CIS Benchmarks

CIS Ubuntu Linux 18.04 LTS Benchmark

v2.1.0 - 03-23-2021

Terms of Use

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

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

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Ubuntu Linux 18.04 LTS systems running on x86 and x64 platforms. This guide was tested against Ubuntu Linux 18.04.5 LTS

The guidance within broadly assumes that operations are being performed as the root user. Operations performed using sudo instead of the root user may produce unexpected results, or fail to make the intended changes to the system. 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.

The guidance in this document includes changes to the running system configuration. Failure to test system configuration changes in a test environment prior to implementation on a production system could lead to loss of services.

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

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Ubuntu Linux 18.04 LTS on a x86 or x64 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://workbench.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

Assessment Status

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

Automated

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

Manual

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - 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:

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.

Contributor
Bill Erickson
Dave Billing
Dominic Pace
Elliot Anderson
Ely Pinto
Fredrik Silverskär
Joy Latten
Koen Laevens
Mark Birch
Tom Pietschmann
Vineetha Hari Pai
Anurag Pal
Bradley Hieber
Thomas Sjögren
James Trigg
Kenneth Karlsson
Richard Costa

Editor
Jonathan Lewis Christopherson
Eric Pinnell

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 (Automated)

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 | grep -E '(cramfs|install)'

install /bin/true

# lsmod | grep cramfs

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /etc/modprobe.d/cramfs.conf`
and add the following line:

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

Run the following command to unload the `cramfs` module:

```
# rmmod cramfs
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled (Automated)

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 | grep -E '(freevxfs|install)'

install /bin/true

# lsmod | grep freevxfs

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/freevxfs.conf`
and add the following line:

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

Run the following command to unload the `freevxfs` module:

```
rmmod freevxfs
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Automated)

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 | grep -E '(jffs2|install)'

install /bin/true

# lsmod | grep jffs2

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/jffs2.conf`
and add the following line:

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

Run the following command to unload the `jffs2` module:

```
# rmmod jffs2
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.4 Ensure mounting of hfs filesystems is disabled (Automated)

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 | grep -E '(hfs|install)'

install /bin/true

# lsmod | grep hfs

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/hfs.conf`
and add the following line:

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

Run the following command to unload the `hfs` module:

```
# rmmod hfs
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Automated)

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 | grep -E '(hfsplus|install)'

install /bin/true

# lsmod | grep hfsplus

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/hfsplus.conf`
and add the following line:

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

Run the following command to unload the `hfsplus` module:

```
# rmmod hfsplus
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.6 Ensure mounting of udf filesystems is disabled (Automated)

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 | grep -E '(udf|install)'

install /bin/true

# lsmod | grep udf

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/udf.conf`
and add the following line:

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

Run the following command to unload the `udf` module:

```
# rmmod udf
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2 Ensure /tmp is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

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.

This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Impact:

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.

Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily.

/tmp utilizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Audit:

Run the following command and verify output shows `/tmp` is mounted to tmpfs or a system partition:

```
# findmnt /tmp

TARGET SOURCE FSTYPE OPTIONS
/tmp   tmpfs  tmpfs  rw,nosuid,nodev,noexec
```

Remediation:

Configure `/etc/fstab` as appropriate.
Example:

```
tmpfs   /tmp   tmpfs     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

OR Run the following commands to enable systemd `/tmp` mounting:
Run the following command to create the tmp.mount file is the correct location:

```
# cp -v /usr/share/systemd/tmp.mount /etc/systemd/system/
```

Edit `/etc/systemd/system/tmp.mount` to configure the `/tmp` mount:

```
  [Mount]
  What=tmpfs
  Where=/tmp
  Type=tmpfs
  Options=mode=1777,strictatime,nosuid,nodev,noexec
```

Run the following command to reload the systemd daemon with the unpdated tmp.mount unit file:

```
# systemctl daemon-reload
```

Run the following command to enable and start tmp.mount

```
# systemctl --now enable tmp.mount
```

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/

Additional Information:

If an entry for `/tmp` exists in `/etc/fstab` it will take precedence over entries in the `tmp.mount` file.

`tmpfs` can be resized using the size={size} parameter in `/etc/fstab` or on the Options line in the tmp.mount file. If we don't specify the size, it will be half the RAM. *Resize `tmpfs` examples:*

- `/etc/fstab`

```
tmpfs   /tmp          tmpfs   rw,noexec,nodev,nosuid,size=2G          0  0
```

- `tmp.mount`

```
[Mount]

What=tmpfs

Where=/tmp

Type=tmpfs

Options=mode=1777,strictatime,size=2G,noexec,nodev,nosuid
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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:

Verify that the `nodev` option is set if a `/tmp` partition exists
Run the following command and verify that nothing is returned:

```
# findmnt -n /tmp | grep -v nodev
```

Remediation:

Edit the `/etc/fstab` file **OR** the `/etc/systemd/system/local-fs.target.wants/tmp.mount` file:
If `/etc/fstab` is used to mount `/tmp`:
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
```

OR If systemd is used to mount `/tmp`:
Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nodev` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to restart the systemd daemon:

```
#  systemctl daemon-reload
```

Run the following command to restart `tmp.mount`

```
# systemctl restart tmp.mount
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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, verify that the `nosuid` option is set
Run the following command and verify that nothing is returned:

```
# findmnt -n /tmp | grep -v nosuid
```

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
```

OR Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nosuid` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp` :

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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

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, verify that the `noexec` option is set.
Run the following command and verify that nothing is returned:

```
# findmnt -n /tmp | grep -v noexec
```

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
```

OR Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `noexec` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp` :

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

CIS Controls:

Version 7

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

1.1.6 Ensure /dev/shm is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`/dev/shm` is a traditional shared memory concept. One program will create a memory portion, which other processes (if permitted) can access. Mounting `tmpfs` at `/dev/shm` is handled automatically by systemd.

Rationale:

Any user can upload and execute files inside the `/dev/shm` similar to the `/tmp` partition. Configuring `/dev/shm` allows an administrator to set the `noexec` option on the mount, making `/dev/shm` 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 `/dev/shm` is mounted:

```
# findmnt /dev/shm

TARGET   SOURCE FSTYPE OPTIONS
/dev/shm tmpfs  tmpfs  rw,nosuid,nodev,noexec
```

Remediation:

Edit `/etc/fstab` and add or edit the following line:

```
tmpfs      /dev/shm    tmpfs   defaults,noexec,nodev,nosuid,seclabel   0 0
```

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

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

Additional Information:

An entry for `/dev/shm` in `/etc/fstab` will take precedence.

`tmpfs` can be resized using the size={size} parameter in `/etc/fstab`. If we don't specify the size, it will be half the RAM.

Example:

```
  tmpfs   /dev/shm    tmpfs   defaults,noexec,nodev,nosuid,size=2G  0   0
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

13 Data Protection
Data Protection

1.1.7 Ensure nodev option set on /dev/shm partition (Automated)

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 nothing is returned:

```
# findmnt -n /dev/shm | grep -v nodev
```

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,nosuid,nodev,noexec /dev/shm
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.8 Ensure nosuid option set on /dev/shm partition (Automated)

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 nothing is returned:

```
# findnmt -n /dev/shm | grep -v nosuid
```

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,nodev,noexec /dev/shm
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.9 Ensure noexec option set on /dev/shm partition (Automated)

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 nothing is returned:

```
# findmnt -n /dev/shm | grep -v noexec
```

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,nosuid,nodev,noexec /dev/shm
```

CIS Controls:

Version 7

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

1.1.10 Ensure separate partition exists for /var (Automated)

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.

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.

Audit:

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

```
# findmnt /var

TARGET SOURCE    FSTYPE   OPTIONS
/var   <device>  <fstype> rw,relatime,attr2,inode64,noquota
```

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.

References:

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

Additional Information:

When modifying `/var` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.11 Ensure separate partition exists for /var/tmp (Automated)

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.

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.

Audit:

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

```
# findmnt /var/tmp

TARGET   SOURCE    FSTYPE   OPTIONS
/var/tmp <device>  <fstype> rw,relatime,attr2,inode64,noquota
```

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.12 Ensure /var/tmp partition includes the nodev option (Automated)

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, verify that the `nodev` option is set.
Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | grep -v nodev
```

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,nosuid,nodev,noexec /var/tmp
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.13 Ensure /var/tmp partition includes the nosuid option (Automated)

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, verify that the `nosuid` option is set.
Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | grep -v nosuid
```

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,nodev,noexec /var/tmp
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.14 Ensure /var/tmp partition includes the noexec option (Automated)

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, verify that the `noexec` option is set.
Run the following command and verify that nothing is returned:

```
# findmnt -n /var/tmp | grep -v noexec
```

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,nosuid,nodev,noexec /var/tmp
```

CIS Controls:

Version 7

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

1.1.15 Ensure separate partition exists for /var/log (Automated)

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.

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.

Audit:

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

```
# findmnt /var/log

TARGET   SOURCE   FSTYPE   OPTIONS
/var/log <device> <fstype> rw,relatime,attr2,inode64,noquota
```

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.

References:

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

Additional Information:

When modifying `/var/log` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode

CIS Controls:

Version 7

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

1.1.16 Ensure separate partition exists for /var/log/audit (Automated)

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.

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.

Audit:

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

```
# findmnt /var/log/audit

TARGET          SOURCE   FSTYPE   OPTIONS
/var/log/audit <device> <fstype> rw,relatime,attr2,inode64,noquota
```

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.

References:

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

Additional Information:

When modifying `/var/log/audit` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

CIS Controls:

Version 7

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

1.1.17 Ensure separate partition exists for /home (Automated)

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` .

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.

Audit:

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

```
# findmnt /home

TARGET SOURCE   FSTYPE   OPTIONS
/home  <device> <fstype> rw,relatime,attr2,inode64,noquota
```

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.

References:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.18 Ensure /home partition includes the nodev option (Automated)

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, verify that the `nodev` option is set.
Run the following command and verify that nothing is returned:

```
# findmnt -n /home | grep -v nodev
```

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
```

Additional Information:

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.19 Ensure nodev option set on removable media partitions (Manual)

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.20 Ensure nosuid option set on removable media partitions (Manual)

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.21 Ensure noexec option set on removable media partitions (Manual)

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.

CIS Controls:

Version 7

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

1.1.22 Ensure sticky bit is set on all world-writable directories (Automated)

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 \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod
a+t '{}'
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.23 Disable Automounting (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

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

Note: 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.

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.

Impact:

The use of 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.

Audit:

`autofs` should be removed or disabled.
Run the following commands to verify that `autofs` is not installed or is disabled
Run the following command to verify `autofs` is not enabled:

```
# systemctl is-enabled autofs

disabled
```

Verify result is not "enabled".
OR
Run the following command to verify that `autofs` is not installed

```
# dpkg -s autofs
```

Output should include:

```
package `autofs` is not installed
```

Remediation:

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

```
# systemctl --now disable autofs
```

OR
Run the following command to remove `autofs`

```
# apt purge autofs
```

CIS Controls:

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices
Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content
Configure devices to not auto-run content from removable media.

1.1.24 Disable USB Storage (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

USB storage provides a means to transfer and store files insuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

Note: An alternative solution to disabling the usb-storage module may be found in USBGuard. Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

Rationale:

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

Audit:

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

```
# modprobe -n -v usb-storage

install /bin/true

# lsmod | grep usb-storage

<No output>
```

Remediation:

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf
Example: `vi /etc/modprobe.d/usb_storage.conf`
and add the following line:

```
install usb-storage /bin/true
```

Run the following command to unload the usb-storage module:

```
rmmod usb-storage
```

CIS Controls:

Version 7

8.4 Configure Anti-Malware Scanning of Removable Devices
Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.

8.5 Configure Devices Not To Auto-run Content
Configure devices to not auto-run content from removable media.

1.2 Configure Software Updates

Debian Family Linux distributions use apt 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 (Manual)

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:

Run the following command and verify package repositories are configured correctly:

```
# apt-cache policy
```

Remediation:

Configure your package manager repositories according to site policy.

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

1.2.2 Ensure GPG keys are configured (Manual)

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:

```
# apt-key list
```

Remediation:

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

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

1.3 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 (Automated)

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:

Run the following commands to verify AIDE is installed:

```
# dpkg -s aide | grep -E '(Status:|not installed)'

Status: install ok installed

# dpkg -s aide-common | grep -E '(Status:|not installed)'

Status: install ok installed
```

Remediation:

Install AIDE using the appropriate package manager or manual installation:

```
# apt install aide aide-common
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.
Run the following commands to initialize AIDE:

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

Additional Information:

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.

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.3.2 Ensure filesystem integrity is regularly checked (Automated)

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 verify a `cron` job scheduled to run the aide check.

```
# grep -Ers '^([^#]+\s+)?(\/usr\/s?bin\/|^\s*)aide(\.wrapper)?\s(--
check|\$AIDEARGS)\b' /etc/cron.* /etc/crontab /var/spool/cron/
```

Ensure a cron job in compliance with site policy is returned.
OR Run the following commands to verify that aidcheck.service and aidcheck.timer are enabled and aidcheck.timer is running

```
# systemctl is-enabled aidecheck.service

# systemctl is-enabled aidecheck.timer
# systemctl status aidecheck.timer
```

Remediation:

If cron will be used to schedule and run aide check:
Run the following command:

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

Add the following line to the crontab:

```
0 5 * * * /usr/bin/aide.wrapper --config /etc/aide/aide.conf --check
```

OR If aidecheck.service and aidecheck.timer will be used to schedule and run aide check:
Create or edit the file `/etc/systemd/system/aidecheck.service` and add the following lines:

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/bin/aide.wrapper --config /etc/aide/aide.conf --check

[Install]
WantedBy=multi-user.target
```

Create or edit the file `/etc/systemd/system/aidecheck.timer` and add the following lines:

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*
# chmod 0644 /etc/systemd/system/aidecheck.*

# systemctl daemon-reload

# systemctl enable aidecheck.service
# systemctl --now enable aidecheck.timer
```

References:

1. https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service
2. https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer

Additional Information:

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

systemd timers, timer file `aidecheck.timer` and service file `aidecheck.service`, have been included as an optional alternative to using `cron`

Ubuntu advises using `/usr/bin/aide.wrapper` rather than calling `/usr/bin/aide` directly in order to protect the database and prevent conflicts

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.4 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 not overridden (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The permissions on `/boot/grub/grub.cfg` are changed to `444` when `grub.cfg` is updated by the `update-grub` command

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 the output:

```
# grep -E '^\s*chmod\s+[0-7][0-7][0-7]\s+\$\{grub_cfg\}\.new' -A 1 -B1
/usr/sbin/grub-mkconfig
```

Verify the output is:

```
if [ "x${grub_cfg}" != "x" ]; then
  chmod 400 ${grub_cfg}.new || true
fi
```

Remediation:

Run the following command to update `chmod 444` to `chmod 400` in `/usr/sbin/grub-mkconfig`:

```
# sed -ri 's/chmod\s+[0-7][0-7][0-7]\s+\$\{grub_cfg\}\.new/chmod 400
${grub_cfg}.new/' /usr/sbin/grub-mkconfig
```

Run the following command to remove check on password not being set to before running `chmod` command:

```
# sed -ri 's/ && ! grep "\^password" \$\{grub_cfg\}.new >\/dev\/null//'
/usr/sbin/grub-mkconfig
```

Default Value:

```
if [ "x${grub_cfg}" != "x" ] && ! grep "^password" ${grub_cfg}.new
>/dev/null; then

  chmod 444 ${grub_cfg}.new || true

fi
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

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

1.4.2 Ensure bootloader password is set (Automated)

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 AppArmor at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

You can add `--unrestricted` to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.

More Information: https://help.ubuntu.com/community/Grub2/Passwords

Audit:

Run the following commands and verify output matches:

```
# grep "^set superusers" /boot/grub/grub.cfg

set superusers="<username>"

# grep "^password" /boot/grub/grub.cfg

password_pbkdf2 <username> <encrypted-password>
```

Remediation:

Create an encrypted password with `grub-mkpasswd-pbkdf2`:

```
# grub-mkpasswd-pbkdf2

Enter password: <password>
Reenter password: <password>
PBKDF2 hash of your password is <encrypted-password>
```

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

```
cat <<EOF
set superusers="<username>"
password_pbkdf2 <username> <encrypted-password>
EOF
```

The superuser/user information and password should not be contained in the /etc/grub.d/00_header file as this file could be overwritten in a package update.
If there is a requirement to be able to boot/reboot without entering the password, edit /etc/grub.d/10_linux and add `--unrestricted` to the line `CLASS=`
Example:

```
CLASS="--class gnu-linux --class gnu --class os --unrestricted"
```

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

```
# update-grub
```

Default Value:

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/grub.cfg` with the appropriate grub configuration file for your environment.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4.3 Ensure permissions on bootloader config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options.

