstab`. Mounting options are configured in the `Options` setting in `/etc/systemd/system/tmp.mount`.

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

1.1.6 Ensure separate partition exists for /var (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify output shows `/var` is mounted:

```
# mount | grep /var
/dev/xvdg1 on /var type ext4 (rw,relatime,data=ordered)
```

Remediation:

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

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

1.1.7 Ensure separate partition exists for /var/tmp (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

Since the `/var/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 `/var/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/var/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:

Run the following command and verify output shows `/var/tmp` is mounted:

```
# mount | grep /var/tmp
tmpfs on /var/tmp type ext4 (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional

tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

1.1.8 Ensure nodev option set on /var/tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

Since the `/var/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 `/var/tmp` .

Audit:

If a `/var/tmp` partition exists run the following command and verify that the `nodev` option is set on `/var/tmp` .

```
# mount | grep /var/tmp
tmpfs on /var/tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/var/tmp` :

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

1.1.9 Ensure nosuid option set on /var/tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

If a `/var/tmp` partition exists run the following command and verify that the `nosuid` option is set on `/var/tmp` .

```
# mount | grep /var/tmp
tmpfs on /var/tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/var/tmp` :

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

1.1.10 Ensure noexec option set on /var/tmp partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

If a `/var/tmp` partition exists run the following command and verify that the `noexec` option is set on `/var/tmp` .

```
# mount | grep /var/tmp
tmpfs on /var/tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/var/tmp` :

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

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

1.1.11 Ensure separate partition exists for /var/log (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify output shows `/var/log` is mounted:

```
# mount | grep /var/log
/dev/xvdh1 on /var/log type ext4 (rw,relatime,data=ordered)
```

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, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)

Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

1.1.12 Ensure separate partition exists for /var/log/audit (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# mount | grep /var/log/audit
/dev/xvdi1 on /var/log/audit type ext4 (rw,relatime,data=ordered)
```

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, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

1.1.13 Ensure separate partition exists for /home (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify output shows `/home` is mounted:

```
# mount | grep /home
/dev/xvdf1 on /home type ext4 (rw,nodev,relatime,data=ordered)
```

Remediation:

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

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

1.1.14 Ensure nodev option set on /home partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Audit:

If a `/home` partition exists run the following command and verify that the `nodev` option is set on `/home` .

```
# mount | grep /home
/dev/xvdf1 on /home type ext4 (rw,nodev,relatime,data=ordered)
```

Remediation:

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

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

Notes:

The actions in this recommendation 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.

1.1.15 Ensure nodev option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify that the `nodev` option is set on `/dev/shm` .

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/dev/shm` :

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

Notes:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

1.1.16 Ensure nosuid option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify that the no `suid` option is set on `/dev/shm`.

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/dev/shm`:

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

Notes:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

1.1.17 Ensure noexec option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

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 command and verify that the `noexec` option is set on `/dev/shm`.

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

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

Run the following command to remount `/dev/shm`:

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

Notes:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

1.1.18 Ensure nodev option set on removable media partitions (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify that the `nodev` option is set on all removable media partitions.

```
# mount
```

Remediation:

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

1.1.19 Ensure nosuid option set on removable media partitions (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify that the `nosuid` option is set on all removable media partitions.

```
# mount
```

Remediation:

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

1.1.20 Ensure noexec option set on removable media partitions (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

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:

Run the following command and verify that the `noexec` option is set on all removable media partitions.

```
# mount
```

Remediation:

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

Critical Controls:

8 Malware Defenses
Malware Defenses

1.1.21 Ensure sticky bit is set on all world-writable directories (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

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

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

No output should be returned.

Remediation:

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

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

Notes:

Some distributions may not support the `--local` option to `df`.

Critical Controls:

13 Data Protection
Data Protection

1.1.22 Disable Automounting (Scored)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

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 its contents available in system even if they lacked permissions to mount it themselves.

Audit:

Run one of the following commands to verify `autofs` is not enabled:

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

Verify all runlevels are listed as "off" or autofs is not available.

```
# systemctl is-enabled autofs
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep autofs
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `autofs` :

```
# chkconfig autofs off
# systemctl disable autofs
# update-rc.d autofs disable
```

Impact:

The use portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

Critical Controls:

8.3 Limit Use Of External Devices (i.e. USB)
Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.

1.2 Configure Software Updates

Most distributions use a package manager such as yum, apt, or zypper to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

For the purpose of this benchmark, the requirement is to ensure that a patch management system is configured and maintained. The specifics on patch update procedures are left to the organization.

1.2.1 Ensure package manager repositories are configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

Audit:

Verify package repositories are configured correctly. Depending on the package management in use one of the following command groups may provide the needed information:

```
# yum repo-list
# apt-cache policy
# zypper repos
```

Remediation:

Configure your package manager repositories according to site policy.

Critical Controls:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

1.2.2 Ensure GPG keys are configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Most packages managers implement GPG key signing to verify package integrity during installation.

Rationale:

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

Audit:

Verify GPG keys are configured correctly for your package manager. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
# apt-key list
# zypper repos
```

Remediation:

Update your package manager GPG keys in accordance with site policy.

Critical Controls:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

1.3 Filesystem Integrity Checking

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

1.3.1 Ensure AIDE is installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

Rationale:

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Audit:

Verify AIDE is installed. Depending on the package management in use one of the following commands may provide the needed information:

```
# rpm -q aide
# dpkg -s aide
```

Remediation:

Install AIDE using the appropriate package manager or manual installation:

```
# yum install aide
# apt-get install aide
# zypper install aide
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE:

```
# aide --init
```

References:

1. AIDE stable manual: http://aide.sourceforge.net/stable/manual.html

Notes:

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

Critical Controls:

3.5 Use File Integrity Tools For Critical System Files
Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

1.3.2 Ensure filesystem integrity is regularly checked (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

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:

Run the following commands to determine if there is a `cron` job scheduled to run the aide check.

```
# crontab -u root -l | grep aide
# grep -r aide /etc/cron.* /etc/crontab
```

Ensure a cron job in compliance with site policy is returned.

Remediation:

Run the following command:

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

Add the following line to the crontab:

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

Notes:

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

Critical Controls:

3.5 Use File Integrity Tools For Critical System Files
Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes;

highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

1.4 Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

1.4.1 Ensure permissions on bootloader config are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually `grub.conf` , `grub.cfg` , or `menu.lst` stored in either `/boot/grub` or `/boot/grub2` . It is commonly symlinked as `/etc/grub.conf` as well.

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /boot/grub/menu.lst
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on your grub configuration:

```
# chown root:root /boot/grub/menu.lst
# chmod og-rwx /boot/grub/menu.lst
```

Notes:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/menu.lst` with the appropriate grub configuration file for your environment

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.4.2 Ensure bootloader password is set (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

For `grub` based systems run the following command and verify output matches:

```
# grep "^password" /boot/grub/menu.lst
password --md5 <encrypted-password>
```

For `grub2` based systems run the following commands and verify output matches:

```
# grep "^set superusers" /boot/grub/menu.lst
set superusers="<username>"
# grep "^password" /boot/grub/grub.cfg
password_pbkdf2 <username> <encrypted-password>
```

Remediation:

For `grub` based systems create an encrypted password with `grub-md5-crypt` :

```
# grub-md5-crypt
Password: <password>
Retype Password: <password>
<encrypted-password>
```

Copy and paste the into the global section of `/boot/grub/menu.lst` :

```
password --md5 <encrypted-password>
```

For `grub2` based systems create an encrypted password with `grub-mkpasswd-pbkdf2` :

```
# 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="<username>"
password_pbkdf2 <username> <encrypted-password>
EOF
```

Run the following command to update the `grub2` configuration:

```
# update-grub
```

Notes:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/menu.lst` with the appropriate grub configuration file for your environment

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.4.3 Ensure authentication required for single user mode (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Single user mode is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

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:

Verify that a password is required for single user mode. This can be done by rebooting the system into single user mode or checking the relevant configuration files. One or more of the following conditions may be used on your system:

- A password is set for the `root` user.
- `/sbin/sulogin` is set for single user mode in `/etc/inittab` :

```
~~:S:respawn:/sbin/sulogin
```

- /sbin/sulogin is set for single user mode in `/etc/sysconfig/init` :

```
SINGLE=/sbin/sulogin
```

Remediation:

Consult your documentation and configure single user mode to require a password for login as appropriate.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.4.4 Ensure interactive boot is not enabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Interactive boot allows console users to interactively select which services start on boot. Not all distributions support this capability.

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

Rationale:

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

Audit:

If interactive boot is available verify it is disabled on your system. On some distributions this is configured via the `PROMPT_FOR_CONFIRM` option in `/etc/sysconfig/boot` :

```
# grep "^PROMPT_FOR_CONFIRM=" /etc/sysconfig/boot
PROMPT_FOR_CONFIRM="no"
```

Remediation:

If interactive boot is available disable it.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.5 Additional Process Hardening

1.5.1 Ensure core dumps are restricted (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following commands and verify output matches:

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

Remediation:

Add the following line to the `/etc/security/limits.conf` file or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Set the following parameter in the `/etc/sysctl.conf` file:

```
fs.suid_dumpable = 0
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid-dumpable=1
```

Critical Controls:

13 Data Protection
Data Protection

1.5.2 Ensure XD/NX support is enabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 command and verify 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.

Notes:

Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.

Critical Controls:

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)
Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

1.5.3 Ensure address space layout randomization (ASLR) is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale:

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

Audit:

Run the following command and verify output matches:

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

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

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

Critical Controls:

8.4 Enable Anti-exploitation Features (i.e. DEP, ASLR, EMET)
Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.

1.5.4 Ensure prelink is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`prelink`is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

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:

Verify `prelink` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
# rpm -q prelink
# dpkg -s prelink
```

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

Uninstall `prelink` using the appropriate package manager or manual installation:

```
# yum remove prelink
# apt-get remove prelink
# zypper remove prelink
```

Critical Controls:

3.5 Use File Integrity Tools For Critical System Files
Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration

changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).

1.6 Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

Impact: Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

1.6.1 Configure SELinux

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under SELinux, every process and every object (files, sockets, pipes) on the system is assigned a security context, a label that includes detailed type information about the object. The kernel allows processes to access objects only if that access is explicitly allowed by the policy in effect. The policy defines transitions, so that a user can be allowed to run software, but the software can run under a different context than the user's default. This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation. Three such policies have been designed for use with RHEL7 and are included with the system: `targeted`, `strict`, and `mls`. These are described as follows:

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

This section provides guidance for the configuration of the `targeted`policy.

Note: This section only applies if SELinux is in use on the system. Recommendations for AppArmor are also included, and additional Mandatory Access Control systems exist beyond these two.

References:

1. NSA SELinux resources:
    1. http://www.nsa.gov/research/selinux
    2. http://www.nsa.gov/research/selinux/list.shtml
2. Fedora SELinux resources:
    1. FAQ: http://docs.fedoraproject.org/selinux-faq
    2. User Guide: http://docs.fedoraproject.org/selinux-user-guide
    3. Managing Services Guide: http://docs.fedoraproject.org/selinux-managing-confined-services-guide
3. SELinux Project web page and wiki:
    1. http://www.selinuxproject.org

4. Chapters 43-45 of Red Hat Enterprise Linux 5: Deployment Guide (Frank Mayer, Karl MacMillan and David Caplan),
5. SELinux by Example: Using Security Enhanced Linux (Prentice Hall, August 6, 2006)

1.6.1.1 Ensure SELinux is not disabled in bootloader configuration (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

Audit:

For `grub` based systems run the following command and verify that no kernel line has the `selinux=0` or `enforcing=0` parameters set:

```
# grep "^\s*kernel" /boot/grub/menu.lst
```

For `grub2` based systems run the following command and verify that no linux line has the `selinux=0` or `enforcing=0` parameters set:

```
# grep "^\s*linux" /boot/grub/menu.lst
```

Remediation:

For `grub` based systems edit `/boot/grub/menu.lst` and remove all instances of `selinux=0` and `enforcing=0` on all `kernel` lines.

For `grub2` based systems edit /etc/default/grub and remove all instances of `selinux=0` and `enforcing=0` from all CMDLINE_LINUX parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""
```

Run the following command to update the `grub2` configuration:

```
# update-grub
```

Notes:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/menu.lst` with the appropriate bootloader configuration file for your environment.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.6.1.2 Ensure the SELinux state is enforcing (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Set SELinux to enable when the system is booted.

Rationale:

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

Audit:

Run the following commands and ensure output matches:

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

# sestatus
SELinux status: enabled
Current mode: enforcing
Mode from config file: enforcing
```

Remediation:

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

```
SELINUX=enforcing
```

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.6.1.3 Ensure SELinux policy is configured (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following commands and ensure output matches either " `targeted` " or " `mls` ":

```
# grep SELINUXTYPE=targeted /etc/selinux/config
SELINUXTYPE=targeted

# sestatus
Policy from config file: targeted
```

Remediation:

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

```
SELINUXTYPE=targeted
```

Notes:

If your organization requires stricter policies, ensure that they are set in the `/etc/selinux/config`file.

1.6.1.4 Ensure SETroubleshoot is not installed (Scored)

Profile Applicability:

- Level 2 - Server

Description:

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

Rationale:

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

Audit:

Verify s `etroubleshoot` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
# rpm -q setroubleshoot
# dpkg -s setroubleshoot
```

Remediation:

Uninstall s `etroubleshoot` using the appropriate package manager or manual installation:

```
# yum remove setroubleshoot
# apt-get remove setroubleshoot
# zypper remove setroubleshoot
```

1.6.1.5 Ensure the MCS Translation Service (mcstrans) is not installed (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Verify `mcstrans` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -q mcstrans
dpkg -s mcstrans
```

Remediation:

Uninstall `mcstrans` using the appropriate package manager or manual installation:

```
yum remove mcstrans
apt-get remove mcstrans
zypper remove mcstrans
```

1.6.1.6 Ensure no unconfined daemons exist (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command and verify not output is produced:

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

Remediation:

Investigate any unconfined daemons found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

Notes:

Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.6.2 Configure AppArmor

AppArmor provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under AppArmor MAC rules are applied by file paths instead of by security contexts as in other MAC systems. As such it does not require support in the filesystem and can be applied to network mounted filesystems for example. AppArmor security policies define what system resources applications can access and what privileges they can do so with. This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the 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.

Note: This section only applies if AppArmor is in use on the system. Recommendations for SELinux are also included, and additional Mandatory Access Control systems exist beyond these two.

References:

1. AppArmor Documentation: http://wiki.apparmor.net/index.php/Documentation
2. Ubuntu AppArmor Documentation: https://help.ubuntu.com/community/AppArmor
3. SUSE AppArmor Documentation: https://www.suse.com/documentation/apparmor/

1.6.2.1 Ensure AppArmor is not disabled in bootloader configuration (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters.

Rationale:

AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

Audit:

For `grub` based systems run the following command and verify that no kernel line has the `apparmor=0` parameter set:

```
# grep "^\s*kernel" /boot/grub/menu.lst
```

For `grub2` based systems run the following command and verify that no linux line the `apparmor=0` parameter set:

```
# grep "^\s*linux" /boot/grub/menu.lst
```

Remediation:

For `grub` based systems edit `/boot/grub/menu.lst` and remove all instances of `apparmor=0` on all `kernel` lines.

For `grub2` based systems edit /etc/default/grub and remove all instances of `apparmor=0` from all CMDLINE_LINUX parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet"
GRUB_CMDLINE_LINUX=""
```

Run the following command to update the `grub2` configuration:

```
# update-grub
```

Notes:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/menu.lst` with the appropriate grub configuration file for your environment.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.6.2.2 Ensure all AppArmor Profiles are enforcing (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

AppArmor profiles define what resources applications are able to access.

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

Audit:

Run the following command and verify that profiles are loaded, no profiles are in complain mode, and no processes are unconfined:

```
# apparmor_status
apparmor module is loaded.
17 profiles are loaded.
17 profiles are in enforce mode.
   /bin/ping
   /sbin/klogd
   /sbin/syslog-ng
   /sbin/syslogd
   /usr/lib/PolicyKit/polkit-explicit-grant-helper
   /usr/lib/PolicyKit/polkit-grant-helper
   /usr/lib/PolicyKit/polkit-grant-helper-pam
   /usr/lib/PolicyKit/polkit-read-auth-helper
   /usr/lib/PolicyKit/polkit-resolve-exe-helper
   /usr/lib/PolicyKit/polkit-revoke-helper
   /usr/lib/PolicyKit/polkitd
   /usr/sbin/avahi-daemon
   /usr/sbin/identd
   /usr/sbin/mdnsd
   /usr/sbin/nscd
   /usr/sbin/ntpd
   /usr/sbin/traceroute
0 profiles are in complain mode.
1 processes have profiles defined.
1 processes are in enforce mode :
   /usr/sbin/nscd (3979)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```

Remediation:

Run the following command to set all profiles to enforce mode:

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

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

Critical Controls:

14.4 Protect Information With Access Control Lists

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

1.6.3 Ensure SELinux or AppArmor are installed (Not Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

SELinux and AppArmor provide Mandatory Access Controls.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Audit:

Verify either SELinux or AppArmor is installed. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q libselinux
# rpm -q apparmor
# dpkg -s libselinux1
# dpkg -s apparmor
```

Remediation:

Install SELinux or apparmor using the appropriate package manager or manual installation:

```
# yum install libselinux
# apt-get install libselinux1
# zypper install libselinux
```

The previous commands install SELinux, use the appropriate package if AppArmor is desired.

Notes:

SELinux and AppArmor both have several package names in use on different distributions. Research the appropriate packages for your environment.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share,

claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.7 Warning Banners

Presenting a warning message prior to the normal user login may assist in 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.

1.7.1 Command Line Warning Banners

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

1.7.1.1 Ensure message of the day is configured properly (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

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 `\r` - operating system release `\s` - operating system name `\v` - operating system version

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. 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:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

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

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, or `\v`.

1.7.1.2 Ensure local login warning banner is configured properly (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

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:

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. 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:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

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

Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , or `\v` :

```
# echo "Authorized uses only. All activity may be monitored and reported." >
/etc/issue
```

1.7.1.3 Ensure remote login warning banner is configured properly (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

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:

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. 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:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

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

Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, or `\v`:

```
# echo "Authorized uses only. All activity may be monitored and reported." >
/etc/issue.net
```

1.7.1.4 Ensure permissions on /etc/motd are configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Rationale:

If the `/etc/motd` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/motd` :

```
# chown root:root /etc/motd
# chmod 644 /etc/motd
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.7.1.5 Ensure permissions on /etc/issue are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Rationale:

If the `/etc/issue` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/issue
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue` :

```
# chown root:root /etc/issue
# chmod 644 /etc/issue
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.7.1.6 Ensure permissions on /etc/issue.net are configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Rationale:

If the `/etc/issue.net` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue.net` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.7.2 Ensure GDM login banner is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

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.

Audit:

If GDM is installed on the system verify that `/etc/dconf/profile/gdm` exists and contains the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Then verify the `banner-message-enable` and `banner-message-text` options are configured in `/etc/dconf/db/gdm.d/01-banner-message`:

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

Remediation:

Create the `/etc/dconf/profile/gdm` file with the following contents:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Create or edit the `banner-message-enable` and `banner-message-text` options in `/etc/dconf/db/gdm.d/01-banner-message`:

```
[org/gnome/login-screen]
banner-message-enable=true
```

```
banner-message-text='Authorized uses only. All activity may be monitored and
reported.'
```

Run the following command to update the system databases:

```
# dconf update
```

Notes:

Additional options and sections may appear in the `/etc/dconf/db/gdm.d/01-banner-message` file.

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

1.8 Ensure updates, patches, and additional security software are installed (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify there are no updates or patches to install. Depending on the package management in use one of the following command groups may provide the needed information:

```
# yum check-update
# apt-get -s upgrade
# zypper list-updates
```

Remediation:

Use your package manager to update all packages on the system according to site policy.

Notes:

Site policy may mandate a testing period before install onto production systems for available updates.

Critical Controls:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system

and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

2 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 some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

2.1 inetd Services

inetd is a super-server daemon that provides internet services and passes connections to configured services. While not commonly used inetd and any unneeded inetd based services should be disabled if possible.

2.1.1 Ensure chargen services are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `chargen` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^chargen" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `chargen` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `chargen` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `chargen` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services

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

9.1 Limit Open Ports, Protocols, and Services

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

2.1.2 Ensure daytime services are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `daytime` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^daytime" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `daytime` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `daytime` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `daytime` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.3 Ensure discard services are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `discard` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^discard" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `discard` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `discard` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `discard` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.4 Ensure echo services are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `echo` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^echo" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `echo` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `echo` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `echo` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.5 Ensure time services are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `time` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^time" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `time` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `time` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `time` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.6 Ensure rsh server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Verify the rsh services are not enabled. Run the following commands and verify results are as indicated:

```
grep -R "^shell" /etc/inetd.*
grep -R "^login" /etc/inetd.*
grep -R "^exec" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `rsh` , `rlogin` , and `rexec` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `shell` , `login` , or `exec` from `/etc/inetd.conf` and `/etc/inetd.d/*` .

Set `disable = yes` on all `rsh` , `rlogin` , and `rexec` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*` .

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not

actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

9.1 Limit Open Ports, Protocols, and Services

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

2.1.7 Ensure talk server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `talk` service is not enabled. Run the following commands and verify results are as indicated:

```
grep -R "^talk" /etc/inetd.*
grep -R "^ntalk" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all talk services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `talk` or `ntalk` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `talk` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.8 Ensure telnet server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `telnet` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^telnet" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `telnet` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `telnet` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `telnet` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

9.1 Limit Open Ports, Protocols, and Services

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

2.1.9 Ensure tftp server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify the `tftp` service is not enabled. Run the following command and verify results are as indicated:

```
grep -R "^tftp" /etc/inetd.*
```

No results should be returned

check `/etc/xinetd.conf` and `/etc/xinetd.d/*` and verify all `tftp` services have `disable = yes` set.

Remediation:

Comment out or remove any lines starting with `tftp` from `/etc/inetd.conf` and `/etc/inetd.d/*`.

Set `disable = yes` on all `tftp` services in `/etc/xinetd.conf` and `/etc/xinetd.d/*`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.1.10 Ensure xinetd is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run one of the following commands to verify `xinetd` is not enabled:

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

Verify all runlevels are listed as "off" or autofs is not available.

```
# systemctl is-enabled xinetd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep xinetd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to verify xinetd is not enabled:

```
# chkconfig xinetd off
# systemctl disable xinetd
# update-rc.d xinetd disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2 Special Purpose Services

This section describes services that are installed on systems 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.

2.2.1 Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as NTP or chrony.

2.2.1.1 Ensure time synchronization is in use (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

On physical systems or virtual systems where host based time synchronization is not available verify either NTP or chrony is installed. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q ntp
# rpm -q chrony
# dpkg -s ntp
# dpkg -s chrony
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use.

Remediation:

On physical systems or virtual systems where host based time synchronization is not available install NTP or chrony using the appropriate package manager or manual installation:

```
# yum install ntp
# apt-get install ntp
# zypper install ntp
```

The previous commands install NTP, use the appropriate package if chrony is desired.

On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

Critical Controls:

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment
Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

2.2.1.2 Ensure ntp is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`ntp` is a daemon which implements the Network Time Protocol (NTP). It 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.

This recommendation only applies if ntp is in use on the system.