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` is 0400 or more restrictive.

```
# stat /boot/grub/grub.cfg

Access: (0400/-r--------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

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

```
# chown root:root /boot/grub/grub.cfg
# chmod u-wx,go-rwx /boot/grub/grub.cfg
```

Additional Information:

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/grub.cfg` with the appropriate grub configuration file for your environment

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.4.4 Ensure authentication required for single user mode (Automated)

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:

Perform the following to determine if a password is set for the `root` user:

```
# grep -Eq '^root:\$[0-9]' /etc/shadow || echo "root is locked"
```

No results should be returned.

Remediation:

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

```
# passwd root
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.5 Additional Process Hardening

1.5.1 Ensure XD/NX support is enabled (Manual)

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.

Note: 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

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.

```
# journalctl | grep 'protection: active'

kernel: NX (Execute Disable) protection: active
```

OR on systems without journalctl:

```
# [[ -n $(grep noexec[0-9]*=off /proc/cmdline) || -z $(grep -E -i ' (pae|nx)
' /proc/cpuinfo) || -n $(grep '\sNX\s.*\sprotection:\s' /var/log/dmesg | grep
-v active) ]] && echo "NX Protection is not active"
```

Nothing should be returned

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.

CIS Controls:

Version 7

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

1.5.2 Ensure address space layout randomization (ASLR) is enabled (Automated)

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 commands and verify output matches:

```
# sysctl kernel.randomize_va_space

kernel.randomize_va_space = 2

# grep -Es "^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-9]+)"
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

Nothing should be returned
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file ending in `.conf`:

```
kernel.randomize_va_space = 2
```

Run the following script to comment out entries that override the default setting of kernel.randomize_va_space:

```
#!/usr/bin/bash

for file in /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /run/sysctl.d/*.conf; do
   if [ -f "$file" ]; then
      grep -Esq "^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-9]|[1-9][0-
9]+)" "$file" && sed -ri 's/^\s*kernel\.randomize_va_space\s*=\s*([0-1]|[3-
9]|[1-9][0-9]+)/# &/gi' "$file"
   fi
done
```

Run the following command to set the active kernel parameter:

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

Default Value:

kernel.randomize_va_space = 2

References:

1. http://manpages.ubuntu.com/manpages/focal/man5/sysctl.d.5.html

Additional Information:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the `".conf"` extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

CIS Controls:

Version 7

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

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

1.5.3 Ensure prelink is disabled (Automated)

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:

```
# dpkg -s prelink | grep -E '(Status:|not installed)'

dpkg-query: package 'prelink' is not installed and no information is
available
```

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

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

```
# apt purge prelink
```

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

1.5.4 Ensure core dumps are restricted (Automated)

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 -Es '^(\*|\s).*hard.*core.*(\s+#.*)?$' /etc/security/limits.conf
/etc/security/limits.d/*

* hard core 0

# sysctl fs.suid_dumpable

fs.suid_dumpable = 0

# grep "fs.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/*

fs.suid_dumpable = 0
```

Run the following command to check if systemd-coredump is installed:

```
# systemctl is-enabled coredump.service
```

If `enabled`, `masked`, or `disabled` is returned systemd-coredump is installed

Remediation:

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

```
* hard core 0
```

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
fs.suid_dumpable = 0
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

IF systemd-coredump is installed:
edit `/etc/systemd/coredump.conf` and add/modify the following lines:

```
Storage=none
ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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.

Notes:

- *Apparmor is the default MAC provided with Debian systems.*
- *Additional Mandatory Access Control systems to include SELinux exist. If a different Mandatory Access Control systems is used, please follow it's vendors guidance for proper implementation in place of the guidance provided in this section*

1.6.1 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.

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/

1.6.1.1 Ensure AppArmor is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

AppArmor provides Mandatory Access Controls.

Rationale:

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

Audit:

Verify that AppArmor is installed:

```
# dpkg -s apparmor | grep -E '(Status:|not installed)'

Status: install ok installed
```

Remediation:

Install AppArmor.

```
# apt install apparmor
```

CIS Controls:

Version 7

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

1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

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

Rationale:

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

Audit:

Run the following commands to verify that all `linux` lines have the `apparmor=1` and `security=apparmor` parameters set:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "apparmor=1"

Nothing should be returned

# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "security=apparmor"

Nothing should be returned
```

Remediation:

Edit `/etc/default/grub` and add the `apparmor=1` and `security=apparmor` parameters to the `GRUB_CMDLINE_LINUX=` line

```
GRUB_CMDLINE_LINUX="apparmor=1 security=apparmor"
```

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

```
# update-grub
```

CIS Controls:

Version 7

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

1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - 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, and are in either enforce or complain mode:

```
# apparmor_status | grep profiles
```

Review output and ensure that profiles are loaded, and in either enforce or complain mode:

```
37 profiles are loaded.
35 profiles are in enforce mode.
2 profiles are in complain mode.
4 processes have profiles defined.
```

Run the following command and verify no processes are unconfined

```
# apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

```
4 processes have profiles defined.
4 processes are in enforce mode.
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:

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

OR
Run the following command to set all profiles to complain mode:

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

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

CIS Controls:

Version 7

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

1.6.1.4 Ensure all AppArmor Profiles are enforcing (Automated)

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 commands and verify that profiles are loaded and are not in complain mode:

```
# apparmor_status | grep profiles
```

Review output and ensure that profiles are loaded, and in enforce mode:

```
34 profiles are loaded.
34 profiles are in enforce mode.
0 profiles are in complain mode.
2 processes have profiles defined.
```

Run the following command and verify that no processes are unconfined:

```
apparmor_status | grep processes
```

Review the output and ensure no processes are unconfined:

```
2 processes have profiles defined.
2 processes are in enforce mode.
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:

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

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

CIS Controls:

Version 7

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

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

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 Ensure message of the day is configured properly (Automated)

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 no results are returned:

```
# grep -Eis "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2
| sed -e 's/"//g'))" /etc/motd
```

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`
OR if the motd is not used, this file can be removed.
Run the following command to remove the motd file:

```
# rm /etc/motd
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7.2 Ensure permissions on /etc/issue.net are configured (Automated)

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 u-x,go-wx /etc/issue.net
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7.3 Ensure permissions on /etc/issue are configured (Automated)

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 u-x,go-wx /etc/issue
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7.4 Ensure permissions on /etc/motd are configured (Automated)

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`, or the file doesn't exist.

```
# stat /etc/motd

Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
  OR
stat: cannot stat '/etc/motd': No such file or directory
```

Remediation:

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

```
# chown root:root /etc/motd
# chmod u-x,go-wx /etc/motd
```

OR run the following command to remove the `/etc/motd` file:

```
# rm /etc/motd
```

Default Value:

File doesn't exist

Additional Information:

If Message of the day is not needing, this file can be removed.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7.5 Ensure remote login warning banner is configured properly (Automated)

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 `\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/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue.net
```

Remediation:

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

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7.6 Ensure local login warning banner is configured properly (Automated)

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 `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

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:

```
# grep -E -i "(\\\v|\\\r|\\\m|\\\s|$(grep '^ID=' /etc/os-release | cut -d= -
f2 | sed -e 's/"//g'))" /etc/issue
```

Remediation:

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

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.8 GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Note: If GDM is not installed on the system, this section can be skipped

1.8.1 Ensure GNOME Display Manager is removed (Manual)

Profile Applicability:

- Level 2 - Server

Description:

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

Rationale:

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

Impact:

Removing the GNOME Display manager will remove the Graphical User Interface (GUI) from the system.

Audit:

Run the following command and verify `gdm3` is not installed:

```
# dpkg -s gdm3 | grep -E '(Status:|not installed)'

dpkg-query: package 'gdm3' is not installed and no information is available
```

Remediation:

Run the following command to uninstall `gdm3`:

```
# apt purge gdm3
```

CIS Controls:

Version 7

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

1.8.2 Ensure GDM login banner is configured (Automated)

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/gdm3/greeter.dconf-defaults` file exists and contains the following:

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

Remediation:

Edit or create the file `/etc/gdm3/greeter.dconf-defaults` and add the following:

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

Example banner message: 'Authorized uses only. All activity may be monitored and reported.'
Run the following command to re-load `GDM` on the next login or reboot:

```
# dpkg-reconfigure gdm3
```

Additional Information:

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.8.3 Ensure disable-user-list is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

The `disable-user-list` option controls is a list of users is displayed on the login screen

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Audit:

Run the following command to verify that disable-user-list is enabled:

```
# grep -E '^\s*disable-user-list\s*=\s*true\b'

disable-user-list=true
```

Remediation:

Edit or create the file `/etc/gdm3/greeter.dconf-defaults` and edit or add the following:

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

Run the following command to re-load GDM on the next login or reboot:

```
# dpkg-reconfigure gdm3
```

Default Value:

false

Additional Information:

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the user list

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.8.4 Ensure XDCMP is not enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

Rationale:

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

Audit:

Run the following command and verify the output:

```
# grep -Eis '^\s*Enable\s*=\s*true' /etc/gdm3/custom.conf

Nothing should be returned
```

Remediation:

Edit the file `/etc/gdm3/custom.conf` and remove the line:

```
Enable=true
```

Default Value:

false (This is denoted by no Enabled= entry in the file `/etc/gdm3/custom.conf` in the [xdmcp] section

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

1.9 Ensure updates, patches, and additional security software are installed (Manual)

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:

```
# apt -s upgrade
```

Remediation:

Run the following command to update all packages following local site policy guidance on applying updates and patches:

```
# apt upgrade
```

OR

```
# apt dist-upgrade
```

Additional Information:

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

- upgrade - is used to install the newest versions of all packages currently installed on the system from the sources enumerated in /etc/apt/sources.list. Packages currently installed with new versions available are retrieved and upgraded; under no circumstances are currently installed packages removed, or packages not already installed retrieved and installed. New versions of currently installed packages that cannot be upgraded without changing the install status of another package will be left at their current version. An update must be performed first so that apt knows that new versions of packages are available.
- dist-upgrade - in addition to performing the function of upgrade, also intelligently handles changing dependencies with new versions of packages; apt has a "smart" conflict resolution system, and it will attempt to upgrade the most important packages at the expense of less important ones if necessary. So, dist-upgrade command may remove some packages. The /etc/apt/sources.list file contains a list of locations from which to retrieve desired package files. See also apt_preferences(5) for a mechanism for overriding the general settings for individual packages.

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

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.

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

2.1 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 deleted from the system to reduce the potential attack surface. If a package is required as a dependency, and the service is not required, the service should be stopped and masked.

The following command can be used to stop and mask the service:

```
# systemctl --now mask <service_name>
```

2.1.1 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 systemd-timesyncd, chrony, or ntp.

Notes:

- *If access to a physical host's clock is available and configured according to site policy, this section can be skipped*
- *Only one time synchronization method should be in use on the system*
- *Only the section related to the time synchronization method in use on the system should be followed, all other time synchronization recommendations should be skipped*
- *If access to a physical host's clock is available and configured according to site policy,* `systemd-timesyncd` *should be stopped and masked*

2.1.1.1 Ensure time synchronization is in use (Automated)

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.

Notes:

- *If access to a physical host's clock is available and configured according to site policy, this section can be skipped*
- *Only one time synchronization method should be in use on the system*
- *If access to a physical host's clock is available and configured according to site policy, systemd-timesyncd should be stopped and masked*

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 that timesyncd, chrony, or NTP is installed. Use one of the following commands to determine the needed information:
If systemd-timesyncd is used:

```
# systemctl is-enabled systemd-timesyncd
```

If chrony is used:

```
# dpkg -s chrony
```

If ntp is used:

```
# dpkg -s ntp
```

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 systems where host based time synchronization is not available, configure systemd-timesyncd. If "full featured" and/or encrypted time synchronization is required, install chrony or NTP.
To install chrony:

```
# apt install chrony
```

To install ntp:

```
# apt install ntp
```

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

CIS Controls:

Version 7

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

2.1.1.2 Ensure systemd-timesyncd is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network. It implements an SNTP client. In contrast to NTP implementations such as chrony or the NTP reference server this only implements a client side, and does not bother with the full NTP complexity, focusing only on querying time from one remote server and synchronizing the local clock to it. The daemon runs with minimal privileges, and has been hooked up with networkd to only operate when network connectivity is available. The daemon saves the current clock to disk every time a new NTP sync has been acquired, and uses this to possibly correct the system clock early at bootup, in order to accommodate for systems that lack an RTC such as the Raspberry Pi and embedded devices, and make sure that time monotonically progresses on these systems, even if it is not always correct. To make use of this daemon a new system user and group "systemd-timesync" needs to be created on installation of systemd.

Notes:

- *If `chrony` or `ntp` are used, `systemd-timesyncd` should be stopped and masked, and this section skipped*
- *This recommendation only applies if `timesyncd` is in use on the system*
- *Only one time synchronization method should be in use on the system*

Rationale:

Proper configuration is vital to ensuring time synchronization is working properly.

Audit:

- Verify that only one time synchronization method is in use on the system:

Run the following command to verify that `ntp` is not installed:

```
dpkg -s ntp

dpkg-query: package 'ntp' is not installed and no information is available
```

Run the following command to verify that `chrony` is not installed:

```
dpkg -s chrony

dpkg-query: package 'chrony' is not installed and no information is available
```

- Ensure that timesyncd is enabled and started

Run the following commands:

```
# systemctl is-enabled systemd-timesyncd.service

enabled
```

- Verify that `systemd-timesyncd` is configured:

Review `/etc/systemd/timesyncd.conf` and ensure that the NTP servers, NTP FallbackNTP servers, and RootDistanceMaxSec listed are in accordance with local policy
Run the following command

```
# timedatectl status
```

This should return something similar to:

```
      Local time: Tue 2019-06-04 15:40:45 EDT
  Universal time: Tue 2019-06-04 19:40:45 UTC
        RTC time: Tue 2019-06-04 19:40:45
       Time zone: America/New_York (EDT, -0400)
     NTP enabled: yes
NTP synchronized: yes
 RTC in local TZ: no
      DST active: yes
 Last DST change: DST began at
                  Sun 2019-03-10 01:59:59 EST
                  Sun 2019-03-10 03:00:00 EDT
 Next DST change: DST ends (the clock jumps one hour backwards) at
                  Sun 2019-11-03 01:59:59 EDT
                  Sun 2019-11-03 01:00:00 EST
```

Remediation:

- Remove additional time synchronization methods:

Run the following commands to remove `ntp` and `chrony`:

```
# apt purge ntp
# apt purge chrony
```

- Configure `systemd-timesyncd`:

Run the following command to enable systemd-timesyncd

```
# systemctl enable systemd-timesyncd.service
```

Edit the file /etc/systemd/timesyncd.conf and add/modify the following lines:

```
NTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org #Servers listed should be In
Accordence With Local Policy

FallbackNTP=2.debian.pool.ntp.org 3.debian.pool.ntp.org #Servers listed
should be In Accordence With Local Policy

RootDistanceMax=1 #should be In Accordence With Local Policy
```

Run the following commands to start systemd-timesyncd.service

```
# systemctl start systemd-timesyncd.service

# timedatectl set-ntp true
```

Additional Information:

The systemd-timesyncd service specifically implements only SNTP. This minimalistic service will set the system clock for large offsets or slowly adjust it for smaller deltas. More complex use cases are not covered by systemd-timesyncd

CIS Controls:

Version 7

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

2.1.1.3 Ensure chrony is configured (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP) and 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.

Notes:

- *If `ntp` or `systemd-timesyncd` are used, `chrony` should be removed and this section skipped*
- *This recommendation only applies if chrony is in use on the system*
- *Only one time synchronization method should be in use on the system*

Rationale:

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

Audit:

Verify that only one time synchronization method is in use on the system:
Run the following command to verify that `ntp` is not installed:

```
dpkg -s ntp | grep -E '(Status:|not installed)'

dpkg-query: package 'ntp' is not installed and no information is available
```

Run the following command to verify that systemd-timsyncd is masked:

```
# systemctl is-enabled systemd-timesyncd

masked
```

Verify that `chrony` is configured:
Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/chrony/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
```

Note: The compiled-in default value is `_chrony`

Remediation:

Remove and/or disable additional time synchronization methods:
Run the following command to remove `ntp`:

```
# apt purge ntp
```

Run the following command to stop and mask systemd-timesyncd:

```
# systemctl --now mask systemd-timesyncd
```

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

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

Add or edit the `user` line to `/etc/chrony/chrony.conf`:

```
user _chrony
```

CIS Controls:

Version 7

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

2.1.1.4 Ensure ntp is configured (Automated)

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.