Rationale:

If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Audit:

Run the following command and verify output matches:

```
# grep "^restrict" /etc/ntp.conf
restrict -4 default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

The `-4` in the first line is optional and options after `default` can appear in any order. Additional restriction lines may exist.

Run the following command and verify remote server is configured properly:

```
# grep "^server" /etc/ntp.conf
server <remote-server>
```

Multiple servers may be configured.

Verify that `ntp` is configured to run as the `ntp` user by running one of the following commands as appropriate for your distribution and verifying output matches:

```
# grep "^OPTIONS" /etc/sysconfig/ntpd
OPTIONS="-u ntp:ntp"
```

Additional options may be present.

```
# grep "RUNASUSER=ntp" /etc/init.d/ntp
RUNASUSER=ntp
```

Remediation:

Add or edit restrict lines in `/etc/ntp.conf` to match the following:

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

Add or edit server lines to `/etc/ntp.conf` as appropriate:

```
server <remote-server>
```

Configure `ntp` to run as the `ntp` user by adding or editing one of the following files as appropriate for your distribution: `/etc/sysconfig/ntpd` :

```
OPTIONS="-u ntp:ntp"
```

`/etc/init.d/ntp`:

```
RUNASUSER=ntp
```

Critical Controls:

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment
Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

2.2.1.3 Ensure chrony is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`chrony` is a daemon which implements 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 `chrony` can be found at http://chrony.tuxfamily.org/. `chrony` can be configured to be a client and/or a server.

Rationale:

If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

This recommendation only applies if chrony is in use on the system.

Audit:

Run the following command and verify remote server is configured properly:

```
# grep "^server" /etc/chrony.conf
server <remote-server>
```

Multiple servers may be configured.

Run the following command and verify the first field for the `chronyd` process is `chrony` :

```
# ps -ef | grep chronyd
chrony     491     1  0 20:32 ?        00:00:00 /usr/sbin/chronyd
```

Remediation:

Add or edit server lines to `/etc/chrony.conf` as appropriate:

```
server <remote-server>
```

Configure `chrony` to run as the `chrony` user by configuring the appropriate startup script for your distribution. Startup scripts are typically stored in `/etc/init.d` or `/etc/systemd` .

Critical Controls:

6.1 Use At Least Two Synchronized Time Sources For All Servers And Network Equipment

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

2.2.2 Ensure X Window System is not installed (Scored)

Profile Applicability:

- Level 1 - Server

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 Windows system is typically used on workstations 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:

Verify X Windows System is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -qa xorg-x11*
dpkg -l xserver-xorg*
```

Remediation:

Remove the X Windows System packages using the appropriate package manager or manual installation:

```
yum remove xorg-x11*
apt-get remove xserver-xorg*
zypper remove xorg-x11*
```

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

2.2.3 Ensure Avahi Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attach surface.

Audit:

Run one of the following commands to disable `avahi-daemon` :

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

Verify all runlevels are listed as "off" or `avahi-daemon` is not available.

```
# systemctl is-enabled avahi-daemon
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep avahi-daemon
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to verify `avahi-daemon` is not enabled:

```
# chkconfig avahi-daemon off
# systemctl disable avahi-daemon
# update-rc.d avahi-daemon disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.4 Ensure CUPS is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

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:

Run one of the following commands to verify `cups` is not enabled:

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

Verify all runlevels are listed as "off" or `cups` is not available.

```
# systemctl is-enabled cups
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep cups
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `cups` :

```
# chkconfig cups off
# systemctl disable cups
# update-rc.d cups disable
```

Impact:

Disabling CUPS will prevent printing from the system, a common task for workstation systems.

References:

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

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.5 Ensure DHCP Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

Unless a system 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:

Run one of the following commands to disable `dhcpd` :

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

Verify all runlevels are listed as "off" or `dhcpd` is not available.

```
# systemctl is-enabled dhcpd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep dhcpd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `dhcpd` :

```
# chkconfig dhcpd off
# systemctl disable dhcpd
# update-rc.d dhcpd disable
```

References:

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

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.6 Ensure LDAP server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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

Audit:

Run one of the following commands to verify `slapd` is not enabled:

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

Verify all runlevels are listed as "off" or `slapd` is not available.

```
# systemctl is-enabled slapd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep slapd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `slapd` :

```
# chkconfig slapd off
# systemctl disable slapd
# update-rc.d slapd disable
```

References:

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

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.7 Ensure NFS and RPC are not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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:

Run one of the following commands to verify `nfs` is not enabled:

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

Verify all runlevels are listed as "off" or `nfs` is not available.

```
# systemctl is-enabled nfs
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep nfs
```

Verify no S* lines are returned.

Run one of the following commands to verify `rpcbind` is not enabled:

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

Verify all runlevels are listed as "off" or `rpcbind` is not available.

```
# systemctl is-enabled rpcbind
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep rpcbind
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `nfs` and `rpcbind`:

```
# chkconfig nfs off
# chkconfig rpcbind off
# systemctl disable nfs
# systemctl disable rpcbind
# update-rc.d nfs disable
# update-rc.d rpcbind disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.8 Ensure DNS Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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 one of the following commands to verify `named` is not enabled:

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

Verify all runlevels are listed as "off" or `named` is not available.

```
# systemctl is-enabled named
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep named
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `named` :

```
# chkconfig named off
# systemctl disable named
# update-rc.d named disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services

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

2.2.9 Ensure FTP Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run one of the following commands to verify `vsftpd` is not enabled:

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

Verify all runlevels are listed as "off" or `vsftpd` is not available.

```
# systemctl is-enabled vsftpd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep vsftpd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `vsftpd` :

```
# chkconfig vsftpd off
# systemctl disable vsftpd
# update-rc.d vsftpd disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Additional FTP servers also exist and should be audited.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.10 Ensure HTTP server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 one of the following commands to verify `httpd` is not enabled:

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

Verify all runlevels are listed as "off" or `httpd` is not available.

```
# systemctl is-enabled httpd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep httpd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `httpd` :

```
# chkconfig httpd off
# systemctl disable httpd
# update-rc.d httpd disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several httpd servers exist and can use other service names. `apache`, `apache2`, `lighttpd`, and `nginx` are example services that provide an HTTP server. These and other services should also be audited.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.11 Ensure IMAP and POP3 server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 by this system, it is recommended that the service be deleted to reduce the potential attack surface.

Audit:

Run one of the following commands to verify `dovecot` is not enabled:

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

Verify all runlevels are listed as "off" or `dovecot` is not available.

```
# systemctl is-enabled dovecot
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep dovecot
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `dovecot` :

```
# chkconfig dovecot off
# systemctl disable dovecot
# update-rc.d dovecot disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Several IMAP/POP3 servers exist and can use other service names. `exim` and `cyrus-imap` are example services that provide an HTTP server. These and other services should also be audited.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.12 Ensure Samba is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run one of the following commands to verify `smb` is not enabled:

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

Verify all runlevels are listed as "off" or `smb` is not available.

```
# systemctl is-enabled smb
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep smb
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `smb` :

```
# chkconfig smb off
# systemctl disable smb
# update-rc.d smb disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the samba service is known as `samba`, not `smb`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.13 Ensure HTTP Proxy Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run one of the following commands to verify `squid` is not enabled:

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

Verify all runlevels are listed as "off" or `squid` is not available.

```
# systemctl is-enabled squid
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep squid
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `squid` :

```
# chkconfig squid off
# systemctl disable squid
# update-rc.d squid disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the squid service is known as `squid3`, not `squid`. Several HTTP proxy servers exist. These and other services should be checked.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.14 Ensure SNMP Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 one of the following commands to verify `snmpd` is not enabled:

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

Verify all runlevels are listed as "off" or `snmpd` is not available.

```
# systemctl is-enabled snmpd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep snmpd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `snmpd` :

```
# chkconfig snmpd off
# systemctl disable snmpd
# update-rc.d snmpd disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services

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

2.2.15 Ensure mail transfer agent is configured for local-only mode (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

Audit:

Run the following command and verify that the MTA is not listening on any non-loopback address (`127.0.0.1` or `::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
```

Notes:

This recommendation is designed around 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.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.16 Ensure rsync service is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run one of the following commands to verify `rsyncd` is not enabled:

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

Verify all runlevels are listed as "off" or `rsyncd` is not available.

```
# systemctl is-enabled rsyncd
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep rsyncd
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `rsyncd` :

```
# chkconfig rsyncd off
# systemctl disable rsyncd
# update-rc.d rsyncd disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the rsync service is known as `rsync`, not `rsyncd`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.2.17 Ensure NIS Server is not enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run one of the following commands to verify `ypserv` is not enabled:

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

Verify all runlevels are listed as "off" or `ypserv` is not available.

```
# systemctl is-enabled ypserv
disabled
```

Verify result is not "enabled".

```
# ls /etc/rc*.d | grep ypserv
```

Verify no S* lines are returned.

Remediation:

Run one of the following commands to disable `ypserv` :

```
# chkconfig ypserv off
# systemctl disable ypserv
# update-rc.d ypserv disable
```

Notes:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the NIS service is known as `nis`, not `ypserv`.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

2.3 Service Clients

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

Note: This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

2.3.1 Ensure NIS Client is not installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Verify `ypbind` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -q ypbind
dpkg -s ypbind
```

Remediation:

Uninstall `ypbind` using the appropriate package manager or manual installation:

```
yum remove ypbind
apt-get remove ypbind
zypper remove ypbind
```

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

2.3.2 Ensure rsh client is not installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify `rsh` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -q rsh
dpkg -s rsh
```

Remediation:

Uninstall `rsh` using the appropriate package manager or manual installation:

```
yum remove rsh
apt-get remove rsh
zypper remove rsh
```

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

2.3.3 Ensure talk client is not installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Verify `talk` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -q talk
dpkg -s talk
```

Remediation:

Uninstall `talk` using the appropriate package manager or manual installation:

```
yum remove talk
apt-get remove talk
zypper remove talk
```

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

2.3.4 Ensure telnet client is not installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Verify `telnet` is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
# rpm -q telnet
# dpkg -s telnet
```

Remediation:

Uninstall `telnet` using the appropriate package manager or manual installation:

```
# yum remove telnet
# apt-get remove telnet
# zypper remove telnet
```

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar

equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

2.3.5 Ensure LDAP client is not installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

Audit:

Verify openldap-clients is not installed. Depending on the package management in use one of the following commands may provide the needed information:

```
# rpm -q openldap-clients
# dpkg -s openldap-clients
```

Remediation:

Uninstall `openldap-clients` using the appropriate package manager or manual installation:

```
# yum remove openldap-clients
# apt-get remove openldap-clients
# zypper remove openldap-clients
```

Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

Notes:

The `openldap-clients` package can go by other names on some distributions. `openldap2-client`, and `ldap-utils` are known alternative package names.

Critical Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

3 Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

3.1 Network Parameters (Host Only)

The following network parameters are intended for use 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.

3.1.1 Ensure IP forwarding is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `net.ipv4.ip_forward` flag is used to tell the system whether it can forward packets or not.

Rationale:

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

Audit:

Run the following command and verify output matches:

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

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.1.2 Ensure packet redirect sending is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2 Network Parameters (Host and Router)

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

3.2.1 Ensure source routed packets are not accepted (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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 system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Audit:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.2 Ensure ICMP redirects are not accepted (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.3 Ensure secure ICMP redirects are not accepted (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.4 Ensure suspicious packets are logged (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system.

Audit:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

3.2.5 Ensure broadcast ICMP requests are ignored (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.6 Ensure bogus ICMP responses are ignored (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.7 Ensure Reverse Path Filtering is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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 system, you will not be able to enable this feature without breaking the routing.

Audit:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.2.8 Ensure TCP SYN Cookies is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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 system 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 system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameter in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.3 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.