Notes:

- *If `chrony` or `systemd-timesyncd` are used, `ntp` should be removed and this section skipped*
- *This recommendation only applies if ntp is in use on the system*
- *Only one time synchronization method should be 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:

- Verify that only one time synchronization method is in use on the system:

Run the following command to verify `chrony` is not in use on the system:

```
# dpkg -s chrony | grep -E '(Status:|not installed)'

dpkg-query: package 'chrony' is not installed and no information is available
```

Run the following command to verify that systemd-timesyncd is not in use on the system:

```
# systemctl is-enabled systemd-timesyncd

masked
```

- Verify that `ntp` is configured:

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 -E "^(server|pool)" /etc/ntp.conf

server <remote-server>
```

Multiple servers may be configured.

Verify that `ntp` is configured to run as the `ntp` user by running the following command and verifying output matches:

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

RUNASUSER=ntp
```

Additional options may be present

Remediation:

- Remove and/or disable additional time synchronization methods:

Run the following command to remove `chrony`:

```
apt purge chrony
```

Run the following command to stop and mask `systemd-timesyncd`:

```
# systemctl --now mask systemd-timesyncd
```

- Configure `ntp`:

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 or pool lines to `/etc/ntp.conf` as appropriate:

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

Configure `ntp` to run as the `ntp` user by adding or editing the `/etc/init.d/ntp` file:

```
RUNASUSER=ntp
```

CIS Controls:

Version 7

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

2.1.2 Ensure X Window System is not installed (Automated)

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.

Impact:

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime, if provided by your distribution.

Audit:

Verify X Windows System is not installed:

```
dpkg -l xserver-xorg*
```

Remediation:

Remove the X Windows System packages:

```
apt purge xserver-xorg*
```

CIS Controls:

Version 7

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

2.1.3 Ensure Avahi Server is not installed (Automated)

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 remove this package to reduce the potential attack surface.

Audit:

Run the following command to verify `avahi-daemon` is not installed:

```
# dpkg -s avahi-daemon | grep -E '(Status:|not installed)'

dpkg-query: package 'avahi-daemon' is not installed and no information is
available
```

Remediation:

Run the following commands to remove `avahi-daemon`:

```
# systemctl stop avahi-daaemon.service
# systemctl stop avahi-daemon.socket
# apt purge avahi-daemon
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.4 Ensure CUPS is not installed (Automated)

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 removed to reduce the potential attack surface.

Impact:

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

Audit:

Run the following command to verify `cups` is not Installed:

```
# dpkg -s cups | grep -E '(Status:|not installed)'

dpkg-query: package 'cups' is not installed and no information is available
```

Remediation:

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

```
# apt purge cups
```

References:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.5 Ensure DHCP Server is not installed (Automated)

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 package be removed to reduce the potential attack surface.

Audit:

Run the following commands to verify `isc-dhcp-server` is not installed:

```
# dpkg -s isc-dhcp-server | grep -E '(Status:|not installed)'

dpkg-query: package 'isc-dhcp-server' is not installed and no information is
available
```

Remediation:

Run the following command to remove `isc-dhcp-server`:

```
# apt purge isc-dhcp-server
```

References:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.6 Ensure LDAP server is not installed (Automated)

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 removed to reduce the potential attack surface.

Audit:

Run the following command to verify `slapd` is not installed:

```
# dpkg -s slapd | grep -E '(Status:|not installed)'

dpkg-query: package 'slapd' is not installed and no information is available
```

Remediation:

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

```
# apt purge slapd
```

References:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.7 Ensure NFS is not installed (Automated)

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 removed to reduce the remote attack surface.

Audit:

Run the following command to verify `nfs` is not installed:

```
# dpkg -s nfs-kernel-server | grep -E '(Status:|not installed)'

dpkg-query: package 'nfs-kernel-server' is not installed and no information
is available
```

Remediation:

Run the following command to remove `nfs`:

```
# apt purge nfs-kernel-server
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.8 Ensure DNS Server is not installed (Automated)

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 the following command to verify `DNS server` is not installed:

```
# dpkg -s bind9 | grep -E '(Status:|not installed)'

dpkg-query: package 'bind9' is not installed and no information is available
```

Remediation:

Run the following commands to disable `DNS server`:

```
# apt purge bind9
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.9 Ensure FTP Server is not installed (Automated)

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 the following command to verify `vsftpd` is not installed:

```
# dpkg -s vsftpd | grep -E '(Status:|not installed)'

dpkg-query: package 'vsftpd' is not installed and no information is available
```

Remediation:

Run the following command to remove `vsftpd`:

```
# apt purge vsftpd
```

Additional Information:

Additional FTP servers also exist and should be audited.

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.10 Ensure HTTP server is not installed (Automated)

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 the following command to verify `apache` is not installed:

```
# dpkg -s apache2 | grep -E '(Status:|not installed)'

dpkg-query: package 'apache2' is not installed and no information is
available
```

Remediation:

Run the following command to remove `apache`:

```
# apt purge apache2
```

Additional Information:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.11 Ensure IMAP and POP3 server are not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot-imapd` and `dovecot-pop3d` are 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 package be removed to reduce the potential attack surface.

Audit:

Run the following command to verify `dovecot-imapd` and `dovecot-pop3d` are not installed:

```
# dpkg -s dovecot-imapd dovecot-pop3d  | grep -E '(Status:|not installed)'

dpkg-query: package 'dovecot-imapd' is not installed and no information is
available
dpkg-query: package 'dovecot-pop3d' is not installed and no information is
available
```

Remediation:

Run one of the following commands to remove `dovecot-imapd` and `dovecot-pop3d`:

```
# apt purge dovecot-imapd dovecot-pop3d
```

Additional Information:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.12 Ensure Samba is not installed (Automated)

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 Server 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 should be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `samba` is not installed:

```
# dpkg -s samba | grep -E '(Status:|not installed)'

dpkg-query: package 'samba' is not installed and no information is available
```

Remediation:

Run the following command to remove `samba`:

```
# apt purge samba
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.13 Ensure HTTP Proxy Server is not installed (Automated)

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 the following command to verify `squid` is not installed:

```
# dpkg -s squid | grep -E '(Status:|not installed)'

dpkg-query: package 'squid' is not installed and no information is available
```

Remediation:

Run the following command to remove `squid`:

```
# apt purge squid
```

Additional Information:

Several HTTP proxy servers exist. These and other services should be checked

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.14 Ensure SNMP Server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

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 can communicate using `SNMPv1`, which transmits data in the clear and does not require authentication to execute commands. `SNMPv3` replaces the simple/clear text password sharing used in `SNMPv2` with more securely encoded parameters. If the the SNMP service is not required, the `net-snmp` package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- *The server should be configured for `SNMP v3` only. `User Authentication` and `Message Encryption` should be configured.*
- *If `SNMP v2` is **absolutely** necessary, modify the community strings' values.*

Audit:

Run the following command to verify `snmpd` is not installed:

```
# dpkg -s snmpd | grep -E '(Status:|not installed)'

dpkg-query: package 'snmpd' is not installed and no information is available
```

Remediation:

Run the following command to remove `snmpd`:

```
# apt purge snmpd
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.15 Ensure mail transfer agent is configured for local-only mode (Automated)

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.

Note: This recommendation is designed around the exim4 mail server, depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

Audit:

Run the following command to verify that the MTA is not listening on any non-loopback address (`127.0.0.1` or`::1`).
Nothing should be returned

```
#  ss -lntu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|::1):25\s'
```

Remediation:

Edit `/etc/exim4/update-exim4.conf.conf` and and or modify following lines to look like the lines below:

```
dc_eximconfig_configtype='local'
dc_local_interfaces='127.0.0.1 ; ::1'
dc_readhost=''
dc_relay_domains=''
dc_minimaldns='false'
dc_relay_nets=''
dc_smarthost=''
dc_use_split_config='false'
dc_hide_mailname=''
dc_mailname_in_oh='true'
dc_localdelivery='mail_spool'
```

Restart exim4:

```
# systemctl restart exim4
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.16 Ensure rsync service is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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

Rationale:

The `rsync` service presents a security risk as it uses unencrypted protocols for communication. The rsync package should be removed to reduce the attack area of the system.

Audit:

Run the following command to verify `rsync` is not installed:

```
# dpkg -s rsync | grep -E '(Status:|not installed)'

dpkg-query: package 'rsync' is not installed and no information is available
```

Remediation:

Run the following command to remove `rsync`:

```
# apt purge rsync
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.1.17 Ensure NIS Server is not installed (Automated)

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 has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed and other, more secure services be used

Audit:

Run the following command to verify `nis` is not installed:

```
# dpkg -s nis | grep -E '(Status:|not installed)'

dpkg-query: package 'nis' is not installed and no information is available
```

Remediation:

Run the following command to remove `nis`:

```
# apt purge nis
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.2 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.

2.2.1 Ensure NIS Client is not installed (Automated)

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 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.

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.

Audit:

Verify `nis` is not installed. Use the following command to provide the needed information:

```
# dpkg -s nis  | grep -E '(Status:|not installed)'

dpkg-query: package 'nis' is not installed and no information is available
```

Remediation:

Uninstall `nis`:

```
# apt purge nis
```

CIS Controls:

Version 7

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

2.2.2 Ensure rsh client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsh-client` 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` .

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.

Audit:

Verify `rsh-client` is not installed. Use the following command to provide the needed information:

```
# dpkg -s rsh-client | grep -E '(Status:|not installed)'

dpkg-query: package 'rsh-client' is not installed and no information is
available
```

Remediation:

Uninstall `rsh`:

```
# apt purge rsh-client
```

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

2.2.3 Ensure talk client is not installed (Automated)

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.

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.

Audit:

Verify `talk` is not installed. The following command may provide the needed information:

```
# dpkg -s talk | grep -E '(Status:|not installed)'

dpkg-query: package 'talk' is not installed and no information is available
```

Remediation:

Uninstall `talk`:

```
# apt purge talk
```

CIS Controls:

Version 7

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

2.2.4 Ensure telnet client is not installed (Automated)

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.

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.

Audit:

Verify `telnet` is not installed. Use the following command to provide the needed information:

```
# dpkg -s telnet | grep -E '(Status:|not installed)'

dpkg-query: package 'telnet' is not installed and no information is available
```

Remediation:

Uninstall `telnet`:

```
# apt purge telnet
```

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

2.2.5 Ensure LDAP client is not installed (Automated)

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.

Impact:

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

Audit:

Verify that `ldap-utils` is not installed. Use the following command to provide the needed information:

```
# dpkg -s ldap-utils | grep -E '(Status:|not installed)'

dpkg-query: package 'ldap-utils' is not installed and no information is
available
```

Remediation:

Uninstall `ldap-utils`:

```
# apt purge ldap-utils
```

CIS Controls:

Version 7

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

2.2.6 Ensure RPC is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Remote Procedure Call (RPC) is a method for creating low level client server applications across different system architectures. It requires an RPC compliant client listening on a network port. The supporting package is rpcbind."

Rationale:

If RPC is not required, it is recommended that this services be removed to reduce the remote attack surface.

Audit:

Run the following command to verify `rpcbind` is not installed:

```
# dpkg -s rpcbind | grep -E '(Status:|not installed)'

dpkg-query: package 'rpcbind' is not installed and no information is
available
```

Remediation:

Run the following command to remove `rpcbind`:

```
# apt purge rpcbind
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

2.3 Ensure nonessential services are removed or masked (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

Rationale:

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

Audit:

Run the following command:

```
# lsof -i -P -n | grep -v "(ESTABLISHED)"
```

Review the output to ensure that all services listed are required on the system. If a listed service is not required, remove the package containing the service. If the package containing a non-essential service is required, stop and mask the non-essential service.

Remediation:

Run the following command to remove the package containing the service:

```
# apt purge <package_name>
```

OR If required packages have a dependency:
Run the following command to stop and mask the service:

```
# systemctl --now mask <service_name>
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3 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 Disable unused network protocols and devices

To reduce the attack surface of a system, unused network protocols and devices should be disabled.

3.1.1 Disable IPv6 (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

Rationale:

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Impact:

If IPv6 is disabled through sysctl config, `SSH X11forwarding` may no longer function as expected. We recommend that SSH X11fowarding be disabled, but if required, the following will allow for `SSH X11forwarding` with IPv6 disabled through sysctl config:

Add the following line the `/etc/ssh/sshd_config` file:

```
AddressFamily inet
```

Run the following command to re-start the openSSH server:

```
# systemctl restart sshd
```

Audit:

Run one of the following commands to verify IPv6 is disabled:
IF IPv6 is disabled through grub
Run the following command:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "ipv6.disable=1"
```

no lines should be returned
OR
IF IPv6 is disabled through sysctl settings:
Run the following commands:

```
# sysctl net.ipv6.conf.all.disable_ipv6

net.ipv6.conf.all.disable_ipv6 = 1

# sysctl net.ipv6.conf.default.disable_ipv6

net.ipv6.conf.default.disable_ipv6 = 1

# grep -E
'^\s*net\.ipv6\.conf\.(all|default)\.disable_ipv6\s*=\s*1\b(\s+#.*)?$'
/etc/sysctl.conf /etc/sysctl.d/*.conf | cut -d: -f2

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

Remediation:

Use **one** of the two following methods to disable IPv6 on the system:
To disable IPv6 through the GRUB2 config:
Edit `/etc/default/grub` and add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

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

```
# update-grub
```

OR
To disable IPv6 through sysctl settings:
Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

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

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.disable_ipv6=1
# sysctl -w net.ipv6.conf.default.disable_ipv6=1
# sysctl -w net.ipv6.route.flush=1
```

CIS Controls:

Version 7

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

3.1.2 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

Description:

Wireless networking is used when wired networks are unavailable. Debian 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.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

Audit:

Run the following script to verify no wireless interfaces are active on the system:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
  nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b' && echo
"Wireless is not enabled" || nmcli radio all
elif [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
  t=0
  drivers=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless
| xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver)";done | sort -u)
  for dm in $drivers; do
    if grep -Eq "^\s*install\s+$dm\s+/bin/(true|false)"
/etc/modprobe.d/*.conf; then
      /bin/true
    else
      echo "$dm is not disabled"
      t=1
    fi
  done
  [[ $t -eq 0 ]] && echo "Wireless is not enabled"
else
  echo "Wireless is not enabled"
fi
```

Output should be:

```
Wireless is not enabled
```

Remediation:

Run the following script to disable any wireless interfaces:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
  nmcli radio all off
else
  if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
    drivers=$(for driverdir in $(find /sys/class/net/*/ -type d -name 
wireless | xargs -0 dirname); do basename "$(readlink -f 
"$driverdir"/device/driver)";done | sort -u)
    for dm in $drivers; do
      echo "install $dm /bin/true" >> /etc/modprobe.d/disable_wireless.conf
    done
  fi
fi
```

Additional Information:

Edited to correct scripts. Do we need to remove other references to a wireless driver from /etc/modprobe.d/? The test system I used had a file iwlwifi.conf to load the correct drivers.

CIS Controls:

Version 7

15.4 Disable Wireless Access on Devices if Not Required
Disable wireless access on devices that do not have a business purpose for wireless access.

15.5 Limit Wireless Access on Client Devices
Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.

3.2 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.

Note:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the the `".conf"` extension. extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

3.2.1 Ensure packet redirect sending is disabled (Automated)

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

# grep -E "^\s*net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.conf.all.send_redirects = 0

# grep -E "^\s*net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

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

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.2.2 Ensure IP forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

Rationale:

Setting the flags 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 commands and verify output matches:

```
# sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 0

# grep -E -s "^\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

No value should be returned
```

IF IPv6 is enabled:
Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.forwarding

net.ipv6.conf.all.forwarding = 0

# grep -E -s "^\s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

No value should be returned
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Run the following command to restore the default parameter and set the active kernel parameter:

```
# grep -Els "^\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while
read filename; do sed -ri "s/^\s*(net\.ipv4\.ip_forward\s*)(=)(\s*\S+\b).*$/#
*REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w
net.ipv4.route.flush=1
```

IF IPv6 is enabled:
Run the following command to restore the default parameter and set the active kernel parameter:

```
# grep -Els "^\s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while
read filename; do sed -ri
"s/^\s*(net\.ipv6\.conf\.all\.forwarding\s*)(=)(\s*\S+\b).*$/# *REMOVED* \1/"
$filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w
net.ipv6.route.flush=1
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3 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.

Note:

Configuration files are read from directories in `/etc/`, `/run/`, `/usr/local/lib/`, and `/lib/`, in order of precedence. Files must have the the "`.conf`" extension. extension. Files in `/etc/` override files with the same name in `/run/`, `/usr/local/lib/`, and `/lib/`. Files in `/run/` override files with the same name under `/usr/`.

All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Thus, the configuration in a certain file may either be replaced completely (by placing a file with the same name in a directory with higher priority), or individual settings might be changed (by specifying additional settings in a file with a different name that is ordered later).

Packages should install their configuration files in `/usr/lib/` (distribution packages) or `/usr/local/lib/` (local installs). Files in `/etc/` are reserved for the local administrator, who may use this logic to override the configuration files installed by vendor packages. It is recommended to prefix all filenames with a two-digit number and a dash, to simplify the ordering of the files.

If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to `/dev/null` in the configuration directory in `/etc/`, with the same filename as the vendor configuration file. If the vendor configuration file is included in the initrd image, the image has to be regenerated.

3.3.1 Ensure source routed packets are not accepted (Automated)

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`, `net.ipv4.conf.default.accept_source_route`, `net.ipv6.conf.all.accept_source_route` and `net.ipv6.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

# grep "net\.ipv4\.conf\.all\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.conf.all.accept_source_route= 0

# grep "net\.ipv4\.conf\.default\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*

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

IF IPv6 is enabled:
Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0

# sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0

# grep "net\.ipv6\.conf\.all\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.conf.all.accept_source_route= 0

# grep "net\.ipv6\.conf\.default\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv6.conf.default.accept_source_route= 0
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

IF IPv6 is enabled:
Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

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

Run the following commands to set the active kernel parameters:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.2 Ensure ICMP redirects are not accepted (Automated)

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` and `net.ipv6.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

# grep "net\.ipv4\.conf\.all\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.conf.all.accept_redirects= 0

# grep "net\.ipv4\.conf\.default\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

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

IF IPv6 is enabled:
Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_redirects

net.ipv6.conf.all.accept_redirects = 0

# sysctl net.ipv6.conf.default.accept_redirects

net.ipv6.conf.default.accept_redirects = 0

# grep "net\.ipv6\.conf\.all\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv6.conf.all.accept_redirects= 0

# grep "net\.ipv6\.conf\.default\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

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

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

IF IPv6 is enabled:
Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.3 Ensure secure ICMP redirects are not accepted (Automated)

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

# grep "net\.ipv4\.conf\.all\.secure_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.conf.all.secure_redirects= 0

# grep "net\.ipv4\.conf\.default\.secure_redirects" /etc/sysctl.conf
/etc/sysctl.d/*

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

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.4 Ensure suspicious packets are logged (Automated)

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

# grep "net\.ipv4\.conf\.all\.log_martians" /etc/sysctl.conf /etc/sysctl.d/*

net.ipv4.conf.all.log_martians = 1

# grep "net\.ipv4\.conf\.default\.log_martians" /etc/sysctl.conf
/etc/sysctl.d/*

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

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

3.3.5 Ensure broadcast ICMP requests are ignored (Automated)

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

# grep "net\.ipv4\.icmp_echo_ignore_broadcasts" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.6 Ensure bogus ICMP responses are ignored (Automated)

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

# grep "net.ipv4.icmp_ignore_bogus_error_responses" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.7 Ensure Reverse Path Filtering is enabled (Automated)

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

# grep "net\.ipv4\.conf\.all\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*

net.ipv4.conf.all.rp_filter = 1

# grep "net\.ipv4\.conf\.default\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*

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

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.8 Ensure TCP SYN Cookies is enabled (Automated)

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

# grep "net\.ipv4\.tcp_syncookies" /etc/sysctl.conf /etc/sysctl.d/*

net.ipv4.tcp_syncookies = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3.9 Ensure IPv6 router advertisements are not accepted (Automated)

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 do 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:

IF IPv6 is enabled:
Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_ra

net.ipv6.conf.all.accept_ra = 0

# sysctl net.ipv6.conf.default.accept_ra

net.ipv6.conf.default.accept_ra = 0

# grep "net\.ipv6\.conf\.all\.accept_ra" /etc/sysctl.conf /etc/sysctl.d/*

net.ipv6.conf.all.accept_ra = 0

# grep "net\.ipv6\.conf\.default\.accept_ra" /etc/sysctl.conf /etc/sysctl.d/*

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

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

IF IPv6 is enabled:
Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` 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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.4 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.

3.4.1 Ensure DCCP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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 a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/dccp.conf`
Add the following line:

```
install dccp /bin/true
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.4.2 Ensure SCTP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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 | grep -E '(sctp|install)'

install /bin/true

# lsmod | grep sctp

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/sctp.conf`
and add the following line:

```
install sctp /bin/true
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.4.3 Ensure RDS is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - 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 a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/rds.conf`
and add the following line:

```
install rds /bin/true
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.4.4 Ensure TIPC is disabled (Automated)

Profile Applicability:

- Level 2 - Server

- Level 2 - 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 | grep -E '(tipc|install)'

install /bin/true

# lsmod | grep tipc

<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vi /etc/modprobe.d/tipc.conf`
and add the following line:

```
install tipc /bin/true
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

3.5 Firewall Configuration

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through

To provide a Host Based Firewall, the Linux kernel includes support for:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem. *Is available in Linux kernels 3.13 and newer*.

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- UncomplicatedFirewall (ufw) - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. `ufw` supports both IPv4 and IPv6 networks
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip_tables, ip6_tables, arp_tables, and ebtables kernel modules.

Notes:

- *Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results*
- *This section is intended only to ensure the resulting firewall rules are in place, not how they are configured*

3.5.1 Configure UncomplicatedFirewall

If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration
- Rules are processed until first matching rule. The first matching rule will be applied.

Notes:

- *Configuration of a live system's firewall directly over a remote connection will often result in being locked out*
- *Rules should be ordered so that `ALLOW` rules come before `DENY` rules.*

3.5.1.1 Ensure ufw is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Uncomplicated Firewall (ufw) is a frontend for iptables and is particularly well-suited for host-based firewalls. ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall

Rationale:

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Note: Only one firewall utility should be installed and configured. *`UFW`* *is dependent on the iptables package*

Audit:

Run the following command to verify that Uncomplicated Firewall (UFW) is installed:

```
# dpkg -s ufw | grep 'Status: install'

Status: install ok installed
```

Remediation:

Run the following command to install Uncomplicated Firewall (UFW):

```
apt install ufw
```

CIS Controls:

Version 7

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

3.5.1.2 Ensure iptables-persistent is not installed with ufw (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-persistent` is a boot-time loader for netfilter rules, iptables plugin

Rationale:

Running both `ufw` and the services included in the iptables-persistent package may lead to conflict

Audit:

Run the following command to verify that the `iptables-persistent` package is not installed:

```
dpkg-query -s iptables-persistent

package 'iptables-persistent' is not installed and no information is
available
```

Remediation:

Run the following command to remove the `iptables-persistent` package:

```
# apt purge iptables-persistent
```

CIS Controls:

Version 7

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

3.5.1.3 Ensure ufw service is enabled (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.

Notes:

- *When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.*
- *Run the following command before running `ufw enable`.*

```
# ufw allow proto tcp from any to any port 22
```

- *The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)*
- *By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using `ufw --force enable`*

Rationale:

The ufw service must be enabled and running in order for ufw to protect the system

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command to verify that ufw is enabled:

```
# systemctl is-enabled ufw

enabled
```

Run the following command to verify that ufw is running:

```
# ufw status | grep Status

Status: active
```

Remediation:

Run the following command to enable ufw:

```
# ufw enable
```

References:

1. http://manpages.ubuntu.com/manpages/precise/en/man8/ufw.8.html

CIS Controls:

Version 7

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

3.5.1.4 Ensure ufw loopback traffic is configured (Automated)

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 for IPv4 and ::1/128 for IPv6).

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 for IPv4 and ::1/128 for IPv6) 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:

```
# ufw status verbose

To                           Action      From
--                           ------      ----
Anywhere on lo               ALLOW IN    Anywhere
Anywhere                     DENY IN     127.0.0.0/8
Anywhere (v6) on lo          ALLOW IN    Anywhere (v6)
Anywhere (v6)                DENY IN     ::1

Anywhere                     ALLOW OUT   Anywhere on lo
Anywhere (v6)                ALLOW OUT   Anywhere (v6) on lo
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ufw allow in on lo
# ufw allow out on lo
# ufw deny in from 127.0.0.0/8
# ufw deny in from ::1
```

CIS Controls:

Version 7

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

3.5.1.5 Ensure ufw outbound connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound connections.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system.*
- *Unlike iptables, when a new outbound rule is added, ufw automatically takes care of associated established connections, so no rules for the latter kind are required.*

Rationale:

If rules are not in place for new outbound 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 connections match site policy:

```
# ufw status numbered
```

Remediation:

Configure ufw in accordance with site policy. The following commands will implement a policy to allow all outbound connections on all interfaces:

```
# ufw allow out on all
```

CIS Controls:

Version 7

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

3.5.1.6 Ensure ufw firewall rules exist for all open ports (Manual)

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.

Notes:

- *Changing firewall settings while connected over network can result in being locked out of the system*
- *The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy*

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:

```
# ss -4tuln

Netid                State                  Recv-Q                 Send-Q
Local Address:Port                                   Peer Address:Port
udp                  UNCONN                 0                      0
127.0.0.53%lo:53                                          0.0.0.0:*
udp                  UNCONN                 0                      0
10.105.106.117%enp1s0:68                                          0.0.0.0:*
tcp                  LISTEN                 0                      128
127.0.0.53%lo:53                                          0.0.0.0:*
tcp                  LISTEN                 0                      128
0.0.0.0:22                                          0.0.0.0:*
```

Run the following command to determine firewall rules:

```
# ufw status verbose

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] Anywhere on lo             ALLOW IN    Anywhere
[ 2] Anywhere                   ALLOW OUT   Anywhere on lo             (out)
[ 3] Anywhere                   DENY IN     127.0.0.0/8
[ 4] 22/tcp                     ALLOW IN    Anywhere
[ 5] Anywhere                   ALLOW OUT   Anywhere on enp1s0         (out)
[ 6] Anywhere                   ALLOW OUT   Anywhere on all            (out)
[ 7] Anywhere (v6) on lo        ALLOW IN    Anywhere (v6)
[ 8] Anywhere (v6)              ALLOW OUT   Anywhere (v6) on lo        (out)
[ 9] Anywhere (v6)              DENY IN     ::1
[10] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[11] Anywhere (v6)              ALLOW OUT   Anywhere (v6) on all       (out)
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.
Lines identified by indexes 4 and 10 are firewall rules 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:

```
# ufw allow in <port>/<tcp or udp protocol>
```

CIS Controls:

Version 7

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

3.5.1.7 Ensure ufw default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny policy on connections ensures that any unconfigured network usage will be rejected.

Note: Any port or protocol without a explicit allow before the default deny will be blocked

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.

Impact:

Any port and protocol not explicitly allowed will be blocked. The following rules should be considered before applying the default deny.

```
ufw allow git

ufw allow in http

ufw allow in https

ufw allow out 53

ufw logging on
```

Audit:

Run the following command and verify that the default policy for **incoming** , **outgoing** , and **routed** directions is **deny** or **reject**:

```
# ufw status verbose
```

Remediation:

Run the following commands to implement a default *deny* policy:

```
# ufw default deny incoming

# ufw default deny outgoing

# ufw default deny routed
```

CIS Controls:

Version 7

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

3.5.2 Configure nftables

If Uncomplicated Firewall (UFW) or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. Please ensure that your kernel supports nf_tables before choosing this option.

Notes:

- *This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset).*
- *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 will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.

Save the script bellow as `/etc/nftables.rules`

```
#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/nftables.rules
# flush nftables rulesset
flush ruleset
# Load nftables ruleset
# nftables config with inet table named filter
table inet filter {
        # Base chain for input hook named input (Filters inbound network
packets)
        chain input {
                type filter hook input priority 0; policy drop;

                # Ensure loopback traffic is configured
                iif "lo" accept
                ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
                ip6 saddr ::1 counter packets 0 bytes 0 drop

                # Ensure established connections are configured
                ip protocol tcp ct state established accept
                ip protocol udp ct state established accept
                ip protocol icmp ct state established accept

                # Accept port 22(SSH) traffic from anywhere
                tcp dport ssh accept

                # Accept ICMP and IGMP from anywhere
                icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept
                icmp type { destination-unreachable, router-advertisement,
router-solicitation, time-exceeded, parameter-problem } accept
                ip protocol igmp accept
        }

        # Base chain for hook forward named forward (Filters forwarded
network packets)
        chain forward {
                type filter hook forward priority 0; policy drop;
        }

        # Base chain for hook output named output (Filters outbount network
packets)
        chain output {
                type filter hook output priority 0; policy drop;
                # Ensure outbound and established connections are configured
                ip protocol tcp ct state established,related,new accept
                ip protocol udp ct state established,related,new accept
                ip protocol icmp ct state established,related,new accept
        }
}
```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables.rules
```

All changes in the nftables subsections are temporary.

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables.rules
```

Add the following line to `/etc/nftables.conf`

```
include "/etc/nftables.rules"
```

3.5.2.1 Ensure nftables is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

Notes:

- *nftables is available in Linux kernel 3.13 and newer*
- *Only one firewall utility should be installed and configured*
- *Changing firewall settings while connected over the network can result in being locked out of the system*

Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Audit:

Run the following command to verify that `nftables` is installed:

```
# dpkg-query -s nftables | grep 'Status: install ok installed'

Status: install ok installed
```

Remediation:

Run the following command to install `nftables`:

```
# apt install nftables
```

CIS Controls:

Version 7

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

3.5.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

Rationale:

Running both the `nftables` service and `ufw` may lead to conflict and unexpected results.

Audit:

Run the following commands to verify that `ufw` is *either* not installed or inactive. *Only one of the following needs to pass.*
Run the following command to verify that `ufw` is not installed:

```
# dpkg-query -s ufw | grep 'Status: install ok installed'

 package 'ufw' is not installed and no information is available
```

Run the following command to verify ufw is disabled:

```
# ufw status

Status: inactive
```

Remediation:

Run *one* of the following commands to either remove `ufw` or disable `ufw`
Run the following command to remove `ufw`:

```
# apt purge ufw
```

Run the following command to disable `ufw`:

```
# ufw disable
```

CIS Controls:

Version 7

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

3.5.2.3 Ensure iptables are flushed with nftables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Audit:

Run the following commands to ensure no iptables rules exist
For iptables:

```
# iptables -L
```

No rules should be returned
For ip6tables:

```
# ip6tables -L
```

No rules should be returned

Remediation:

Run the following commands to flush iptables:
For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

CIS Controls:

Version 7

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

3.5.2.4 Ensure a nftables table exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Audit:

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:
Example:

```
table inet filter
```

Remediation:

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

CIS Controls:

Version 7

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

3.5.2.5 Ensure nftables base chains exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Impact:

If configuring nftables over ssh, `creating` a `base chain` with a policy of `drop` will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains exist for `INPUT`.

```
# nft list ruleset | grep 'hook input'

type filter hook input priority 0;
```

Run the following commands and verify that base chains exist for `FORWARD`.

```
# nft list ruleset | grep 'hook forward'

type filter hook forward priority 0;
```

Run the following commands and verify that base chains exist for `OUTPUT`.