3.3.1 Ensure IPv6 router advertisements are not accepted (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This setting disables the system's ability to accept IPv6 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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.3.2 Ensure IPv6 redirects are not accepted (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify output matches:

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

Remediation:

Set the following parameters in the `/etc/sysctl.conf` file:

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

Run the following commands to set the active kernel parameters:

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

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches

Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.3.3 Ensure IPv6 is disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify output includes indicated line:

```
# modprobe -c | grep ipv6
...
options ipv6 disable=1
...
```

Remediation:

Create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
options ipv6 disable=1
```

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

3.4 TCP Wrappers

3.4.1 Ensure TCP Wrappers is installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify TCP Wrappers is installed. Depending on the package management in use one of the following commands may provide the needed information:

```
rpm -q tcpd
dpkg -s tcpd
```

Remediation:

Install TCP Wrappers using the appropriate package manager or manual installation:

```
yum install tcpd
apt-get install tcpd
zypper install tcpd
```

Notes:

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.

Critical Controls:

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

3.4.2 Ensure /etc/hosts.allow is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system.

Audit:

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

```
# cat /etc/hosts.allow
```

Remediation:

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

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

where each / 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.

Notes:

Contents of the `/etc/hosts.allow` file will vary depending on your network configuration.

Critical Controls:

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

3.4.3 Ensure /etc/hosts.deny is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system.

Audit:

Run the following command and verify the contents of the `/etc/hosts.deny` file:

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

Remediation:

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

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

Notes:

Contents of the `/etc/hosts.deny` file may include additional options depending on your network configuration.

Critical Controls:

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

3.4.4 Ensure permissions on /etc/hosts.allow are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/hosts.allow
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/hosts.allow` :

```
# chown root:root /etc/hosts.allow
# chmod 644 /etc/hosts.allow
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.4.5 Ensure permissions on /etc/hosts.deny are 644 (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/hosts.deny
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/hosts.deny` :

```
# chown root:root /etc/hosts.deny
# chmod 644 /etc/hosts.deny
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

3.5 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.

Note: This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

3.5.1 Ensure DCCP is disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

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

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

Remediation:

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

```
install dccp /bin/true
```

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services

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

3.5.2 Ensure SCTP is disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

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

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

Remediation:

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

```
install sctp /bin/true
```

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

3.5.3 Ensure RDS is disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

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

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

Remediation:

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

```
install rds /bin/true
```

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

3.5.4 Ensure TIPC is disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

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

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

Remediation:

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

```
install tipc /bin/true
```

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

3.6 Firewall Configuration

IPtables is an application that allows a system administrator to configure the IPv4 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPtables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note: This section broadly assumes starting with an empty IPtables firewall ruleset (established by flushing the rules with `iptables -F`). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.6.1 Ensure iptables is installed (Scored)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

`iptables` allows configuration of the IPv4 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to `iptables`.

Rationale:

iptables is required for firewall management and configuration.

Audit:

Verify iptables is installed. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q iptables
# dpkg -s iptables
```

Remediation:

Install `iptables` using the appropriate package manager or manual installation:

```
# yum install iptables
# apt-get install iptables
# zypper install iptables
```

Critical Controls:

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

3.6.2 Ensure default deny firewall policy (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the `INPUT` , `OUTPUT` , and `FORWARD` chains is `DROP` or `REJECT` :

```
# iptables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

Critical Controls:

9.2 Leverage Host-based Firewalls

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

3.6.3 Ensure loopback traffic is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       127.0.0.0/8          0.0.0.0/0

 # iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

Critical Controls:

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

3.6.4 Ensure outbound and established connections are configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

Critical Controls:

9.2 Leverage Host-based Firewalls

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

3.6.5 Ensure firewall rules exist for all open ports (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
```

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       all  --  *      *       127.0.0.0/8         0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.

The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

Notes:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

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

3.7 Ensure wireless interfaces are disabled (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

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

Rationale:

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

Audit:

Run the following command to determine wireless interfaces on the system:

```
# iwconfig
```

Run the following command and verify wireless interfaces are active:

```
# ip link show up
```

Remediation:

Run the following command to disable any wireless interfaces:

```
# ip link set <interface> down
```

Disable any wireless interfaces in your network configuration.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

Critical Controls:

15.4 Configure Only Authorized Wireless Access On Client Machines
Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices

that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

4 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`).

4.1 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.

The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations. **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.

Note: Several recommendations in this section filter based off of `auid>=500` for unprivileged non-system users. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

Note: Once all configuration changes have been made to `/etc/audit/audit.rules`, the auditd configuration must be reloaded:

```
# service auditd reload
```

4.1.1 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.

4.1.1.1 Ensure audit log storage size is configured (Not Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and ensure output is in compliance with site policy:

```
# grep max_log_file /etc/audit/auditd.conf
max_log_file = <MB>
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

Notes:

The max_log_file parameter is measured in megabytes.

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)

Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.1.1.2 Ensure system is disabled when audit logs are full (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following commands and verify output matches:

```
# 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:

Set the following parameters in `/etc/audit/auditd.conf`:

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

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.1.1.3 Ensure audit logs are not automatically deleted (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Audit:

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.1.2 Ensure auditd service is enabled (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run one of the following commands to verify `auditd` is enabled:

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

Verify runlevels 2 through 5 are "on".

```
# systemctl is-enabled auditd
enabled
```

Verify result is "enabled".

```
# ls /etc/rc*.d | grep auditd
```

Verify S* lines are returned for runlevels 2 through 5.

Remediation:

Run one of the following commands to enable `auditd` :

```
# chkconfig auditd on
# systemctl enable auditd
# update-rc.d auditd enable
```

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.1.3 Ensure auditing for processes that start prior to auditd is enabled (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure `grub` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

For `grub` based systems run the following command and verify that each kernel line has the `audit=1` parameter set:

```
# grep "^\s*kernel" /boot/grub/menu.lst
```

For `grub2` based systems run the following command and verify that each linux line has the `audit=1` parameter set:

```
# grep "^\s*linux" /boot/grub/menu.lst
```

Remediation:

For `grub` based systems edit `/boot/grub/menu.lst` to include `audit=1` on all `kernel` lines.

For `grub2` based systems edit /etc/default/grub and add audit=1 to GRUB_CMDLINE_LINUX:

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

Run the following command to update the `grub2` configuration:

```
# update-grub
```

Notes:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Replace `/boot/grub/menu.lst` with the appropriate grub configuration file for your environment.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.1.4 Ensure events that modify date and time information are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

On a 32 bit system run the following command and verify the output matches:

```
# 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
```

On a 64 bit system run the following command and verify the output matches:

```
# 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
```

Remediation:

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
```

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
```

Critical Controls:

3.6 Implement Automated Configuration Monitoring System (i.e. Configuration Assessment Tools)

Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

4.1.5 Ensure events that modify user/group information are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# 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
```

Critical Controls:

5.4 Log Administrative User Addition And Removal

Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

4.1.6 Ensure events that modify the system's network environment are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the `/etc/issue` and `/etc/issue.net` files (messages displayed pre-login), `/etc/hosts` (file containing host names and associated IP addresses) and `/etc/sysconfig/network` (directory containing network interface scripts and configurations) files.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Audit:

On a 32 bit system run the following command and verify the output matches:

```
# grep system-locale /etc/audit/audit.rules
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

On a 64 bit system run the following command and verify the output matches:

```
# grep system-locale /etc/audit/audit.rules
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

Remediation:

For 32 bit systems add the following lines to the `/etc/audit/audit.rules` file:

```
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

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

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

Notes:

`/etc/sysconfig/network` is common to Red Hat and SUSE based distributions. You should expand or replace this coverage to any network configuration files on your system such as `/etc/network` on Debian based distributions.

Critical Controls:

3.6 Implement Automated Configuration Monitoring System (i.e. Configuration Assessment Tools)
Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor SELinux/AppArmor 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 or /etc/apparmor and /etc/apparmor.d directories.

Rationale:

Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit:

On systems using SELinux run the following command and verify output matches:

```
# grep MAC-policy /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
```

On systems using AppArmor run the following command and verify output matches:

```
# grep MAC-policy /etc/audit/audit.rules
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Remediation:

On systems using SELinux add the following line to the `/etc/audit/audit.rules` file:

```
-w /etc/selinux/ -p wa -k MAC-policy
```

On systems using AppArmor add the following line to the `/etc/audit/audit.rules` file:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Critical Controls:

3.6 Implement Automated Configuration Monitoring System (i.e. Configuration Assessment Tools)

Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

4.1.8 Ensure login and logout events are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# 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
```

Critical Controls:

5.5 Log Failed Administrative Login Attempts
Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

16.10 Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during

unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

16.4 Automatically Log Off Users After Standard Period Of Inactivity

Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

4.1.9 Ensure session initiation information is collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# 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
```

Notes:

The `last` command can be used to read `/var/log/wtmp` (`last` with no parameters) and `/var/run/utmp` (`last -f /var/run/utmp`)

Critical Controls:

5.5 Log Failed Administrative Login Attempts
Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

16.10 Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

4.1.10 Ensure discretionary access control permission modification events are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 user ids (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:

On a 32 bit system run the following command and verify the output matches:

```
# 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
```

On a 64 bit system run the following command and verify the output matches:

```
# 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
```

Remediation:

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
```

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
```

Critical Controls:

3.6 Implement Automated Configuration Monitoring System (i.e. Configuration Assessment Tools)

Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 a 32 bit system run the following command and verify the output matches:

```
# 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
```

On a 64 bit system run the following command and verify the output matches:

```
# 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
```

Remediation:

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
```

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
```

Critical Controls:

14.6 Enforce Detailed Audit Logging For Sensitive Information
Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

14.6 Enforce Detailed Audit Logging For Sensitive Information
Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

4.1.12 Ensure use of privileged commands is collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing with a list of partitions where programs can be executed from on your system:

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

Verify all resulting lines are in the `/etc/audit/audit.rules` file.

Remediation:

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows: `-F path=" $1 "` - will populate each file name found through the find command and processed by awk. `-F perm=x` - will write an audit record if the file is executed. `-F auid>=500` - will write a record if the user executing the command is not a privileged user. `-F auid!= 4294967295` - will ignore Daemon events

All audit records should be tagged with the identifier "privileged".

Run the following command replacing with a list of partitions where programs can be executed from on your system:

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

```
-k privileged" }'
```

Add all resulting lines to the `/etc/audit/audit.rules` file.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

4.1.13 Ensure successful file system mounts are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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.

Audit:

On a 32 bit system run the following command and verify the output matches:

```
# grep mounts /etc/audit/audit.rules
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

On a 64 bit system run the following command and verify the output matches:

```
# 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
```

Remediation:

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
```

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
```

Notes:

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).

Critical Controls:

13 Data Protection
Data Protection

4.1.14 Ensure file deletion events by users are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

On a 32 bit system run the following command and verify the output matches:

```
# 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
```

On a 64 bit system run the following command and verify the output matches:

```
# 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
```

Remediation:

For 32 bit systems add the following lines 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
```

For 64 bit systems add the following lines 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
```

Notes:

At a minimum, configure the audit system to collect file deletion events for all users and root.

4.1.15 Ensure changes to system administration scope (sudoers) is collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# grep scope /etc/audit/audit.rules
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Remediation:

Add the following line to the `/etc/audit/audit.rules` file:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

Critical Controls:

5.4 Log Administrative User Addition And Removal
Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

4.1.16 Ensure system administrator actions (sudolog) are collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# 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
```

Notes:

The system must be configured with `su`disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through `sudo`. This will not be effective on the console, as administrators can log in as root.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.5 Log Failed Administrative Login Attempts
Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

4.1.17 Ensure kernel module loading and unloading is collected (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

On a 32 bit system run the following command and verify the output matches:

```
# grep modules /etc/audit/audit.rules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit arch=b32 -S init_module -S delete_module -k modules
```

On a 64 bit system run the following command and verify the output matches:

```
# grep modules /etc/audit/audit.rules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit arch=b64 -S init_module -S delete_module -k modules
```

Remediation:

For 32 bit systems add the following lines to the `/etc/audit/audit.rules` file:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit arch=b32 -S init_module -S delete_module -k modules
```

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

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit arch=b64 -S init_module -S delete_module -k modules
```

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4.1.18 Ensure the audit configuration is immutable (Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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:

Run the following command and verify output matches:

```
# grep "^\s*[^#]" /etc/audit/audit.rules | tail -1
-e 2
```

Remediation:

Add the following line to the end of the `/etc/audit/audit.rules` file.