```
# nft list ruleset | grep 'hook output'

type filter hook output priority 0;
```

Remediation:

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook
<(input|forward|output)> priority 0 \; }
```

Example:

```
# nft create chain inet filter input { type filter hook input priority 0 \; }

# nft create chain inet filter forward { type filter hook forward priority 0
\; }

# nft create chain inet filter output { type filter hook output priority 0 \;
}
```

CIS Controls:

Version 7

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

3.5.2.6 Ensure nftables loopback traffic is configured (Automated)

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

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 traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands to verify that the loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'

iif "lo" accept

# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'

ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
```

IF IPv6 is enabled on the system:
Run the following command to verify that the IPv6 loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'

ip6 saddr ::1 counter packets 0 bytes 0 drop
```

Remediation:

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept

# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

IF IPv6 is enabled on the system:
Run the following command to implement the IPv6 loopback rule:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

CIS Controls:

Version 7

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

3.5.2.7 Ensure nftables outbound and established connections are configured (Manual)

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 commands and verify all rules for established incoming connections match site policy: site policy:

```
# nft list ruleset | awk '/hook input/,/}/' | grep -E 'ip protocol
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept
```

Run the folllowing command and verify all rules for new and established outbound connections match site policy

```
# nft list ruleset | awk '/hook output/,/}/' | grep -E 'ip protocol
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established,related,new accept
ip protocol udp ct state established,related,new accept
ip protocol icmp ct state established,related,new accept
```

Remediation:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# nft add rule inet filter input ip protocol tcp ct state established accept

# nft add rule inet filter input ip protocol udp ct state established accept

# nft add rule inet filter input ip protocol icmp ct state established accept

# nft add rule inet filter output ip protocol tcp ct state
new,related,established accept

# nft add rule inet filter output ip protocol udp ct state
new,related,established accept

# nft add rule inet filter output ip protocol icmp ct state
new,related,established accept
```

CIS Controls:

Version 7

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

3.5.2.8 Ensure nftables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to `accept`, the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Impact:

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Audit:

Run the following commands and verify that base chains contain a policy of `DROP`.

```
# nft list ruleset | grep 'hook input'

type filter hook input priority 0; policy drop;

# nft list ruleset | grep 'hook forward'

type filter hook forward priority 0; policy drop;

# nft list ruleset | grep 'hook output'

type filter hook output priority 0; policy drop;
```

Remediation:

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

```
# nft chain <table family> <table name> <chain name> { policy drop \; }
```

Example:

```
# nft chain inet filter input { policy drop \; }

# nft chain inet filter forward { policy drop \; }

# nft chain inet filter output { policy drop \; }
```

Default Value:

accept

References:

1. Manual Page nft

CIS Controls:

Version 7

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

3.5.2.9 Ensure nftables service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the `/etc/nftables.conf` file during boot or the starting of the nftables service

Audit:

Run the following command and verify that the nftables service is enabled:

```
# systemctl is-enabled nftables

enabled
```

Remediation:

Run the following command to enable the nftables service:

```
# systemctl enable nftables
```

CIS Controls:

Version 7

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

3.5.2.10 Ensure nftables rules are permanent (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Audit:

Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot:
Run the following command to verify the input base chain:

```
# [ -n "$(grep -E '^\s*include' /etc/nftables.conf)" ] && awk '/hook
input/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print $2 }'
/etc/nftables.conf)
```

Output should be similar to:

```
                type filter hook input priority 0; policy drop;

                # Ensure loopback traffic is configured
                iif "lo" accept
                ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
                ip6 saddr ::1 counter packets 0 bytes 0 drop

                # Ensure established connections are configured
                ip protocol tcp ct state established accept
                ip protocol udp ct state established accept
                ip protocol icmp ct state established accept

                # Accept port 22(SSH) traffic from anywhere
                tcp dport ssh accept

                # Accept ICMP and IGMP from anywhere
                icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept
```

Review the input base chain to ensure that it follows local site policy
Run the following command to verify the forward base chain:

```
# [ -n "$(grep -E '^\s*include' /etc/nftables.conf)" ] && awk '/hook
forward/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print $2 }'
/etc/nftables.conf)
```

Output should be similar to:

```
        # Base chain for hook forward named forward (Filters forwarded
network packets)
        chain forward {
                type filter hook forward priority 0; policy drop;
        }
```

Review the forward base chain to ensure that it follows local site policy.
Run the following command to verify the forward base chain:

```
# [ -n "$(grep -E '^\s*include' /etc/nftables.conf)" ] && awk '/hook
output/,/}/' $(awk '$1 ~ /^\s*include/ { gsub("\"","",$2);print $2 }'
/etc/nftables.conf)
```

Output should be similar to:

```
        # Base chain for hook output named output (Filters outbound network
packets)
        chain output {
                type filter hook output priority 0; policy drop;
                # Ensure outbound and established connections are configured
                ip protocol tcp ct state established,related,new accept
                ip protocol tcp ct state established,related,new accept
                ip protocol udp ct state established,related,new accept
                ip protocol icmp ct state established,related,new accept
        }
```

Review the output base chain to ensure that it follows local site policy.

Remediation:

Edit the `/etc/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot
Example:

```
# vi /etc/nftables.conf
```

Add the line:

```
include "/etc/nftables.rules"
```

CIS Controls:

Version 7

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

3.5.3 Configure iptables

If Uncomplicated Firewall (UFW) or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

IPtables is an application that allows a system administrator to configure the IPv4 and IPv6 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: Configuration of a live system's firewall directly over a remote connection will often result in being locked out

3.5.3.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

3.5.3.1.1 Ensure iptables packages are installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Audit:

Run the following command to verify that `iptables` and `iptables-persistent` are installed:

```
# apt list iptables iptables-persistent | grep installed

iptables-persistent/<version> [installed,automatic]
iptables/<version> [installed,automatic]
```

Remediation:

Run the following command to install `iptables` and `iptables-persistent`

```
# apt install iptables iptables-persistent
```

CIS Controls:

Version 7

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

3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

Rationale:

Running both `iptables` and `nftables` may lead to conflict.

Audit:

Run the following commend to verify that nftables is not installed:

```
#  dpkg -s nftables

dpkg-query: package 'nftables' is not installed
```

Remediation:

Run the following command to remove `nftables`:

```
# apt purge nftables
```

CIS Controls:

Version 7

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

3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.

- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration

Rationale:

Running `iptables.persistent` with ufw enabled may lead to conflict and unexpected results.

Audit:

Run the following commands to verify that `ufw` is *either* not installed or disabled. *Only one of the following needs to pass.*
Run the following command to verify that `ufw` is not installed:

```
# dpkg-query -s ufw

 package 'ufw' is not installed and no information is available
```

Run the following command to verify ufw is disabled:

```
# ufw status

Status: inactive
```

Run the following commands to verify that the `ufw` service is masked:

```
# systemctl is-enabled ufw

masked
```

Remediation:

Run *one* of the following commands to either remove `ufw` or stop and mask `ufw`
Run the following command to remove `ufw`:

```
# apt purge ufw
```

OR
Run the following commands to disable `ufw`:

```
# ufw disable
```

CIS Controls:

Version 7

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

3.5.3.2 Configure IPv4 iptables

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

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
```

3.5.3.2.1 Ensure iptables default deny firewall policy (Automated)

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.

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*

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
```

CIS Controls:

Version 7

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

3.5.3.2.2 Ensure iptables loopback traffic is configured (Automated)

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).

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*

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
```

CIS Controls:

Version 7

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

3.5.3.2.3 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established connections.

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*

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
```

CIS Controls:

Version 7

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

3.5.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated)

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.

Note:

- 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

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:

```
# ss -4tuln

Netid  State      Recv-Q Send-Q    Local Address:Port                   Peer
Address:Port
udp    UNCONN     0      0                     *:68
*:*
udp    UNCONN     0      0                     *:123
*:*
tcp    LISTEN     0      128                   *:22
*:*
```

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
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

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

3.5.3.3 Configure IPv6 ip6tables

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

If IPv6 in enabled on the system, the ip6tables should be configured.

Note: This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -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 ip6tables rules
ip6tables -F

# Ensure default deny firewall policy
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Ensure loopback traffic is configured
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT
ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.5.3.3.1 Ensure ip6tables default deny firewall policy (Automated)

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.

Note:

- 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

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:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

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

3.5.3.3.2 Ensure ip6tables loopback traffic is configured (Automated)

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 (::1).

Note:

- 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

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 (::1) 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):

```
# ip6tables -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 DROP       all      *       *       ::1                  ::/0


# ip6tables -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
```

OR verify IPv6 is disabled:
Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s ::1 -j DROP
```

CIS Controls:

Version 7

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

3.5.3.3.3 Ensure ip6tables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Note:

- 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

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:

```
# ip6tables -L -v -n
```

OR verify IPv6 is disabled:
Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

CIS Controls:

Version 6

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

Version 7

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

3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated)

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.

Note:

- 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

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:

```
# ss -6tuln

Netid  State      Recv-Q Send-Q    Local Address:Port                   Peer
Address:Port
udp    UNCONN     0      0                   ::1:123
:::*
udp    UNCONN     0      0                    :::123
:::*
tcp    LISTEN     0      128                  :::22
:::*
tcp    LISTEN     0      20                  ::1:25
:::*
```

Run the following command to determine firewall rules:

```
# ip6tables -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 DROP       all      *      *       ::1                  ::/0
    0     0 ACCEPT     tcp      *      *       ::/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.
OR verify IPv6 is disabled:
Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/bash

output=""
grubfile="$(find -L /boot -name 'grub.cfg' -type f)"
[ -f "$grubfile" ] && ! grep "^\s*linux" "$grubfile" | grep -vq
ipv6.disable=1 && output="ipv6 disabled in grub config"
grep -Eqs "^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf \
/run/sysctl.d/*.conf && grep -Eqs
"^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" /etc/sysctl.conf
/etc/sysctl.d/*.conf \
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf && sysctl
net.ipv6.conf.all.disable_ipv6 | grep -Eq \
"^\s*net\.ipv6\.conf\.all\.disable_ipv6\s*=\s*1\b" && sysctl
net.ipv6.conf.default.disable_ipv6 | \
grep -Eq "^\s*net\.ipv6\.conf\.default\.disable_ipv6\s*=\s*1\b" &&
output="ipv6 disabled in sysctl config"
[ -n "$output" ] && echo -e  "\n$output" || echo -e "\n*** IPv6 is enabled on
the system ***"
```

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

CIS Controls:

Version 7

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

4 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.

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 AppArmor 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.

Notes:

- *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*
- *Audit rules that have `arch`as a rule parameter:*
    - *On 64 bit systems, you will need two rules, one for 64 bit and one for 32 bit*
    - *On 32 bit systems, only the 32 bit rule is needed*
- *Several recommendations in this section filter based off of `auid>=1000` for unprivileged non-system users. Some systems may have a non-default UID_MIN setting, consult the `UID_MIN` setting in `/etc/login.defs` to determine the UID_MIN setting for your system*
- *The audits in this section look for a `key` value. The `key value` may be different for the audit rules on your system. If a different `key` value, denoted by `-k` or `key=` is used on your system, please replace the `grep <key_value>` with the `key value` in use on your system*
- *Once all audit rules have been added to a file or files in the `/etc/audit/rules.d/` directory, the auditd service must be re-started, or the system rebooted, for the new rules to be included*

4.1.1 Ensure auditing is enabled

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

4.1.1.1 Ensure auditd is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command and verify auditd is installed:

```
# dpkg -s auditd audispd-plugins
```

Remediation:

Run the following command to Install auditd

```
# apt install auditd audispd-plugins
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.1.1.2 Ensure auditd service is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Enable and start the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd

enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `auditd` :

```
# systemctl --now enable auditd
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)

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.

Note: 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/grub.cfg` with the appropriate grub configuration file for your environment.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

Run the following command and verify that each linux line has the `audit=1` parameter set:

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "audit=1"
```

Nothing should be returned

Remediation:

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
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The backlog limit has a default setting of 64

Rationale:

during boot if audit=1, then the backlog will hold 64 records. If more that 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected.

Audit:

Run the following commands and verify the `audit_backlog_limit=` parameter is set to an appropriate size for your organization

```
# grep "^\s*linux" /boot/grub/grub.cfg | grep -v "audit_backlog_limit="
```

Nothing should be returned

```
# grep "audit_backlog_limit=" /boot/grub/grub.cfg
```

Ensure the the returned value complies with local site policy
Recommended that this value be `8192` or larger.

Remediation:

Edit /etc/default/grub and add `audit_backlog_limit=<BACKLOG SIZE>` to GRUB_CMDLINE_LINUX:
Example:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

Run the following command to update the grub2 configuration:

```
# update-grub
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.1.2 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.

4.1.2.1 Ensure audit log storage size is configured (Automated)

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.

Notes:

- *The max_log_file parameter is measured in megabytes*
- *Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in auditd configurations*
- *Manual audit of custom configurations should be evaluated for effectiveness and completeness*

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>
```

CIS Controls:

Version 7

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

4.1.2.2 Ensure audit logs are not automatically deleted (Automated)

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
```

CIS Controls:

Version 7

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

4.1.2.3 Ensure system is disabled when audit logs are full (Automated)

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
```

CIS Controls:

Version 7

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

4.1.3 Ensure events that modify date and time information are collected (Automated)

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"

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep time-change /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep time-change
```

Verify the output matches:

```
-a always,exit -F arch=b32 -S stime,settimeofday,adjtimex -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F key=time-change
-w /etc/localtime -p wa -k time-change
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep time-change /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep time-change
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday -F key=time-change
-a always,exit -F arch=b32 -S stime,settimeofday,adjtimex -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F key=time-change
-w /etc/localtime -p wa -k time-change
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-time-change.rules`*
Add the following lines:

```
-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 Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-time-change.rules`*
Add the following lines:

```
-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
```

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

4.1.4 Ensure events that modify user/group information are collected (Automated)

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.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep identity /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep identity
```

Verify the output matches:

```
-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:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:
Example: *`vi /etc/audit/rules.d/50-identity.rules`*
Add the following lines:

```
-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
```

CIS Controls:

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

4.1.5 Ensure events that modify the system's network environment are collected (Automated)

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/network` (directory containing network interface scripts and configurations) files.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Audit:

On a 32 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep system-locale /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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/network -p wa -k system-locale
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep system-locale
```

Verify the output matches:

```
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep system-locale /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-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/network -p wa -k system-locale
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep system-locale
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/network -p wa -k system-locale
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-system-locale.rules`*
Add the following lines:

```
-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/network -p wa -k system-locale
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-system-locale.rules`*
Add the following lines:

```
-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/network -p wa -k system-locale
```

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

4.1.6 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor 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 `/etc/apparmor` and `/etc/apparmor.d` directories.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep MAC-policy /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep MAC-policy
```

Verify output matches:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-MAC-policy.rules`*
Add the following lines:

```
-w /etc/apparmor/ -p wa -k MAC-policy
-w /etc/apparmor.d/ -p wa -k MAC-policy
```

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

4.1.7 Ensure login and logout events are collected (Automated)

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

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep logins /etc/audit/rules.d/*.rules
```

Verify output includes:

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep logins
```

Verify output includes:

```
-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:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:
Example: *`vi /etc/audit/rules.d/50-logins.rules`*
Add the following lines:

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p wa -k logins
```

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login
Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

16.13 Alert on Account Login Behavior Deviation
Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

4.1.8 Ensure session initiation information is collected (Automated)

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` tracks all currently logged in users. All audit records will be tagged with the identifier "session." The `/var/log/wtmp` file tracks logins, logouts, shutdown, and reboot events. 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."

Note:

- The `last` command can be used to read `/var/log/wtmp` (`last` with no parameters) and `/var/run/utmp` (`last -f /var/run/utmp`)
- Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep -E '(session|logins)' /etc/audit/rules.d/*.rules
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep -E '(session|logins)'
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:
Example: *`vi /etc/audit/rules.d/50-session.rules`*
Add the following lines:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
```

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login
Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

16.13 Alert on Account Login Behavior Deviation
Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

4.1.9 Ensure discretionary access control permission modification events are collected (Automated)

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 >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier "perm_mod."

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -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>=1000 -F auid!=4294967295
-k perm_mod
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -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>=1000 -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>=1000 -F auid!=4294967295
-k perm_mod
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:

Example: *`vi /etc/audit/rules.d/50-perm_mod.rules`*

Add the following lines:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -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>=1000 -F auid!=4294967295
-k perm_mod
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: *`vi /etc/audit/rules.d/50-perm_mod.rules`*

Add the following lines:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -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>=1000 -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>=1000 -F auid!=4294967295
-k perm_mod
```

Additional Information:

Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

CIS Controls:

Version 7

5.5 Implement Automated Configuration Monitoring Systems
Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

4.1.10 Ensure unsuccessful unauthorized file access attempts are collected (Automated)

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 > = 1000), 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."

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -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>=1000 -F auid!=4294967295 -k access
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-
EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -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>=1000 -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>=1000 -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>=1000 -F auid!=4294967295 -k access
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-
EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-
EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-
EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-access.rules`*
Add the following lines:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -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>=1000 -F auid!=4294967295 -k access
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-access.rules`*
Add the following lines:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -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>=1000 -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>=1000 -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>=1000 -F auid!=4294967295 -k access
```

Additional Information:

Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace audit>=1000 with audit>=<UID_MIN for your system> in the Audit and Remediation procedures.

CIS Controls:

Version 7

14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).

4.1.11 Ensure use of privileged commands is collected (Automated)

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.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing `<partition>` with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print \
"-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F auid!=4294967295 \
-k privileged" }'
```

Verify all resulting lines are a `.rules` file in `/etc/audit/rules.d/` and the output of `auditctl -l`.

Note: The `.rules` file output will be `auid!=-1` not `auid!=4294967295`

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>=1000` - 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 `key` "privileged".
Run the following command replacing with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k
privileged" }'
```

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules` and add all resulting lines to the file.
Example:

```
# find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a
always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk '/^\s*UID_MIN/{print
$2}' /etc/login.defs)"' -F auid!=4294967295 -k privileged" }' >>
/etc/audit/rules.d/50-privileged.rules
```

Additional Information:

Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace audit>=1000 with audit>=<UID_MIN for your system> in the Audit and Remediation procedures.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.1.12 Ensure successful file system mounts are collected (Automated)

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

Note:

- This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).
- Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-mounts.rules`*
Add the following lines:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-mounts.rules`*
Add the following lines:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
mounts
```

Additional Information:

Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace audit>=1000 with audit>=<UID_MIN for your system> in the Audit and Remediation procedures.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.1.13 Ensure file deletion events by users are collected (Automated)

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".

Note:

- At a minimum, configure the audit system to collect file deletion events for all users and root.
- Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -
F auid!=-1 -F key=delete
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/50-delete.rules`
Add the following lines:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/50-delete.rules`
Add the following lines:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=1000 -F auid!=4294967295 -k delete
```

Additional Information:

Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace audit>=1000 with audit>=<UID_MIN for your system> in the Audit and Remediation procedures.

CIS Controls:

Version 7

13 Data Protection
Data Protection

4.1.14 Ensure changes to system administration scope (sudoers) is collected (Automated)

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."

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:

```
# grep scope /etc/audit/rules.d/*.rules

# auditctl -l | grep scope
```

Verify output of both matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-scope.rules`*
Add the following lines:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

CIS Controls:

Version 7

4.8 Log and Alert on Changes to Administrative Group Membership
Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

4.1.15 Ensure system administrator command executions (sudo) are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`sudo` provides users with temporary elevated privileges to perform operations. Monitor the administrator with temporary elevated privileges and the operation(s) they performed.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

Rationale:

creating an audit log of administrators with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo logfile` to verify if unauthorized commands have been executed.

Audit:

On a 32 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
/etc/audit/rules.d/cis.rules:-a exit,always -F arch=b32 -C euid!=uid -F
euid=0 -Fauid>=1000 -F auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F
auid!=-1 -F key=actions
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
-a exit,always -F arch=b64 -C euid!=uid -F euid=0 -Fauid>=1000 -F
auid!=4294967295 -S execve -k actions
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -Fauid>=1000 -F
auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F
auid!=-1 -F key=actions
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F
auid!=-1 -F key=actions
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:
Example: `vi /etc/audit/rules.d/50-actions.rules
Add the following line:

```
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -Fauid>=1000 -F
auid!=4294967295 -S execve -k actions
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:
Example: `vi /etc/audit/rules.d/50-actions.rules`
Add the following lines:

```
-a always,exit -F arch=b64 -C euid!=uid -F euid=0 -Fauid>=1000 -F
auid!=4294967295 -S execve -k actions
-a always,exit -F arch=b32 -C euid!=uid -F euid=0 -Fauid>=1000 -F
auid!=4294967295 -S execve -k actions
```

CIS Controls:

Version 7

4.9 Log and Alert on Unsuccessful Administrative Account Login
Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

4.1.16 Ensure kernel module loading and unloading is collected (Automated)

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".

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a system reboot.

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 commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module,delete_module -F key=modules
```

On a 64 bit system run the following commands:
Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module,delete_module -F key=modules
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-modules.rules`*
Add the following lines:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: *`vi /etc/audit/rules.d/50-modules.rules`*
Add the following lines:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.1.17 Ensure the audit configuration is immutable (Automated)

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.

Note: Reloading the auditd config to set active settings requires the auditd service to be restarted, and may require a 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/rules.d/*.rules | tail -1

-e 2
```

Remediation:

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the line

```
-e 2
```

at the end of the file

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

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 is installed (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

The `rsyslog` software is a recommended replacement 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` 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. Use the following command to provide the needed information:

```
# dpkg -s rsyslog
```

Remediation:

Install rsyslog:

```
# apt install rsyslog
```

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.2.1.2 Ensure rsyslog Service is enabled (Automated)

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:

```
# systemctl is-enabled rsyslog
```

Verify result is `enabled`.

Remediation:

Run the following commands to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

Additional Information:

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

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.2.1.3 Ensure logging is configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files 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 and /etc/rsyslog.d/*.conf files as appropriate for your environment:

```
*.emerg                                  :omusrmsg:*
auth,authpriv.*                          /var/log/auth.log
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 reload the `rsyslog` configuration:

```
# systemctl reload rsyslog
```

References:

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

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.2.1.4 Ensure rsyslog default file permissions configured (Automated)

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 every instance of `$FileCreateMode` is `0640` or more restrictive:

```
# grep ^\s*\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

If `$FileCreateMode` is not found, the default value 0644 is used and at least one `$FileCreateMode` has to be added.

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and set every instance of `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

References:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)

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

Note: Ensure that the selection of logfiles being sent follows local site policy

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host.

```
# grep -E '^\s*([^#]+\s+)?action\(([^#]+\s+)?\btarget=\"?[^#"]+\"?\b'
/etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `target=<FQDN or IP of remote loghost>`
OR

```
# grep -E '^[^#]\s*\S+\.\*\s+@' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include either the FQDN or the IP of the remote loghost

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add one of the following lines:
Newer syntax:

```
<files to sent to the remote log server> action(type="omfwd" target="<FQDN or
ip of loghost>" port="<port number>" protocol="tcp"

action.resumeRetryCount="<number of re-tries>"
                                              queue.type="LinkedList"
queue.size=<number of messages to queue>")
```

Example:

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"
           action.resumeRetryCount="100"
           queue.type="LinkedList" queue.size="1000")
```

Older syntax:

```
*.* @@<FQDN or ip of loghost>
```

Example:

```
*.* @@192.168.2.100
```

Run the following command to reload the `rsyslog` configuration:

```
# systemctl restart rsyslog
```

References:

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

Additional Information:

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

The `*.*` is a "wildcard" to send all logs to the remote loghost

CIS Controls:

Version 7

6.6 Deploy SIEM or Log Analytic tool
Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

6.8 Regularly Tune SIEM
On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)

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.

Note: The `$ModLoad imtcp` line can have the `.so` extension added to the end of the module, or use the full path to the module

Audit:

Run the following commands: and verify the resulting lines are:

- Not commented on designated log hosts
- Commented or not present on all others

Run the following command and verify the output for `$ModLoad imtcp`

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output for designated log hosts:

```
$ModLoad imtcp
```

Output for systems that are not log hosts: *(No output is also acceptable)*

```
# $ModLoad imtcp
```

Run the following command and verify the output for `'$InputTCPServerRun`

```
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output for designated log hosts:

```
$InputTCPServerRun 514
```

Output for systems that are not log hosts: *(No output is also acceptable)*

```
# $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

$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

# $InputTCPServerRun 514
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

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

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

4.2.2 Configure journald

systemd-journald is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources: Kernel log messages, via kmsg

Any changes made to the systemd-journald configuration will require a re-start of systemd-journald

4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

Notes:

- *This recommendation assumes that recommendation 4.2.1.5, "Ensure rsyslog is configured to send logs to a remote log host" has been implemented.*
- *As noted in the journald man pages, journald logs may be exported to rsyslog either through the process mentioned here, or through a facility like* `systemd-journald.service`*. There are trade-offs involved in each implementation, where* `ForwardToSyslog` *will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as* `systemd-journald.service`*, on the other hand, will record bootup events, but may delay sending the information to rsyslog, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.*
- *The main configuration file* `/etc/systemd/journald.conf` *is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters*

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 `/etc/systemd/journald.conf` and verify that logs are forwarded to syslog

```
# grep -e ForwardToSyslog /etc/systemd/journald.conf

ForwardToSyslog=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

References:

1. https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

CIS Controls:

Version 7

6.5 Central Log Management
Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

4.2.2.2 Ensure journald is configured to compress large log files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Note: The main configuration file `/etc/systemd/journald.conf` *is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters*

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Audit:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep -e Compress /etc/systemd/journald.conf

Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

References:

1. https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

CIS Controls:

Version 7

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

4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss.

Note: The main configuration file `/etc/systemd/journald.conf` *is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters*

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Audit:

Review `/etc/systemd/journald.conf` and verify that logs are persisted to disk:

```
# grep -e Storage /etc/systemd/journald.conf

Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

References:

1. https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.2.3 Ensure permissions on all logfiles are configured (Automated)

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.

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

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 commands to set permissions on all existing log files:

```
find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-
w,o-rwx "{}" +
```

CIS Controls:

Version 7

13 Data Protection
Data Protection

4.3 Ensure logrotate is configured (Manual)

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 unmanageably large. The file `/etc/logrotate.d/rsyslog` is the configuration file used to rotate log files created by `rsyslog`.

Note: If no `maxage` setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.

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/rsyslog` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/rsyslog` to ensure logs are rotated according to site policy.

CIS Controls:

Version 7

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

4.4 Ensure logrotate assigns appropriate permissions (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files 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:

```
# grep -Es "^\s*create\s+\S+" /etc/logrotate.conf /etc/logrotate.d/* | grep -
E -v "\s(0)?[0-6][04]0\s"

Nothing should be returned
```

Remediation:

Edit `/etc/logrotate.conf` and update the `create` line to read 0640 or more restrictive, following local site policy
Example:

```
create 0640 root utmp
```

CIS Controls:

Version 7

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

5 Access, Authentication and Authorization

5.1 Configure time-based job schedulers

`cron` is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

`at` provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Notes:

- *Other methods exist for scheduling jobs, such as `systemd timers`. If another method is used, it should be secured in accordance with local site policy*
- *`systemd timers` are systemd unit files whose name ends in `.timer` that control `.service` files or events*
  - *Timers can be used as an alternative to `cron` and `at`*
  - *Timers have built-in support for calendar time events, monotonic time events, and can be run asynchronously*
- *If `cron` and `at` are not installed, this section can be skipped*

5.1.1 Ensure cron daemon is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `cron` daemon is used to execute batch jobs on the system.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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:

Run the following command to verify `cron` is enabled:

```
# systemctl is-enabled cron

enabled
```

Run the following command to verify that `cron` is running:

```
# systemctl status cron | grep 'Active: active (running) '

Active: active (running) since <Day Date Time>
```

Remediation:

Run the following command to enable and start `cron`:

```
# systemctl --now enable cron
```

CIS Controls:

Version 7

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 (Automated)

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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
```

CIS Controls:

Version 7

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

5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.hourly` directory:

```
# chown root:root /etc/cron.hourly/

# chmod og-rwx /etc/cron.hourly/
```

CIS Controls:

Version 7

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

5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)

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.

Note: Other methods, such as systemd timers, exist for scheduling jobs. If another method is used, cron should be removed, and the alternate method should be secured in accordance with local site policy

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: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on the /etc/cron.daily directory:

```
# chown root:root /etc/cron.daily/

# chmod og-rwx /etc/cron.daily/
```

CIS Controls:

Version 7

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

5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/

# chmod og-rwx /etc/cron.weekly/
```

CIS Controls:

Version 7

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

5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/

# chmod og-rwx /etc/cron.monthly/
```

CIS Controls:

Version 7

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

5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)

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.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

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: (0700/drwx------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/

# chmod og-rwx /etc/cron.d/
```

CIS Controls:

Version 7

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

5.1.8 Ensure cron is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure `/etc/cron.allow` to allow specific users to use this service. If `/etc/cron.allow` does not exist, then `/etc/cron.deny` is checked. Any user not specifically defined in this file is allowed to use cron. By removing the file, only users in `/etc/cron.allow` are allowed to use cron.

Notes:

- *Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy*
- *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 command and verify that `/etc/cron.deny` does not exist:

```
# stat /etc/cron.deny

stat: cannot stat `/etc/cron.deny': No such file or directory
```

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access`, does not grant write or execute to group, and does not grant permissions to `other` for`/etc/cron.allow`:

```
# stat /etc/cron.allow

Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to remove `/etc/cron.deny`:

```
# rm /etc/cron.deny
```

Run the following command to create `/etc/cron.allow`

```
# touch /etc/cron.allow
```

Run the following commands to set permissions and ownership for `/etc/cron.allow`:

```
# chmod g-wx,o-rwx /etc/cron.allow

# chown root:root /etc/cron.allow
```

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

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

5.1.9 Ensure at is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure `/etc/at.allow` to allow specific users to use this service. If `/etc/at.allow` does not exist, then `/etc/at.deny` is checked. Any user not specifically defined in this file is allowed to use `at`. By removing the file, only users in `/etc/at.allow` are allowed to use `at`.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `at` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

On many systems, only the system administrator is authorized to schedule `at` jobs. Using the `at.allow` file to control who can run `at` 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 command and verify that `/etc/at.deny` does not exist:

```
# 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 write or execute to group, and does not grant permissions to `other` for`/etc/at.allow`:

```
# stat /etc/at.allow

Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to remove `/etc/at.deny`:

```
# rm /etc/at.deny
```

Run the following command to create `/etc/at.allow`

```
# touch /etc/at.allow
```

Run the following commands to set permissions and ownership for `/etc/at.allow`:

```
# chmod g-wx,o-rwx /etc/at.allow

# chown root:root /etc/at.allow
```

CIS Controls:

Version 7

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

5.2 Configure sudo

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

5.2.1 Ensure sudo is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

Note: Use the sudo-ldap package if you need LDAP support for sudoers

Rationale:

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

Audit:

Verify that sudo in installed.
Run the following command and inspect the output to confirm that sudo is installed:

```
# dpkg -s sudo
```

OR

```
# dpkg -s sudo-ldap
```

Remediation:

Install sudo using the following command.

```
# apt install sudo
```

OR

```
# apt install sudo-ldap
```

References:

1. SUDO(8)
2. http://www.sudo.ws/

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

5.2.2 Ensure sudo commands use pty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can be configured to run only from a pseudo-pty

Note: visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Rationale:

Attackers can run a malicious program using sudo, which would again fork a background process that remains even when the main program has finished executing.

Audit:

Verify that sudo can only run other commands from a pseudo-pty
Run the following command:

```
# grep -Ei '^\s*Defaults\s+([^#]+,\s*)?use_pty(,\s+\S+\s*)*(\s+#.*)?$'
/etc/sudoers /etc/sudoers.d/*
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with visudo -f and add the following line:

```
Defaults use_pty
```

References:

1. SUDO(8)

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

5.2.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server

- Level 1 - Workstation

Description:

sudo can use a custom log file.

Note: visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Rationale:

A sudo log file simplifies auditing of sudo commands

Audit:

Verify that sudo has a custom log file configured
Run the following command:

```
# grep -Ei '^\s*Defaults\s+logfile=\S+' /etc/sudoers /etc/sudoers.d/*
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with visudo -f and add the following line: and add the following line:

```
Defaults  logfile="<PATH TO CUSTOM LOG FILE>"
```

Example:

```
Defaults  logfile="/var/log/sudo.log"
```

CIS Controls:

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.3 Configure SSH Server

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.
  - *Command to remove the SSH daemon:*
  - `# apt purge openssh-server`
- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:
  - *Command to re-load the SSH daemon configuration:*
  - `# systemctl reload sshd`

5.3.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

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.