```
-e 2
```

Critical Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

4.2 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise and ease log analysis.

4.2.1 Configure rsyslog

The `rsyslog` software is recommended as a replacement for the`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. **Note:** This section only applies if `rsyslog` is installed on the system.

4.2.1.1 Ensure rsyslog Service is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

If the `rsyslog` service is not activated the system may default to the `syslogd` service or lack logging instead.

Audit:

Run one of the following commands to verify `rsyslog` is enabled:

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

Verify runlevels 2 through 5 are "on".

```
# systemctl is-enabled rsyslog
enabled
```

Verify result is "enabled".

```
# ls /etc/rc*.d | grep rsyslog
```

Verify S* lines are returned for runlevels 2 through 5.

Remediation:

Run one of the following commands to enable `rsyslog` :

```
# chkconfig rsyslog on
# systemctl enable rsyslog
# update-rc.d rsyslog enable
```

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

Some distributions may configure syslog daemon selection via a setting in a configuration file such as `/etc/sysconfig/syslog` and a centralized init script.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.2.1.2 Ensure logging is configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/rsyslog.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the `/etc/rsyslog.conf` file to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the following lines in the `/etc/rsyslog.conf` file as appropriate for your environment:

```
*.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
```

Run the following command to restart `rsyslogd`:

```
# pkill -HUP rsyslogd
```

References:

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

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.2.1.3 Ensure rsyslog default file permissions configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that `$FileCreateMode` is `0640` or more restrictive:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf
```

Remediation:

Edit the /etc/rsyslog.conf and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

References:

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

Notes:

You should also ensure this is not overridden with less restrictive settings in any `/etc/rsyslog.d/*` conf file.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 `loghost.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 `loghost.example.com` is the name of your central log host).

```
*.* @@loghost.example.com
```

Run the following command to restart `rsyslog` :

```
# pkill -HUP rsyslogd
```

References:

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

Notes:

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.

Critical Controls:

6.6 Deploy A SIEM OR Log Analysis Tools For Aggregation And Correlation/Analysis
Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

By default, `rsyslog` does not listen for log messages coming in from remote systems. The `ModLoad` tells `rsyslog` to load the `imtcp.so` module so it can listen over a network via TCP. The `InputTCPServerRun` option instructs `rsyslogd` to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `rsyslog` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `rsyslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Run the following commands and verify the resulting lines are uncommented on designated log hosts and commented or removed on all others:

```
# 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 or add the following lines:

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

For hosts that are not designated as log hosts, edit the `/etc/rsyslog.conf` file and comment or remove the following lines:

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

Run the following command to restart `rsyslogd` :

```
# pkill -HUP rsyslogd
```

References:

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

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

4.2.2 Configure syslog-ng

The `syslog-ng` software is recommended as a replacement for the`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. **Note:** This section only applies if `syslog-ng` is installed on the system.

4.2.2.1 Ensure syslog-ng service is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Once the `syslog-ng` package is installed it needs to be activated.

Rationale:

If the `syslog-ng` service is not activated the system may default to the `syslogd` service or lack logging instead.

Audit:

Run one of the following commands to verify `syslog-ng` is enabled:

```
# chkconfig --list syslog-ng
syslog-ng                0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

Verify runlevels 2 through 5 are "on".

```
# systemctl is-enabled syslog-ng
enabled
```

Verify result is "enabled".

```
# ls /etc/rc*.d | grep syslog-ng
```

Verify S* lines are returned for runlevels 2 through 5.

Remediation:

Run one of the following commands to enable `syslog-ng` :

```
# chkconfig syslog-ng on
# systemctl enable syslog-ng
```

```
# update-rc.d autofs syslog-ng
```

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

Some distributions may configure syslog daemon selection via a setting in a configuration file such as `/etc/sysconfig/syslog` and a centralized init script.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.2.2.2 Ensure logging is configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/syslog-ng/syslog-ng.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `syslog-ng` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the `/etc/syslog-ng/syslog-ng.conf` file to ensure appropriate logging is set. In addition, run the following command and ensure that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the log lines in the `/etc/syslog-ng/syslog-ng.conf` file as appropriate for your environment:

```
log { source(src); source(chroots); filter(f_console); destination(console);
};
log { source(src); source(chroots); filter(f_console); destination(xconsole);
};
log { source(src); source(chroots); filter(f_newscrit);
destination(newscrit); };
log { source(src); source(chroots); filter(f_newserr); destination(newserr);
};
log { source(src); source(chroots); filter(f_newsnotice);
destination(newsnotice); };
log { source(src); source(chroots); filter(f_mailinfo);
destination(mailinfo); };
log { source(src); source(chroots); filter(f_mailwarn);
destination(mailwarn); };
log { source(src); source(chroots); filter(f_mailerr);  destination(mailerr);
};
log { source(src); source(chroots); filter(f_mail); destination(mail); };
```

```
log { source(src); source(chroots); filter(f_acpid); destination(acpid);
flags(final); };
log { source(src); source(chroots); filter(f_acpid_full);
destination(devnull); flags(final); };
log { source(src); source(chroots); filter(f_acpid_old); destination(acpid);
flags(final); };
log { source(src); source(chroots); filter(f_netmgm); destination(netmgm);
flags(final); };
log { source(src); source(chroots); filter(f_local);
destination(localmessages); };
log { source(src); source(chroots); filter(f_messages);
destination(messages); };
log { source(src); source(chroots); filter(f_iptables);
destination(firewall); };
log { source(src); source(chroots); filter(f_warn); destination(warn); };
```

Run the following command to restart syslog-ng:

```
# pkill -HUP syslog-ng
```

References:

1. See the syslog-ng man page for more information.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting

Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.2.2.3 Ensure syslog-ng default file permissions configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

syslog-ng will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `syslog-ng` data is archived and protected.

Audit:

Run the following command and verify the `perm` option is `0640` or more restrictive:

```
# grep ^options /etc/syslog-ng/syslog-ng.conf
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600);
threaded(yes); };
```

Remediation:

Edit the `/etc/syslog-ng/syslog-ng.conf` and set `perm` option to `0640` or more restrictive:

```
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600);
threaded(yes); };
```

References:

1. See the syslog-ng man pages for more information.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

4.2.2.4 Ensure syslog-ng is configured to send logs to a remote log host (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `syslog-ng` utility supports the ability to send logs it gathers to a remote log host or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Audit:

Review the `/etc/syslog-ng/syslog-ng.conf` file and verify that logs are sent to a central host (where `logfile.example.com` is the name of your central log host):

```
destination logserver { tcp("logfile.example.com" port(514)); };
log { source(src); destination(logserver); };
```

Remediation:

Edit the `/etc/syslog-ng/syslog-ng.conf` file and add the following lines (where `logfile.example.com` is the name of your central log host).

```
destination logserver { tcp("logfile.example.com" port(514)); };
log { source(src); destination(logserver); };
```

Run the following command to restart syslog-ng:

```
# pkill -HUP syslog-ng
```

References:

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

Critical Controls:

6.6 Deploy A SIEM OR Log Analysis Tools For Aggregation And Correlation/Analysis

Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

4.2.2.5 Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

By default, `syslog-ng` does not listen for log messages coming in from remote systems.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `syslog-ng` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `syslog-ng` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Review the /etc/syslog-ng/syslog-ng.conf file and verify the following lines are configured appropriately on designated log hosts:

```
source net{ tcp(); };
destination remote { file("/var/log/remote/${FULLHOST}-log"); };
log { source(net); destination(remote); };
```

Remediation:

On designated log hosts edit the `/etc/syslog-ng/syslog-ng.conf` file and configure the following lines are appropriately:

```
source net{ tcp(); };
destination remote { file("/var/log/remote/${FULLHOST}-log"); };
log { source(net); destination(remote); };
```

On non designated log hosts edit the `/etc/syslog-ng/syslog-ng.conf` file and remove or edit any sources that accept network sourced log messages.

Run the following command to restart `syslog-ng` :

```
# pkill -HUP syslog-ng
```

References:

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

Critical Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

4.2.3 Ensure rsyslog or syslog-ng is installed (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` and `syslog-ng` software are recommended replacements to the original `syslogd` daemon which provide 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.

Rationale:

The security enhancements of `rsyslog` and `syslog-ng` 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:

Verify either rsyslog or syslog-ng is installed. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q rsyslog
# rpm -q syslog-ng
# dpkg -s rsyslog
# dpkg -s syslog-ng
```

Remediation:

Install rsyslog or `syslog-ng` using the appropriate package manager or manual installation:

```
# yum install rsyslog
# apt-get install rsyslog
# zypper install rsyslog
```

The previous commands install `rsyslog` , use the appropriate package if `syslog-ng` is desired.

Critical Controls:

6.2 Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and

various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

4.2.4 Ensure permissions on all logfiles are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log -type f -ls
```

Remediation:

Run the following command to set permissions on all existing log files:

```
# chmod -R g-wx,o-rwx /var/log/*
```

Notes:

You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

4.3 Ensure logrotate is configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageable large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`.

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 `/etc/logrotate.conf` and `/etc/logrotate.d/` * and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/` * to ensure logs are rotated according to site policy.

Critical Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

5 Access, Authentication and Authorization

5.1 Configure cron

5.1.1 Ensure cron daemon is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Based on your system configuration, run the appropriate one of the following commands to verify `cron` is enabled:

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

Verify runlevels 2 through 5 are "on".

```
# systemctl is-enabled crond
enabled
```

Verify result is "enabled".

```
# ls /etc/rc*.d | grep crond
```

Verify S* lines are returned for runlevels 2 through 5.

Remediation:

Based on your system configuration, run the appropriate one of the following commands to enable `cron` :

```
# chkconfig crond on
# systemctl enable crond
# update-rc.d crond enable
```

Notes:

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

Critical Controls:

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

5.1.2 Ensure permissions on /etc/crontab are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/crontab
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.3 Ensure permissions on /etc/cron.hourly are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.hourly
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.hourly` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.4 Ensure permissions on /etc/cron.daily are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.daily
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.daily` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.5 Ensure permissions on /etc/cron.weekly are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.weekly
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.weekly` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.6 Ensure permissions on /etc/cron.monthly are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.monthly
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.monthly` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.7 Ensure permissions on /etc/cron.d are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.d
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.d` :

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

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.1.8 Ensure at/cron is restricted to authorized users (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and ensure `/etc/cron.deny` and `/etc/at.deny` do not exist:

```
# stat /etc/cron.deny
stat: cannot stat `/etc/cron.deny': No such file or directory
# stat /etc/at.deny
stat: cannot stat` /etc/at.deny': No such file or directory
```

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` for both `/etc/cron.allow` and `/etc/at.allow` :

```
# stat /etc/cron.allow
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
# stat /etc/at.allow
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to remove `/etc/cron.deny` and `/etc/at.deny` and create and set permissions and ownership for `/etc/cron.allow` and `/etc/at.allow` :

```
# rm /etc/cron.deny
# 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
```

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.2 SSH Server Configuration

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. 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.

Note: The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is not required the SSH daemon can be removed and this section skipped.

Note: Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:

```
# service sshd reload
```

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd` . The command below sets the owner and group of the file to root.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/ssh/sshd_config
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config` :

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.2.2 Ensure SSH Protocol is set to 2 (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output matches:

```
# grep "^Protocol" /etc/ssh/sshd_config
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

5.2.3 Ensure SSH LogLevel is set to INFO (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `INFO` parameter specifies that 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:

Run the following command and verify that output matches:

```
# grep "^LogLevel" /etc/ssh/sshd_config
LogLevel INFO
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel INFO
```