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
```

Default Value:

Access: (0600/-rw-------) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Version 7

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

5.3.2 Ensure permissions on SSH private host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, The possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Audit:

Run the following command and verify Uid is 0/root and Gid is 0/root and permissions are `0600` or more restrictive:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;
```

Example Output:

```
  File: /etc/ssh/ssh_host_rsa_key
  Size: 1679            Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 8388989     Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-03-02 13:40:55.591022871 +0000
Modify: 2021-02-18 16:59:09.338020640 +0000
Change: 2021-02-18 16:59:09.338020640 +0000
 Birth: -
  File: /etc/ssh/ssh_host_dsa_key
  Size: 668             Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 8420538     Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-02-18 16:59:09.442020643 +0000
Modify: 2021-02-18 16:59:09.442020643 +0000
Change: 2021-02-18 16:59:09.442020643 +0000
 Birth: -
  File: /etc/ssh/ssh_host_ecdsa_key
  Size: 227             Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 8421198     Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-03-02 13:40:55.595022900 +0000
Modify: 2021-02-18 16:59:09.446020643 +0000
Change: 2021-02-18 16:59:09.446020643 +0000
 Birth: -
  File: /etc/ssh/ssh_host_ed25519_key
  Size: 411             Blocks: 8          IO Block: 4096   regular file
Device: 802h/2050d      Inode: 8421406     Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2021-03-02 13:40:55.595022900 +0000
Modify: 2021-02-18 16:59:09.454020644 +0000
Change: 2021-02-18 16:59:09.454020644 +0000
 Birth: -
```

Remediation:

Run the following commands to set permissions, ownership, and group on the private SSH host key files:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,go-rwx
{} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {}
\;
```

CIS Controls:

Version 7

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

5.3.3 Ensure permissions on SSH public host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec stat {} \;
```

Example Output:

```
  File: ‘/etc/ssh/ssh_host_rsa_key.pub’
  Size: 382             Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631758     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.881750616 +0000
 Birth: -
  File: ‘/etc/ssh/ssh_host_ecdsa_key.pub’
  Size: 162             Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631761     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.917750616 +0000
 Birth: -
  File: ‘/etc/ssh/ssh_host_ed25519_key.pub’
  Size: 82              Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631763     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.961750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set permissions and ownership on the SSH host public key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod u-x,go-
wx {} \;
#find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root
{} \;
```

CIS Controls:

Version 7

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

5.3.4 Ensure SSH access is limited (Automated)

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 space 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 space 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 space 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 space 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 command:

```
sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Ei
'^\s*(allow|deny)(users|groups)\s+\S+'
```

Verify that the output matches at least one of the following lines:

```
allowusers <userlist>
allowgroups <grouplist>
denyusers <userlist>
denygroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <grouplist>
```

Default Value:

None

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

5.3.5 Ensure SSH LogLevel is appropriate (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`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.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

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.

Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep loglevel

loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -i 'loglevel' /etc/ssh/sshd_config | grep -Evi '(VERBOSE|INFO)'

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

OR

```
LogLevel INFO
```

Default Value:

LogLevel INFO

References:

1. https://www.ssh.com/ssh/sshd_config/

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.3.6 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through an existing SSH shell session 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.

Impact:

X11 programs on the server will not be able to be forwarded to a ssh-client display.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i x11forwarding

x11forwarding no
```

Run the following command and verify that the output matches:

```
# grep -Ei '^\s*x11forwarding\s+yes' /etc/ssh/sshd_config

Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

Default Value:

X11Forwarding yes

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

5.3.7 Ensure SSH MaxAuthTries is set to 4 or less (Automated)

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep maxauthtries

maxauthtries 4
```

Run the following command and verify that the output:

```
# grep -Ei '^\s*maxauthtries\s+([5-9]|[1-9][0-9]+)' /etc/ssh/sshd_config

Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

MaxAuthTries 6

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

16.13 Alert on Account Login Behavior Deviation
Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

5.3.8 Ensure SSH IgnoreRhosts is enabled (Automated)

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep ignorerhosts

ignorerhosts yes
```

Run the following command and verify the output:

```
# grep -Ei '^\s*ignorerhosts\s+no\b' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

IgnoreRhosts yes

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

5.3.9 Ensure SSH HostbasedAuthentication is disabled (Automated)

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep hostbasedauthentication

hostbasedauthentication no
```

Run the following command and verify the output matches:

```
# grep -Ei '^\s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

HostbasedAuthentication no

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

5.3.10 Ensure SSH root login is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh. 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`. 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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep permitrootlogin

permitrootlogin no
```

Run the following command and verify the output:

```
# grep -Ei '^\s*PermitRootLogin\s+yes' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

PermitRootLogin without-password

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

5.3.11 Ensure SSH PermitEmptyPasswords is disabled (Automated)

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep permitemptypasswords

permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Ei '^\s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

PermitEmptyPasswords no

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

5.3.12 Ensure SSH PermitUserEnvironment is disabled (Automated)

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 a Trojan's programs)

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permituserenvironment

permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Ei '^\s*PermitUserEnvironment\s+yes' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.3.13 Ensure only strong Ciphers are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the ciphers that SSH can use during communication.

Note: Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack
- The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue
- The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Ei '^\s*ciphers\s+([^#]+,)?(3des-
cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-
cbc|cast128-cbc|rijndael-cbc@lysator.liu.se)\b'

Nothing should be returned
```

Run the following command and verify the output:

```
grep -Ei '^\s*ciphers\s+([^#]+,)?(3des-cbc|aes128-cbc|aes192-cbc|aes256-
cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbc|rijndael-
cbc@lysator.liu.se)\b' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers
Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

References:

1. https://nvd.nist.gov/vuln/detail/CVE-2016-2183
2. https://nvd.nist.gov/vuln/detail/CVE-2015-2808
3. https://www.kb.cert.org/vuls/id/565052
4. https://www.openssh.com/txt/cbc.adv
5. https://nvd.nist.gov/vuln/detail/CVE-2008-5161
6. https://nvd.nist.gov/vuln/detail/CVE-2013-4548
7. https://www.kb.cert.org/vuls/id/565052
8. https://www.openssh.com/txt/cbc.adv
9. SSHD_CONFIG(5)

Additional Information:

Weak Ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The Following are ciphers supported by openSSH v7.6p1:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

"Strong" ciphers currently FIPS 140-2 approved:

```
aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-
ctr
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.3.14 Ensure only strong MAC algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable Specifies the available MAC (message authentication code) algorithms. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated.

Note: Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.

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 the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Ei '^\s*macs\s+([^#]+,)?(hmac-
md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|hmac-sha1-96|umac-
64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-
ripemd160-etm@openssh\.com|hmac-sha1-etm@openssh\.com|hmac-sha1-96-
etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com)\b'

Nothing should be returned
```

Run the following command and verify the output:

```
# grep -Ei '^\s*macs\s+([^#]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-
sha1|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-
etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-
etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-
128-etm@openssh\.com)\b' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site approved MACs
Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-
512,hmac-sha2-256
```

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

References:

1. More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH
2. SSHD_CONFIG(5)

Additional Information:

Weak MAC algorithms:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

MAC algorithms supported by openSSH v7.6p1:

```
hmac-md5
hmac-md5-96
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

"Strong" MAC algorithms currently FIPS 140-2 approved:

```
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-
256,hmac-sha2-512
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

5.3.15 Ensure only strong Key Exchange algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Ei
'^\s*kexalgorithms\s+([^#]+,)?(diffie-hellman-group1-sha1|diffie-hellman-
group14-sha1|diffie-hellman-group-exchange-sha1)\b'

Nothing should be returned
```

Run the following command and verify the output:

```
# grep -Ei '^\s*kexalgorithms\s+([^#]+,)?(diffie-hellman-group1-sha1|diffie-
hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\b'
/etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms
Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-
nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-
sha256
```

Default Value:

kexalgorithms diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

References:

1. SSHD_CONFIG(5)

Additional Information:

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

Key Exchange algorithms supported by OpenSSH 7.6p1:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

"Strong" Key Exchange Algorithms currently FIPS 140-2 approved:

```
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-
group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-
sha512,diffie-hellman-group14-sha256
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.3.16 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions.

- `ClientAliveInterval` sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. The default value is `3`.
  - The client alive messages are sent through the encrypted channel
  - Setting `ClientAliveCountMax` to `0` disables connection termination

Example: The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds

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 reduces this risk.

- The recommended `ClientAliveInterval` setting is no greater than `900` seconds (15 minutes)
- The recommended `ClientAliveCountMax` setting is `0`
- At the 15 minute interval, if the ssh session is inactive, the session will be terminated.

Impact:

In some cases this setting may cause termination of long-running scripts over SSH or remote automation tools which rely on SSH. In developing the local site policy, the requirements of such scripts should be considered and appropriate ServerAliveInterval and ClientAliveInterval settings should be calculated to insure operational continuity.

Audit:

Run the following commands and verify `ClientAliveInterval` is between `1` and `900`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep clientaliveinterval

clientaliveinterval 900
```

Run the following command and verify `ClientAliveCountMax` is `0`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep clientalivecountmax

clientalivecountmax 3
```

Run the following commands and verify the output:

```
# grep -Ei '^\s*ClientAliveInterval\s+(0|9[0-9][1-9]|[1-9][0-9][0-9][0-
9]+|1[6-9]m|[2-9][0-9]m|[1-9][0-9][0-9]+m)\b' /etc/ssh/sshd_config

Nothing should be returned

# grep -Ei '^\s*ClientAliveCountMax\s+([1-9]|[1-9][0-9]+)\b'
/etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters according to site policy. This should include `ClientAliveInterval` between `1` and `900` and `ClientAliveCountMax` of `0`:

```
ClientAliveInterval 900

ClientAliveCountMax 0
```

Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

References:

1. https://man.openbsd.org/sshd_config

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

5.3.17 Ensure SSH LoginGraceTime is set to one minute or less (Automated)

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 between `1` and `60` seconds or `1m`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep logingracetime

logingracetime 60
```

Run the following command and verify the output:

```
# grep -Ei '^\s*LoginGraceTime\s+(0|6[1-9]|[7-9][0-9]|[1-9][0-9][0-
9]+|[^1]m)' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

LoginGraceTime 2m

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.3.18 Ensure SSH warning banner is configured (Automated)

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:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep banner

banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.3.19 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

UsePAM Enables the Pluggable Authentication Module interface. If set to “yes” this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication in addition to PAM account and session module processing for all authentication types

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Impact:

If UsePAM is enabled, you will not be able to run sshd(5) as a non-root user.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i usepam

usepam yes
```

Run the following command and verify the output:

```
# grep -Ei '^\s*UsePAM\s+no' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
UsePAM yes
```

Default Value:

usePAM yes

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.3.20 Ensure SSH AllowTcpForwarding is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines

Rationale:

Leaving port forwarding enabled can expose the organization to security risks and back-doors.

SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network

Impact:

SSH tunnels are widely used in many corporate environments that employ mainframe systems as their application backends. In those environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding

allowtcpforwarding no
```

Run the following command and verify the output:

```
# grep -Ei '^\s*AllowTcpForwarding\s+yes' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
AllowTcpForwarding no
```

Default Value:

AllowTcpForwarding yes

References:

1. https://www.ssh.com/ssh/tunneling/example
2. SSHD_CONFIG(5)

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

13.5 Monitor and Detect Any Unauthorized Use of Encryption
Monitor all traffic leaving the organization and detect any unauthorized use of encryption.

5.3.21 Ensure SSH MaxStartups is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i maxstartups

maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Ei '^\s*maxstartups\s+(((1[1-9]|[1-9][0-9][0-9]+):([0-9]+):([0-
9]+))|(([0-9]+):(3[1-9]|[4-9][0-9]|[1-9][0-9][0-9]+):([0-9]+))|(([0-9]+):([0-
9]+):(6[1-9]|[7-9][0-9]|[1-9][0-9][0-9]+)))' /etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
maxstartups 10:30:60
```

Default Value:

MaxStartups 10:30:100

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.3.22 Ensure SSH MaxSessions is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter Specifies the maximum number of open sessions permitted per network connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxSessions` is `10` or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -i maxsessions

maxsessions 10
```

Run the following command and verify the output:

```
grep -Ei '^\s*MaxSessions\s+(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+)'
/etc/ssh/sshd_config

Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxSessions 10
```

Default Value:

MaxSessions 10

References:

1. SSHD_CONFIG(5)

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

5.4 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.

5.4.1 Ensure password creation requirements are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `pam_pwquality.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_pwquality.so` options.

The following options are set in the `/etc/security/pwquality.conf` file:

- Password Length:
  - `minlen = 14` - password must be 14 characters or more
- Password complexity:
  - `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)

    OR

  - `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 following is st in the `/etc/pam.d/common-password` file:

- `retry=3` - Allow 3 tries before sending back a failure. 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 conform to organization policy.
Run the following command to verify the minimum password length is 14 or more characters.

```
# grep '^\s*minlen\s*' /etc/security/pwquality.conf

minlen = 14
```

Run one of the following commands to verify the required password complexity:

```
# grep '^\s*minclass\s*' /etc/security/pwquality.conf

minclass = 4
```

OR

```
# grep -E '^\s*[duol]credit\s*' /etc/security/pwquality.conf

dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

Run the following command to verify the number of attempts allowed before sending back a failure are no more than 3

```
# grep -E
'^\s*password\s+(requisite|required)\s+pam_pwquality\.so\s+(\S+\s+)*retry=[1-
3]\s*(\s+\S+\s*)*(\s+#.*)?$' /etc/pam.d/common-password

password        requisite                       pam_pwquality.so retry=3
```

Remediation:

Run the following command to install the pam_pwquality module:

```
apt install libpam-pwquality
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

OR

```
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Edit the `/etc/pam.d/common-password` file to include the appropriate options for `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so retry=3
```

Additional Information:

Additional module options may be set, recommendation requirements only cover including `try_first_pass` and `minlen` set to 14 or more.

Settings in `/etc/security/pwquality.conf` must use spaces around the `=` symbol.

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.4.2 Ensure lockout for failed password attempts is configured (Automated)

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.

- deny=`n` - `n` represents the number of failed attempts before the account is locked
- unlock_time=`n` - `n` represents the number of seconds before the account is unlocked
- audit - Will log the user name into the system log if the user is not found.
- silent - Don't print informative messages. Set the lockout number and unlock time in accordance with local site policy.

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` modules found in `/etc/pam.d/common-auth`:

```
# grep "pam_tally2" /etc/pam.d/common-auth

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

Verify the pam_deny.so module and pam_tally2.so modules are included in `/etc/pam.d/common-account`:

```
# grep -E "pam_(tally2|deny)\.so" /etc/pam.d/common-account

account requisite                        pam_deny.so
account required                         pam_tally2.so
```

Remediation:

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

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

Edit the `/etc/pam.d/common-account` file and add the account lines bellow:

```
account     requisite    pam_deny.so
account     required     pam_tally2.so
```

Additional Information:

- Add pam_tally2 to the account section `account required pam_tally2.so` for the counter to reset to 0 when using sudo
- Use of the "audit" keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.
- If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` module, the user can be unlocked by issuing the command `/sbin/pam_tally2 -u <username> --reset`. This command sets the failed count to 0, effectively unlocking the user.

CIS Controls:

Version 7

16.7 Establish Process for Revoking Access

Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

5.4.3 Ensure password reuse is limited (Automated)

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.

Audit:

Run the following commands and ensure the `remember` option is '`5`' or more and included in all results:

```
# grep -E
'^\s*password\s+required\s+pam_pwhistory\.so\s+([^#]+\s+)?remember=([5-9]|[1-
9][0-9]+)\b' /etc/pam.d/common-password

password required pam_pwhistory.so remember=5
```

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `remember` option and conform to site policy as shown:

```
password required pam_pwhistory.so remember=5
```

Additional Information:

Changes only apply to accounts configured on the local system.

CIS Controls:

Version 7

16 <u>Account Monitoring and Control</u>
Account Monitoring and Control

5.4.4 Ensure password hashing algorithm is SHA-512 (Automated)

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:

Run the following commands and ensure the sha512 option is included in all results:

```
# grep -E
'^\s*password\s+(\[success=1\s+default=ignore\]|required)\s+pam_unix\.so\s+([
^#]+\s+)?sha512\b' /etc/pam.d/common-password
```

Output should be similar to:

```
password        [success=1 default=ignore]      pam_unix.so obscure sha512
```

Remediation:

Edit the `/etc/pam.d/common-password` file to include the `sha512` option for `pam_unix.so` as shown:

```
password [success=1 default=ignore] pam_unix.so sha512
```

Additional Information:

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

The following command can be used:

```
# awk -F: '( $3 >= $(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs) && $1 !=
"nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

5.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.5.1 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.

5.5.1.1 Ensure minimum days between password changes is configured (Automated)

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 1 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` conforms to site policy (no less than 1 day):

```
# grep PASS_MIN_DAYS /etc/login.defs

PASS_MIN_DAYS 1
```

Run the following command and Review list of users and PAS_MIN_DAYS to Verify that all users' PAS_MIN_DAYS conforms to site policy (no less than 1 day):

```
# awk -F : '(/^[^:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow

No <user>:<PASS_MIN_DAYS> should be returned
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 1 in `/etc/login.defs` :

```
PASS_MIN_DAYS 1
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 1 <user>
```

Default Value:

PASS_MIN_DAYS 0

CIS Controls:

Version 6

16 Account Monitoring and Control
Account Monitoring and Control

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.5.1.2 Ensure password expiration is 365 days or less (Automated)

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.