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.2.4 Ensure SSH X11 forwarding is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output matches:

```
# grep "^X11Forwarding" /etc/ssh/sshd_config
X11Forwarding no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

5.2.5 Ensure SSH MaxAuthTries is set to 4 or less (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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, set the number based on site policy.

Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# grep "^MaxAuthTries" /etc/ssh/sshd_config
MaxAuthTries 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.2.6 Ensure SSH IgnoreRhosts is enabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output matches:

```
# grep "^IgnoreRhosts" /etc/ssh/sshd_config
IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Critical Controls:

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

5.2.7 Ensure SSH HostbasedAuthentication is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output matches:

```
# grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Critical Controls:

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

5.2.8 Ensure SSH root login is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 system 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:

Run the following command and verify that output matches:

```
# grep "^PermitRootLogin" /etc/ssh/sshd_config
PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Critical Controls:

5.8 Administrators Should Not Directly Log In To A System (i.e. use RunAs/sudo)
Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitEmptyPasswords` parameter specifies if the SSH 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:

Run the following command and verify that output matches:

```
# grep "^PermitEmptyPasswords" /etc/ssh/sshd_config
PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.2.10 Ensure SSH PermitUserEnvironment is disabled (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output matches:

```
# grep PermitUserEnvironment /etc/ssh/sshd_config
PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.2.11 Ensure only approved ciphers are used (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command and verify that output does not contain any cipher block chaining (-cbc) algorithms:

```
# grep "Ciphers" /etc/ssh/sshd_config
Ciphers aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,chacha20-poly1305@openssh.com
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

References:

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

Notes:

Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

5.2.12 Ensure only approved MAC algorithms are used (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Audit:

Run the following command and verify that output does not contain any unlisted MAC algorithms:

```
# grep "MACs" /etc/ssh/sshd_config
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com,curve25519-
sha256@libssh.org,diffie-hellman-group-exchange-sha256
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com,curve25519-
sha256@libssh.org,diffie-hellman-group-exchange-sha256
```

References:

1. More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH

Notes:

Some organizations may have stricter requirements for approved ciphers. Ensure that MACs used are in compliance with site policy.

Critical Controls:

3.4 Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

5.2.13 Ensure SSH Idle Timeout Interval is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify `ClientAliveInterval` is 300 or less and `ClientAliveCountMax` is 3 or less:

```
# grep "^ClientAliveInterval" /etc/ssh/sshd_config
ClientAliveInterval 300
# grep "^ClientAliveCountMax" /etc/ssh/sshd_config
ClientAliveCountMax 0
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters as follows:

```
ClientAliveInterval 300
```

```
ClientAliveCountMax 0
```

Critical Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

5.2.14 Ensure SSH LoginGraceTime is set to one minute or less (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `LoginGraceTime` parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the `LoginGraceTime` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Audit:

Run the following command and verify that output `LoginGraceTime` is 60 or less:

```
# grep "^LoginGraceTime" /etc/ssh/sshd_config
LoginGraceTime 60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

5.2.15 Ensure SSH access is limited (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 user IDs 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 group names. Numeric group IDs 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 user IDs 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 group IDs 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:

Run the following commands and verify that output matches for at least one:

```
# 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>
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.8 Administrators Should Not Directly Log In To A System (i.e. use RunAs/sudo)
Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

5.2.16 Ensure SSH warning banner is configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Audit:

Run the following command and verify that output matches:

```
# grep "^Banner" /etc/ssh/sshd_config
Banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

5.3 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

5.3.1 Ensure password creation requirements are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_cracklib.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the `pam_cracklib.so` options.

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 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 pam_pwquality.so module functions similarly but the `minlen`, `dcredit`, `ucredit`, `ocredit`, and `lcredit` parameters are stored in the `/etc/security/pwquality.conf` file.

The settings shown above are 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:

Verify password creation requirements are as listed or stricter. This setting is commonly configured with the `pam_cracklib.so` or `pam_pwquality.so` options found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` . Examples:

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

If `pam_pwquality.so` is in use also verify settings in `/etc/security/pwquality.conf` :

```
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

Remediation:

Set password creation requirements to conform to site policy. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_cracklib.so` or `pam_pwquality.so` lines to include the required option:

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

If `pam_pwquality.so` is in use also configure settings in `/etc/security/pwquality.conf` :

```
minlen=14
dcredit=-1
ucredit=-1
ocredit=-1
lcredit=-1
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

Critical Controls:

5.7 User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

16.12 Use Long Passwords For All User Accounts

Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

5.3.2 Ensure lockout for failed password attempts is configured (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Lock out users after *n* unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. 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 user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Verify password lockouts are configured. These settings are commonly configured with the `pam_tally2.so` and `pam_failock.so` modules found in `/etc/pam.d/common-auth` or `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`. Examples:

```
auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth sufficient pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
```

The `pam_faillock.so` lines should surround a `pam_unix.so` line as listed here.

Remediation:

Set password lockouts to conform to site policy. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_tally2.so` or `pam_faillock.so` lines as appropriate:

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

```
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth sufficient pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` or `pam_faillock.so` module, the user can be unlocked by issuing the command `pam_tally2 -u <username> --reset` or `faillock -u --reset` respectively. This command sets the failed count to 0, effectively unlocking the user.

Critical Controls:

16.7 Configure Account Lockouts
Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.

5.3.3 Ensure password reuse is limited (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Verify remembered password history is `5` or more. This setting is commonly configured with the `pam_unix.so` or `pam_pwhistory.so remember` options found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` . Examples:

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

Remediation:

Set remembered password history to conform to site policy. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_pwhistory.so` or `pam_unix.so` lines to include the `remember` option:

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

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

Critical Controls:

16 Account Monitoring and Control

Account Monitoring and Control

5.3.4 Ensure password hashing algorithm is SHA-512 (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

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

Audit:

Verify password hashing algorithm is sha512. This setting is commonly configured with the `pam_unix.so sha512` option found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` . Example:

```
password sufficient pam_unix.so sha512
```

Remediation:

Set password hashing algorithm to sha512. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_unix.so` lines to include the sha512 option:

```
password sufficient pam_unix.so sha512
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# cat /etc/passwd | awk -F: '( $3 >= 500 && $1 != "nfsnobody" ) { print $1 }'
| xargs -n 1 chage -d 0
```

This command assumes a system UID split at 500. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

5.4 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.4.1 Set Shadow Password Suite Parameters

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 user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

5.4.1.1 Ensure password expiration is 90 days or less (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 90 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following command and verify `PASS_MAX_DAYS` is 90 or less:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 90
```

Verify all users with a password have their maximum days between password change set to 90 or less:

```
# egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<list of users>
# 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 user parameters for all users with a password set to match:

```
# chage --maxdays 90 <user>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 5th field should be 90 or less for all users with a password.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.4.1.2 Ensure minimum days between password changes is 7 or more (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following command and verify `PASS_MIN_DAYS` is 7 or more:

```
# grep PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 7
```

Verify all users with a password have their minimum days between password change set to 7 or more:

```
# egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<list of users>
# 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 user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 5th field should be 7 or more for all users with a password.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.4.1.3 Ensure password expiration warning days is 7 or more (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following command and verify `PASS_WARN_AGE` is 7 or more:

```
# grep PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

```
# egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<list of users>
# 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 user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 6th field should be 7 or more for all users with a password.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.4.1.4 Ensure inactive password lock is 30 days or less (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 30 days after password expiration 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:

Run the following command and verify `INACTIVE` is 30 or less:

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

Verify all users with a password have Password inactive no more than 30 days after password expires:

```
# egrep ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1
<list of users>
# chage --list <user>
Password inactive                                       : <date>
```

Remediation:

Notes:

You can also check this setting in `/etc/shadow` directly. The 7th field should be 30 or less for all users with a password.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.4.2 Ensure system accounts are non-login (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

There are a number of accounts provided with most distributions 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 prevented from being used to provide an interactive shell. By default, most distributions 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 `/sbin/nologin`. This prevents the account from potentially being used to run any commands.

Audit:

Run the following script and verify no results are returned:

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

Remediation:

Set the shell for any accounts returned by the audit script to `/sbin/nologin`:

```
# usermod -s /sbin/nologin <user>
```

The following script will automatically set all user shells required to `/sbin/nologin` and lock the `sync`, `shutdown`, and `halt` users:

```
#!/bin/bash

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

Notes:

The above scripts assume all UID's below 500 are system accounts. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you. Additionally the `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

5.4.3 Ensure default group for the root account is GID 0 (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the `root` account helps prevent `root` -owned files from accidentally becoming accessible to non-privileged users.

Audit:

Run the following command and verify the result is `0` :

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

Remediation:

Run the following command to set the `root` user default group to GID `0` :

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

Critical Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

5.4.4 Ensure default user umask is 027 or more restrictive (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

Audit:

Run the following commands and verify all umask lines returned are 027 or more restrictive.

```
# grep "^umask" /etc/bashrc
umask 027
# grep "^umask" /etc/profile
umask 027
```

Remediation:

Edit the `/etc/bashrc` and `/etc/profile` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
umask 027
```

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

Critical Controls:

13 Data Protection
Data Protection

5.5 Ensure root login is restricted to system console (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

5.6 Ensure access to the su command is restricted (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in the wheel group to execute `su`.

Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following command and verify output includes matching line:

```
# grep pam_wheel.so /etc/pam.d/su
auth required pam_wheel.so use_uid
```

Run the following command and verify users in `wheel` group match site policy:

```
# 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
```

Create a comma separated list of users in the wheel statement in the `/etc/group` file:

```
wheel:x:10:root,<user list>
```

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Audit system file permissions (Not Scored)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The RPM and Debian package managers have a number of useful options. One of these, the `--verify` (or `-V` for RPM) option, can be used to verify that system packages are correctly installed. The `--verify` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

```
Code   Meaning
S      File size differs.
M      File mode differs (includes permissions and file type).
5      The MD5 checksum differs.
D      The major and minor version numbers differ on a device file.
L      A mismatch occurs in a link.
U      The file ownership differs.
G      The file group owner differs.
T      The file time (mtime) differs.
```

The `rpm -qf` or `dpkg -S` command can be used to determine which package a particular file belongs to. For example the following commands determines which package the `/bin/bash` file belongs to:

```
# rpm -qf /bin/bash
bash-4.1.2-29.el6.x86_64
# dpkg -S /bin/bash
bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V bash-4.1.2-29.el6.x86_64
.M.......    /bin/bash
# dpkg --verify bash
??5?????? c /etc/bash.bashrc
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`
.M...... c /etc/passwd
S.5....T c /etc/printcap
```

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Audit:

Run one of the following commands to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename>
# dpkg --verify > <filename>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

References:

1. http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html

Notes:

Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.

Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.1.2 Ensure permissions on /etc/passwd are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/passwd
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd` :

```
# chown root:root /etc/passwd
# chmod 644 /etc/passwd
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.3 Ensure permissions on /etc/shadow are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow`, and `Access` is `640` or more restrictive:

```
# stat /etc/shadow
Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/shadow` :

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

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

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.4 Ensure permissions on /etc/group are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/group
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/group` :

```
# chown root:root /etc/group
# chmod 644 /etc/group
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.5 Ensure permissions on /etc/gshadow are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

Audit:

Run the following command and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow`, and `Access` is `640` or more restrictive:

```
# stat /etc/gshadow
Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/gshadow` :

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

# chmod o-rwx,g-rw /etc/gshadow
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.6 Ensure permissions on /etc/passwd- are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd-` file contains backup user account information.

Rationale:

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

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `600` or more restrictive:

```
# stat /etc/passwd-
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd-` :

```
# chown root:root /etc/passwd-
# chmod 600 /etc/passwd-
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.7 Ensure permissions on /etc/shadow- are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

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

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `600` or more restrictive:

```
# stat /etc/shadow-
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/shadow-` :

```
# chown root:root /etc/shadow-
# chmod 600 /etc/shadow-
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.8 Ensure permissions on /etc/group- are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

Rationale:

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

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `600` or more restrictive:

```
# stat /etc/group-
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/group-` :

```
# chown root:root /etc/group-
# chmod 600 /etc/group-
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.9 Ensure permissions on /etc/gshadow- are configured (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

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

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `600` or more restrictive:

```
# stat /etc/gshadow-
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/gshadow-` :

```
# chown root:root /etc/gshadow-
# chmod 600 /etc/gshadow-
```

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.1.10 Ensure no world writable files exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

Run the following command and verify no files are returned:

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

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -0002
```

Remediation:

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

Critical Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

6.1.11 Ensure no unowned files or directories exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

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

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nouser
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Critical Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

6.1.12 Ensure no ungrouped files or directories exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

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

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nogroup
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Critical Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

6.1.13 Audit SUID executables (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

Run the following command to list SUID files:

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

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation:

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6.1.14 Audit SGID executables (Not Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following command to list SGID files:

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

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -2000
```

Remediation:

Ensure that no rogue SGID 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.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are

required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6.2 User and Group Settings

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

6.2.1 Ensure password fields are not empty (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

```
# cat /etc/shadow | 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:

```
# 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.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

```
# grep '^+:' /etc/passwd
```

Remediation:

Remove any legacy '+' entries from `/etc/passwd` if they exist.

Critical Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

```
# grep '^+:' /etc/shadow
```

Remediation:

Remove any legacy '+' entries from `/etc/shadow` if they exist.

Critical Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

```
# grep '^+:' /etc/group
```

Remediation:

Remove any legacy '+' entries from `/etc/group` if they exist.

Critical Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

6.2.5 Ensure root is the only UID 0 account (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 5.6 Ensure access to the su command is restricted.

Audit:

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

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

Remediation:

Remove any users other than `root` with UID `0` or assign them a new UID if appropriate.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6.2.6 Ensure root PATH Integrity (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in `root` 's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
if [ "`echo $PATH | grep ::`" != "" ]; then
    echo "Empty Directory in PATH (::)"
fi

if [ "`echo $PATH | grep :$`"  != "" ]; 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.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6.2.7 Ensure all users' home directories exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following script and verify no results are returned:

```
#!/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.

Notes:

The audit script checks all users UID 500 and above except nfsnobody. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

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

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2.9 Ensure users own their home directories (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

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.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2.10 Ensure users' dot files are not group or world writable (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for dir in `cat /etc/passwd | egrep -v '(root|sync|halt|shutdown)' | 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=`ls -ld $file | cut -f1 -d" "`

      if [ `echo $fileperm | cut -c6`  != "-" ]; then
        echo "Group Write permission set on file $file"
      fi
      if [ `echo $fileperm | cut -c9`  != "-" ]; then
        echo "Other Write permission set on file $file"
      fi
    fi
  done
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.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2.11 Ensure no users have .forward files (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for dir in `cat /etc/passwd |\
  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.

Critical Controls:

7 Email and Web Browser Protections
Email and Web Browser Protections

6.2.12 Ensure no users have .netrc files (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for dir in `cat /etc/passwd |\
  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.

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.2.13 Ensure users' .netrc Files are not group or world accessible (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

`.netrc`files may contain unencrypted passwords that may be used to attack other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

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

Notes:

While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

Critical Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

6.2.14 Ensure no users have .rhosts files (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following script and verify no results are returned:

```
#!/bin/bash

for dir in `cat /etc/passwd | egrep -v '(root|halt|sync|shutdown)' | 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:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.rhosts` files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

Critical Controls:

16.14 Encrypt/Hash All Authentication Files And Monitor Their Access

Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group`.

Rationale:

Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
  grep -q -P "^.*?:[^:]*:$i:" /etc/group
  if [ $? -ne 0 ]; then
    echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
  fi
done
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.16 Ensure no duplicate UIDs exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cat /etc/passwd | cut -f3 -d":" | sort -n | uniq -c | while read x ; do
  [ -z "${x}" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    users=`awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs`
    echo "Duplicate UID ($2): ${users}"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.17 Ensure no duplicate GIDs exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

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

Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Notes:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.18 Ensure no duplicate user names exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cat /etc/passwd | cut -f1 -d":" | sort -n | uniq -c | while read x ; do
  [ -z "${x}" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    uids=`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 audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.19 Ensure no duplicate group names exist (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group` . Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cat /etc/group | cut -f1 -d":" | sort -n | uniq -c | while read x ; do
  [ -z "${x}" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    gids=`gawk -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 audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

Critical Controls:

16 Account Monitoring and Control
Account Monitoring and Control

6.2.20 Ensure shadow group is empty (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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:

Run the following commands and verify no results are returned:

```
# grep ^shadow /etc/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.

Critical Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Initial Setup**		
1.1	**Filesystem Configuration**		
1.1.1	**Disable unused filesystems**		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Scored)	☐	☐
1.1.1.2	Ensure mounting of freevxfs filesystems is disabled (Scored)	☐	☐
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Scored)	☐	☐
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Scored)	☐	☐
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Scored)	☐	☐
1.1.1.6	Ensure mounting of squashfs filesystems is disabled (Scored)	☐	☐
1.1.1.7	Ensure mounting of udf filesystems is disabled (Scored)	☐	☐
1.1.1.8	Ensure mounting of FAT filesystems is disabled (Scored)	☐	☐
1.1.2	Ensure separate partition exists for /tmp (Scored)	☐	☐
1.1.3	Ensure nodev option set on /tmp partition (Scored)	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition (Scored)	☐	☐
1.1.5	Ensure noexec option set on /tmp partition (Scored)	☐	☐
1.1.6	Ensure separate partition exists for /var (Scored)	☐	☐
1.1.7	Ensure separate partition exists for /var/tmp (Scored)	☐	☐
1.1.8	Ensure nodev option set on /var/tmp partition (Scored)	☐	☐
1.1.9	Ensure nosuid option set on /var/tmp partition (Scored)	☐	☐
1.1.10	Ensure noexec option set on /var/tmp partition (Scored)	☐	☐
1.1.11	Ensure separate partition exists for /var/log (Scored)	☐	☐
1.1.12	Ensure separate partition exists for /var/log/audit (Scored)	☐	☐
1.1.13	Ensure separate partition exists for /home (Scored)	☐	☐
1.1.14	Ensure nodev option set on /home partition (Scored)	☐	☐
1.1.15	Ensure nodev option set on /dev/shm partition (Scored)	☐	☐
1.1.16	Ensure nosuid option set on /dev/shm partition (Scored)	☐	☐
1.1.17	Ensure noexec option set on /dev/shm partition (Scored)	☐	☐
1.1.18	Ensure nodev option set on removable media partitions (Not Scored)	☐	☐
1.1.19	Ensure nosuid option set on removable media partitions (Not Scored)	☐	☐
1.1.20	Ensure noexec option set on removable media partitions (Not Scored)	☐	☐
1.1.21	Ensure sticky bit is set on all world-writable directories (Scored)	☐	☐
1.1.22	Disable Automounting (Scored)	☐	☐
1.2	**Configure Software Updates**		

1.2.1	Ensure package manager repositories are configured (Not Scored)	☐	☐
1.2.2	Ensure GPG keys are configured (Not Scored)	☐	☐
1.3	**Filesystem Integrity Checking**		
1.3.1	Ensure AIDE is installed (Scored)	☐	☐
1.3.2	Ensure filesystem integrity is regularly checked (Scored)	☐	☐
1.4	**Secure Boot Settings**		
1.4.1	Ensure permissions on bootloader config are configured (Scored)	☐	☐
1.4.2	Ensure bootloader password is set (Scored)	☐	☐
1.4.3	Ensure authentication required for single user mode (Not Scored)	☐	☐
1.4.4	Ensure interactive boot is not enabled (Not Scored)	☐	☐
1.5	**Additional Process Hardening**		
1.5.1	Ensure core dumps are restricted (Scored)	☐	☐
1.5.2	Ensure XD/NX support is enabled (Not Scored)	☐	☐
1.5.3	Ensure address space layout randomization (ASLR) is enabled (Scored)	☐	☐
1.5.4	Ensure prelink is disabled (Scored)	☐	☐
1.6	**Mandatory Access Control**		
1.6.1	**Configure SELinux**		
1.6.1.1	Ensure SELinux is not disabled in bootloader configuration (Scored)	☐	☐
1.6.1.2	Ensure the SELinux state is enforcing (Scored)	☐	☐
1.6.1.3	Ensure SELinux policy is configured (Scored)	☐	☐
1.6.1.4	Ensure SETroubleshoot is not installed (Scored)	☐	☐
1.6.1.5	Ensure the MCS Translation Service (mcstrans) is not installed (Scored)	☐	☐
1.6.1.6	Ensure no unconfined daemons exist (Scored)	☐	☐
1.6.2	**Configure AppArmor**		
1.6.2.1	Ensure AppArmor is not disabled in bootloader configuration (Scored)	☐	☐
1.6.2.2	Ensure all AppArmor Profiles are enforcing (Scored)	☐	☐
1.6.3	Ensure SELinux or AppArmor are installed (Not Scored)	☐	☐
1.7	**Warning Banners**		
1.7.1	**Command Line Warning Banners**		
1.7.1.1	Ensure message of the day is configured properly (Scored)	☐	☐
1.7.1.2	Ensure local login warning banner is configured properly (Not Scored)	☐	☐
1.7.1.3	Ensure remote login warning banner is configured properly (Not Scored)	☐	☐
1.7.1.4	Ensure permissions on /etc/motd are configured (Not Scored)	☐	☐

1.7.1.5	Ensure permissions on /etc/issue are configured (Scored)	☐	☐
1.7.1.6	Ensure permissions on /etc/issue.net are configured (Not Scored)	☐	☐
1.7.2	Ensure GDM login banner is configured (Scored)	☐	☐
1.8	Ensure updates, patches, and additional security software are installed (Not Scored)	☐	☐
2	**Services**		
2.1	**inetd Services**		
2.1.1	Ensure chargen services are not enabled (Scored)	☐	☐
2.1.2	Ensure daytime services are not enabled (Scored)	☐	☐
2.1.3	Ensure discard services are not enabled (Scored)	☐	☐
2.1.4	Ensure echo services are not enabled (Scored)	☐	☐
2.1.5	Ensure time services are not enabled (Scored)	☐	☐
2.1.6	Ensure rsh server is not enabled (Scored)	☐	☐
2.1.7	Ensure talk server is not enabled (Scored)	☐	☐
2.1.8	Ensure telnet server is not enabled (Scored)	☐	☐
2.1.9	Ensure tftp server is not enabled (Scored)	☐	☐
2.1.10	Ensure xinetd is not enabled (Scored)	☐	☐
2.2	**Special Purpose Services**		
2.2.1	**Time Synchronization**		
2.2.1.1	Ensure time synchronization is in use (Not Scored)	☐	☐
2.2.1.2	Ensure ntp is configured (Scored)	☐	☐
2.2.1.3	Ensure chrony is configured (Scored)	☐	☐
2.2.2	Ensure X Window System is not installed (Scored)	☐	☐
2.2.3	Ensure Avahi Server is not enabled (Scored)	☐	☐
2.2.4	Ensure CUPS is not enabled (Scored)	☐	☐
2.2.5	Ensure DHCP Server is not enabled (Scored)	☐	☐
2.2.6	Ensure LDAP server is not enabled (Scored)	☐	☐
2.2.7	Ensure NFS and RPC are not enabled (Scored)	☐	☐
2.2.8	Ensure DNS Server is not enabled (Scored)	☐	☐
2.2.9	Ensure FTP Server is not enabled (Scored)	☐	☐
2.2.10	Ensure HTTP server is not enabled (Scored)	☐	☐
2.2.11	Ensure IMAP and POP3 server is not enabled (Scored)	☐	☐
2.2.12	Ensure Samba is not enabled (Scored)	☐	☐
2.2.13	Ensure HTTP Proxy Server is not enabled (Scored)	☐	☐
2.2.14	Ensure SNMP Server is not enabled (Scored)	☐	☐
2.2.15	Ensure mail transfer agent is configured for local-only mode (Scored)	☐	☐
2.2.16	Ensure rsync service is not enabled (Scored)	☐	☐
2.2.17	Ensure NIS Server is not enabled (Scored)	☐	☐
2.3	**Service Clients**		
2.3.1	Ensure NIS Client is not installed (Scored)	☐	☐
2.3.2	Ensure rsh client is not installed (Scored)	☐	☐

2.3.3	Ensure talk client is not installed (Scored)	☐	☐
2.3.4	Ensure telnet client is not installed (Scored)	☐	☐
2.3.5	Ensure LDAP client is not installed (Scored)	☐	☐
3	**Network Configuration**		
3.1	**Network Parameters (Host Only)**		
3.1.1	Ensure IP forwarding is disabled (Scored)	☐	☐
3.1.2	Ensure packet redirect sending is disabled (Scored)	☐	☐
3.2	**Network Parameters (Host and Router)**		
3.2.1	Ensure source routed packets are not accepted (Scored)	☐	☐
3.2.2	Ensure ICMP redirects are not accepted (Scored)	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted (Scored)	☐	☐
3.2.4	Ensure suspicious packets are logged (Scored)	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored (Scored)	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored (Scored)	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled (Scored)	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled (Scored)	☐	☐
3.3	**IPv6**		
3.3.1	Ensure IPv6 router advertisements are not accepted (Not Scored)	☐	☐
3.3.2	Ensure IPv6 redirects are not accepted (Not Scored)	☐	☐
3.3.3	Ensure IPv6 is disabled (Not Scored)	☐	☐
3.4	**TCP Wrappers**		
3.4.1	Ensure TCP Wrappers is installed (Scored)	☐	☐
3.4.2	Ensure /etc/hosts.allow is configured (Scored)	☐	☐
3.4.3	Ensure /etc/hosts.deny is configured (Scored)	☐	☐
3.4.4	Ensure permissions on /etc/hosts.allow are configured (Scored)	☐	☐
3.4.5	Ensure permissions on /etc/hosts.deny are 644 (Scored)	☐	☐
3.5	**Uncommon Network Protocols**		
3.5.1	Ensure DCCP is disabled (Not Scored)	☐	☐
3.5.2	Ensure SCTP is disabled (Not Scored)	☐	☐
3.5.3	Ensure RDS is disabled (Not Scored)	☐	☐
3.5.4	Ensure TIPC is disabled (Not Scored)	☐	☐
3.6	**Firewall Configuration**		
3.6.1	Ensure iptables is installed (Scored)	☐	☐
3.6.2	Ensure default deny firewall policy (Scored)	☐	☐
3.6.3	Ensure loopback traffic is configured (Scored)	☐	☐
3.6.4	Ensure outbound and established connections are configured (Not Scored)	☐	☐
3.6.5	Ensure firewall rules exist for all open ports (Scored)	☐	☐
3.7	Ensure wireless interfaces are disabled (Not Scored)	☐	☐
4	**Logging and Auditing**		
4.1	**Configure System Accounting (auditd)**		

4.1.1	**Configure Data Retention**		
4.1.1.1	Ensure audit log storage size is configured (Not Scored)	☐	☐
4.1.1.2	Ensure system is disabled when audit logs are full (Scored)	☐	☐
4.1.1.3	Ensure audit logs are not automatically deleted (Scored)	☐	☐
4.1.2	Ensure auditd service is enabled (Scored)	☐	☐
4.1.3	Ensure auditing for processes that start prior to auditd is enabled (Scored)	☐	☐
4.1.4	Ensure events that modify date and time information are collected (Scored)	☐	☐
4.1.5	Ensure events that modify user/group information are collected (Scored)	☐	☐
4.1.6	Ensure events that modify the system's network environment are collected (Scored)	☐	☐
4.1.7	Ensure events that modify the system's Mandatory Access Controls are collected (Scored)	☐	☐
4.1.8	Ensure login and logout events are collected (Scored)	☐	☐
4.1.9	Ensure session initiation information is collected (Scored)	☐	☐
4.1.10	Ensure discretionary access control permission modification events are collected (Scored)	☐	☐
4.1.11	Ensure unsuccessful unauthorized file access attempts are collected (Scored)	☐	☐
4.1.12	Ensure use of privileged commands is collected (Scored)	☐	☐
4.1.13	Ensure successful file system mounts are collected (Scored)	☐	☐
4.1.14	Ensure file deletion events by users are collected (Scored)	☐	☐
4.1.15	Ensure changes to system administration scope (sudoers) is collected (Scored)	☐	☐
4.1.16	Ensure system administrator actions (sudolog) are collected (Scored)	☐	☐
4.1.17	Ensure kernel module loading and unloading is collected (Scored)	☐	☐
4.1.18	Ensure the audit configuration is immutable (Scored)	☐	☐
4.2	**Configure Logging**		
4.2.1	**Configure rsyslog**		
4.2.1.1	Ensure rsyslog Service is enabled (Scored)	☐	☐
4.2.1.2	Ensure logging is configured (Not Scored)	☐	☐
4.2.1.3	Ensure rsyslog default file permissions configured (Scored)	☐	☐
4.2.1.4	Ensure rsyslog is configured to send logs to a remote log host (Scored)	☐	☐
4.2.1.5	Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)	☐	☐
4.2.2	**Configure syslog-ng**		
4.2.2.1	Ensure syslog-ng service is enabled (Scored)	☐	☐
4.2.2.2	Ensure logging is configured (Not Scored)	☐	☐

4.2.2.3	Ensure syslog-ng default file permissions configured (Scored)	☐	☐
4.2.2.4	Ensure syslog-ng is configured to send logs to a remote log host (Scored)	☐	☐
4.2.2.5	Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)	☐	☐
4.2.3	Ensure rsyslog or syslog-ng is installed (Scored)	☐	☐
4.2.4	Ensure permissions on all logfiles are configured (Scored)	☐	☐
4.3	Ensure logrotate is configured (Not Scored)	☐	☐
5	**Access, Authentication and Authorization**		
5.1	**Configure cron**		
5.1.1	Ensure cron daemon is enabled (Scored)	☐	☐
5.1.2	Ensure permissions on /etc/crontab are configured (Scored)	☐	☐
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Scored)	☐	☐
5.1.4	Ensure permissions on /etc/cron.daily are configured (Scored)	☐	☐
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Scored)	☐	☐
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Scored)	☐	☐
5.1.7	Ensure permissions on /etc/cron.d are configured (Scored)	☐	☐
5.1.8	Ensure at/cron is restricted to authorized users (Scored)	☐	☐
5.2	**SSH Server Configuration**		
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Scored)	☐	☐
5.2.2	Ensure SSH Protocol is set to 2 (Scored)	☐	☐
5.2.3	Ensure SSH LogLevel is set to INFO (Scored)	☐	☐
5.2.4	Ensure SSH X11 forwarding is disabled (Scored)	☐	☐
5.2.5	Ensure SSH MaxAuthTries is set to 4 or less (Scored)	☐	☐
5.2.6	Ensure SSH IgnoreRhosts is enabled (Scored)	☐	☐
5.2.7	Ensure SSH HostbasedAuthentication is disabled (Scored)	☐	☐
5.2.8	Ensure SSH root login is disabled (Scored)	☐	☐
5.2.9	Ensure SSH PermitEmptyPasswords is disabled (Scored)	☐	☐
5.2.10	Ensure SSH PermitUserEnvironment is disabled (Scored)	☐	☐
5.2.11	Ensure only approved ciphers are used (Scored)	☐	☐
5.2.12	Ensure only approved MAC algorithms are used (Scored)	☐	☐
5.2.13	Ensure SSH Idle Timeout Interval is configured (Scored)	☐	☐
5.2.14	Ensure SSH LoginGraceTime is set to one minute or less (Scored)	☐	☐
5.2.15	Ensure SSH access is limited (Scored)	☐	☐
5.2.16	Ensure SSH warning banner is configured (Scored)	☐	☐
5.3	**Configure PAM**		
5.3.1	Ensure password creation requirements are configured	☐	☐

	(Scored)		
5.3.2	Ensure lockout for failed password attempts is configured (Not Scored)	☐	☐
5.3.3	Ensure password reuse is limited (Not Scored)	☐	☐
5.3.4	Ensure password hashing algorithm is SHA-512 (Not Scored)	☐	☐
5.4	**User Accounts and Environment**		
5.4.1	**Set Shadow Password Suite Parameters**		
5.4.1.1	Ensure password expiration is 90 days or less (Scored)	☐	☐
5.4.1.2	Ensure minimum days between password changes is 7 or more (Scored)	☐	☐
5.4.1.3	Ensure password expiration warning days is 7 or more (Scored)	☐	☐
5.4.1.4	Ensure inactive password lock is 30 days or less (Scored)	☐	☐
5.4.2	Ensure system accounts are non-login (Scored)	☐	☐
5.4.3	Ensure default group for the root account is GID 0 (Scored)	☐	☐
5.4.4	Ensure default user umask is 027 or more restrictive (Scored)	☐	☐
5.5	Ensure root login is restricted to system console (Not Scored)	☐	☐
5.6	Ensure access to the su command is restricted (Scored)	☐	☐
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Audit system file permissions (Not Scored)	☐	☐
6.1.2	Ensure permissions on /etc/passwd are configured (Scored)	☐	☐
6.1.3	Ensure permissions on /etc/shadow are configured (Scored)	☐	☐
6.1.4	Ensure permissions on /etc/group are configured (Scored)	☐	☐
6.1.5	Ensure permissions on /etc/gshadow are configured (Scored)	☐	☐
6.1.6	Ensure permissions on /etc/passwd- are configured (Scored)	☐	☐
6.1.7	Ensure permissions on /etc/shadow- are configured (Scored)	☐	☐
6.1.8	Ensure permissions on /etc/group- are configured (Scored)	☐	☐
6.1.9	Ensure permissions on /etc/gshadow- are configured (Scored)	☐	☐
6.1.10	Ensure no world writable files exist (Scored)	☐	☐
6.1.11	Ensure no unowned files or directories exist (Scored)	☐	☐
6.1.12	Ensure no ungrouped files or directories exist (Scored)	☐	☐
6.1.13	Audit SUID executables (Not Scored)	☐	☐
6.1.14	Audit SGID executables (Not Scored)	☐	☐
6.2	**User and Group Settings**		
6.2.1	Ensure password fields are not empty (Scored)	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd (Scored)	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow (Scored)	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group (Scored)	☐	☐
6.2.5	Ensure root is the only UID 0 account (Scored)	☐	☐
6.2.6	Ensure root PATH Integrity (Scored)	☐	☐
6.2.7	Ensure all users' home directories exist (Scored)	☐	☐

6.2.8	Ensure users' home directories permissions are 750 or more restrictive (Scored)	☐	☐
6.2.9	Ensure users own their home directories (Scored)	☐	☐
6.2.10	Ensure users' dot files are not group or world writable (Scored)	☐	☐
6.2.11	Ensure no users have .forward files (Scored)	☐	☐
6.2.12	Ensure no users have .netrc files (Scored)	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible (Scored)	☐	☐
6.2.14	Ensure no users have .rhosts files (Scored)	☐	☐
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group (Scored)	☐	☐
6.2.16	Ensure no duplicate UIDs exist (Scored)	☐	☐
6.2.17	Ensure no duplicate GIDs exist (Scored)	☐	☐
6.2.18	Ensure no duplicate user names exist (Scored)	☐	☐
6.2.19	Ensure no duplicate group names exist (Scored)	☐	☐
6.2.20	Ensure shadow group is empty (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
04-01-2016	1.0.0	Initial Release
01-31-2017	1.0.1	Critical Controls Mapping