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. It is recommended that the PASS_MAX_DAYS parameter does not exceed 365 days and is greater than the value of PASS_MIN_DAYS.

Audit:

Run the following command and verify PASS_MAX_DAYS conforms to site policy, does not exceed 365 days, and is greater than PASS_MIN_DAYS:

```
# grep PASS_MAX_DAYS /etc/login.defs

PASS_MAX_DAYS 365
```

Run the following command and Review list of users and PASS_MAX_DAYS to verify that all users' PASS_MAX_DAYS conforms to site policy, does not exceed 365 days, and is no less than PASS_MIN_DAYS

```
# awk -F: '(/^[^:]+:[^!*]/ && ($5>365 || $5~/([0-1]|-1|\s*)/)){print $1 " "
$5}' /etc/shadow

No <user>:<PASS_MAX_DAYS> should be returned
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs` :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

Default Value:

PASS_MAX_DAYS 99999

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Additional Information:

A value of -1 will disable password expiration

The password expiration `must be greater than the minimum days between password changes` or users will be unable to change their password

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.5.1.3 Ensure password expiration warning days is 7 or more (Automated)

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 conforms to site policy (No less than 7 days):

```
# 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:
Run the following command and Review list of users and PASS_WARN_AGE to verify that all users' PASS_WARN_AGE conforms to site policy (No less than 7 days):

```
# awk -F: '(/^[^:]+:[^!*]/ && $6<7){print $1 " " $6}' /etc/shadow

No <user>:<PASS_WARN_AGE> should be returned
```

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>
```

Default Value:

PASS_WARN_AGE 7

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.5.1.4 Ensure inactive password lock is 30 days or less (Automated)

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` conforms to sire policy (no more than 30 days):

```
# useradd -D | grep INACTIVE

INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:
Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}'
/etc/shadow

No <user>:<INACTIVE> should be returned
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.5.1.5 Ensure all users last password change date is in the past (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

All users should have a password change date in the past.

Rationale:

If a users recorded password change date is in the future then they could bypass any set password expiration.

Audit:

Run the following command and verify nothing is returned

```
#  awk -F : '/^[^:]+:[^!*]/{print $1}' /etc/shadow | while read -r usr; do [
"$(date --date="$(chage --list "$usr" | grep '^Last password change' | cut -
d: -f2)" +%s)" -gt "$(date "+%s")" ] && echo "user: $usr password change
date: $(chage --list "$usr" | grep '^Last password change' | cut -d: -f2)";
done
```

Remediation:

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

5.5.2 Ensure system accounts are secured (Automated)

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 the `nologin` shell. This prevents the account from potentially being used to run any commands.

Audit:

Run the following commands and verify no results are returned:

```
# awk -F: '$1!~/(root|sync|shutdown|halt|^\+)/ && $3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' &&
$7!~/((\/usr)?\/sbin\/nologin)/ && $7!~/(\/bin)?\/false/ {print}' /etc/passwd

# awk -F: '($1!~/(root|^\+)/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!~/LK?/) {print $1}'
```

Note: The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell

Remediation:

Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non-root accounts returned by the audit:

```
# usermod -L <user>
```

The following command will set all system accounts to a non login shell:

```
# awk -F: '$1!~/(root|sync|shutdown|halt|^\+)/ && $3<'"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' &&
$7!~/((\/usr)?\/sbin\/nologin)/ && $7!~/(\/bin)?\/false/ {print $1}'
/etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user";
done
```

The following command will automatically lock not root system accounts:

```
# awk -F: '($1!~/(root|^\+)/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!~/LK?/) {print $1}' | while read -r user; do usermod -L "$user";
done
```

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

5.5.3 Ensure default group for the root account is GID 0 (Automated)

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
```

CIS Controls:

Version 7

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

5.5.4 Ensure default user umask is 027 or more restrictive (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The user file-creation mode mask (`umask`) is use to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (rwxrwxrwx), and for any newly created file it is 0666 (rw-rw-rw-). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either `octal` or `Symbolic` values

- `Octal` (Numeric) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx,g=rx,o=` is the `Symbolic` equivalent of the `Octal` `umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

Setting the default `umask`:

- `pam_umask` module:
  - will set the umask according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to `yes` in `/etc/login.defs` (default):
    - will enable setting of the umask group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the primary group name
    - userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user

- System Wide Shell Configuration File:
    - /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the .profile, however this file is used to set an initial PATH or PS1 for all shell users of the system. *is only executed for interactive login shells, or shells executed with the --login parameter*
    - /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh. It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.
    - /etc/bash.bashrc - System wide version of .bashrc. etc/bashrc also invokes /etc/profile.d/*.sh if non-login shell, but redirects output to /dev/null if non-interactive. *Is only executed for interactive shells or if BASH_ENV is set to /etc/bash.bashrc*

User Shell Configuration Files:

- ~/.profile - Is executed to configure your shell before the initial command prompt. *Is only read by login shells.*
- ~/.bashrc - Is executed for interactive shells. *only read by a shell that's both interactive and non-login*

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.

Impact:

Setting **USERGROUPS_ENAB no** in /etc/login.defs may change the expected behavior of useradd and userdel.

Setting **USERGROUPS_ENAB yes** in /etc/login.defs

- userdel will remove the user's group if it contains no more members
- useradd will create by default a group with the name of the user.

Audit:

Run the following to verify:

- A default user umask is set to enforce a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive
- No less restrictive System Wide `umask` is set

Run the following script to verify that a default user umask is set enforcing a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive:

```
#!/bin/bash

passing=""
grep -Eiq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && grep
-Eqi '^\s*USERGROUPS_ENAB\s*"?no"?\b' /etc/login.defs && grep -Eq
'^\s*session\s+(optional|requisite|required)\s+pam_umask\.so\b'
/etc/pam.d/common-session && passing=true
grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-
7]7|u=(r?|w?|x?)(r?|w?|x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile*
/etc/bash.bashrc* && passing=true
[ "$passing" = true ] && echo "Default user umask is set"
```

Verify output is: "Default user umask is set"
Run the following to verify that no less restrictive system wide umask is set:

```
# grep -RPi '(^|^[^#]*)\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-
6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-
6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(
,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*

No file should be returned
```

Remediation:

Run the following command and remove or modify the `umask` of any returned files:

```
# grep -RPi '(^|^[^#]*)\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-
6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-
6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(
,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*
```

Follow **one** of the following methods to set the default user umask:
Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

```
UMASK 027

USERGROUPS_ENAB no
```

Edit `/etc/pam.d/common-session` and add or edit the following:

```
session optional                        pam_umask.so
```

OR
Configure umask in one of the following files:

- A file in the `/etc/profile.d/` directory ending in .sh
- `/etc/profile`
- `/etc/bash.bashrc`

Example: *`/etc/profile.d/set_umask.sh`*

```
umask 027
```

Note: this method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Default Value:

UMASK 022

References:

1. pam_umask(8)

Additional Information:

- Other methods of setting a default user `umask` exist
- If other methods are in use in your environment they should be audited
- The default user `umask` can be overridden with a user specific `umask`
- The user creating the directories or files has the discretion of changing the permissions:
  - Using the `chmod` command
  - Setting a different default `umask` by adding the `umask` command into a `User Shell Configuration File`, (`.bashrc`), in their home directory
  - Manually changing the umask for the duration of a login session by running the `umask` command

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

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

5.5.5 Ensure default user shell timeout is 900 seconds or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- TMOUT=*n* - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- export TMOUT - exports the TMOUT variable

`System Wide Shell Configuration Files:`

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. *is only executed for interactive login shells, or shells executed with the --login parameter.*
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bash.bashrc` - System wide version of `bash.bashrc`. `etc/bash.bashrc` also invokes /etc/profile.d/*.sh if *non-login* shell, but redirects output to `/dev/null` if *non-interactive. Is only executed for interactive shells or if `BASH_ENV` is set to `/etc/bash.bashrc`.*

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

Audit:

Run the following commands to verify that `TMOUT` is configured to include a timeout of no more than `900` seconds, to be `readonly`, and to be `exported`:
Run the following command to verify that `TMOUT` is configured in: a `.sh` file in `/etc/profile.d/`, in `/etc/profile`, or in `/etc/bash.bashrc`:

```
# for f in /etc/bash.bashrc /etc/profile /etc/profile.d/*.sh ; do grep -Eq
'(^|^[^#]*;)\s*(readonly|export(\s+[^$#;]+\s*)*)?\s*TMOUT=(900|[1-8][0-9][0-
9]|[1-9][0-9]|[1-9])\b' $f && grep -Eq '(^|^[^#]*;)\s*readonly\s+TMOUT\b' $f
&& grep -Eq '(^|^[^#]*;)\s*export\s+([^$#;]+\s+)*TMOUT\b' $f && echo "TMOUT
correctly configured in file: $f"; done

TMOUT correctly configured in file: <name of file where TMOUT is configured>
```

Run the following command to verify that `TMOUT` is not being changed to a longer timeout:

```
# grep -P '^\s*([^$#;]+\s+)*TMOUT=(9[0-9][1-9]|0+|[1-
9]\d{3,})\b\s*(\S+\s*)*(\s+#.*)?$' /etc/profile /etc/profile.d/*.sh
/etc/bash.bashrc

Nothing should be returned
```

Remediation:

Review `/etc/bash.bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy. `TMOUT` should not exceed 900 or be equal to `0`.
Configure `TMOUT` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bash.bashrc`

`TMOUT` configuration examples:

- As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

Additional Information:

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 are also checked

Other methods of setting a timeout exist not covered here

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

5.6 Ensure root login is restricted to system console (Manual)

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.

CIS Controls:

Version 7

4.3 Ensure the Use of Dedicated Administrative Accounts
Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

5.7 Ensure access to the su command is restricted (Automated)

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 adding, or uncommenting, the `pam_wheel.so` statement in `/etc/pam.d/su` , the `su` command will only allow users in a specific group to execute `su`. This group should be empty to reinforce the use of `sudo` for privileged access.

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 the output matches the line:

```
# grep pam_wheel.so /etc/pam.d/su

auth required pam_wheel.so use_uid group=<group_name>
```

Run the following command and verify that the group specified in `<group_name>` contains no users:

```
# grep <group_name> /etc/group

<group_name>:x:<GID>:
```

There should be no users listed after the Group ID field.

Remediation:

Create an empty group that will be specified for use of the `su` command. The group should be named according to site policy.
Example:

```
# groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:
Example:

```
auth required pam_wheel.so use_uid group=sugroup
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

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 (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The Debian package manager has a number of useful options. One of these, the `--verify` 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 `dpkg -S` command can be used to determine which package a particular file belongs to. For example the following command determines which package the `/bin/bash` file belongs to:

```
# dpkg -S /bin/bash

bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# dpkg --verify bash

??5?????? c /etc/bash.bashrc
```

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 assessed 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.*

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 the following command 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.

```
# dpkg --verify <package name>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

CIS Controls:

Version 7

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

6.1.2 Ensure permissions on /etc/passwd are configured (Automated)

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 u-x,go-wx /etc/passwd
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.3 Ensure permissions on /etc/passwd- are configured (Automated)

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 `644` or more restrictive:

```
# 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 u-x,go-wx /etc/passwd-
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.4 Ensure permissions on /etc/group are configured (Automated)

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 u-x,go-wx /etc/group
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.5 Ensure permissions on /etc/group- are configured (Automated)

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 `644` or more restrictive:

```
# 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 u-x,go-wx /etc/group-
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.6 Ensure permissions on /etc/shadow are configured (Automated)

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 **one** of the following commands to set ownership of /etc/shadow to root and group to either root or shadow:

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

Run the following command to remove excess permissions form /etc/shadow:

```
# chmod u-x,g-wx,o-rwx /etc/shadow
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.7 Ensure permissions on /etc/shadow- are configured (Automated)

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 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: (   42/  shadow)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/shadow-` to `root` and group to either `root` or `shadow`:

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

Run the following command to remove excess permissions form `/etc/shadow-`:

```
# chmod u-x,g-wx,o-rwx /etc/shadow-
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.8 Ensure permissions on /etc/gshadow are configured (Automated)

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 `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: (   42/  shadow)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/gshadow` to `root` and group to either `root` or `shadow`:

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

Run the following command to remove excess permissions form `/etc/gshadow`:

```
# chmod u-x,g-wx,o-rwx /etc/gshadow
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.9 Ensure permissions on /etc/gshadow- are configured (Automated)

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` 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: (   42/  shadow)
```

Remediation:

Run **one** of the following commands to set ownership of `/etc/gshadow-` to `root` and group to either `root` or `shadow`:

```
# chown root:root /etc/gshadow-
# chown root:shadow /etc/gshadow-
```

Run the following command to remove excess permissions form `/etc/gshadow-`:

```
# chmod u-x,g-wx,o-rwx /etc/gshadow-
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.1.10 Ensure no world writable files exist (Automated)

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.

CIS Controls:

Version 7

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

6.1.11 Ensure no unowned files or directories exist (Automated)

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.

CIS Controls:

Version 7

13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization
Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

6.1.12 Ensure no ungrouped files or directories exist (Automated)

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.

CIS Controls:

Version 7

13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization
Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

6.1.13 Audit SUID executables (Manual)

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.1.14 Audit SGID executables (Manual)

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.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2 User and Group Settings

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

Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Local accounts can uses shadowed passwords. With shadowed passwords, The passwords are saved in shadow password file, `/etc/shadow`, encrypted by a salted one-way hash. Accounts with a shadowed password have an `x` in the second field in `/etc/passwd`.

Rationale:

The `/etc/passwd` file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the `/etc/passwd` file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the `/etc/passwd` file. This can be mitigated by using shadowed passwords, thus moving the passwords in the `/etc/passwd` file to `/etc/shadow`. The `/etc/shadow` file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

Notes:

- *All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.*
- *A user account with an empty second field in `/etc/passwd` allows the account to be logged into by providing only the username.*

Audit:

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

```
# awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}'
/etc/passwd
```

Remediation:

Run the following command to set accounts to use shadowed passwords:

```
# sed -e 's/^\([a-zA-Z0-9_]*\):[^:]*:/\1:x:/' -i /etc/passwd
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.2.2 Ensure password fields are not empty (Automated)

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:

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

Remediation:

If any accounts in the `/etc/shadow` file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

CIS Controls:

Version 7

4.4 Use Unique Passwords
Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

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.

CIS Controls:

Version 7

16.6 Maintain an Inventory of Accounts
Maintain an inventory of all accounts organized by authentication system.

16.7 Establish Process for Revoking Access
Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

16.8 Disable Any Unassociated Accounts
Disable any account that cannot be associated with a business process or business owner.

6.2.4 Ensure all users' home directories exist (Automated)

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.

Note: The audit script checks all users with interactive shells except `halt`, `sync`, `shutdown`, and `nfsnobody`

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

awk -F: '($1!~/(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
        if [ ! -d "$dir" ]; then
                echo "User: \"$user\" home directory: \"$dir\" 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.
The following script will create a home directory for users with an interactive shell whose home directory doesn't exist:

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ ! -d "$dir" ]; then
    mkdir "$dir"
    chmod g-w,o-wrx "$dir"
    chown "$user" "$dir"
  fi
done
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2.5 Ensure users own their home directories (Automated)

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

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $1 " " $6 }' | while read -r
user dir; do
  if [ ! -d "$dir" ]; then
    echo "User: \"$user\" home directory: \"$dir\" does not exist."
  else
   owner=$(stat -L -c "%U" "$dir")
   if [ "$owner" != "$user" ]; then
     echo "User: \"$user\" home directory: \"$dir\" 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.
The following script will create missing home directories, set the owner, and set the permissions for interactive users' home directories:

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $1 " " $6 }' | while read -r
user dir; do
  if [ ! -d "$dir" ]; then
    echo "User: \"$user\" home directory: \"$dir\" does not exist, creating
home directory"
    mkdir "$dir"
    chmod g-w,o-rwx "$dir"
    chown "$user" "$dir"
  else
    owner=$(stat -L -c "%U" "$dir")
    if [ "$owner" != "$user" ]; then
      chmod g-w,o-rwx "$dir"
      chown "$user" "$dir"
    fi
  fi
done
```

CIS Controls:

Version 7

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

6.2.6 Ensure users' home directories permissions are 750 or more restrictive (Automated)

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

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) {print $1 " " $6}' /etc/passwd | while
read -r user dir; do
  if [ ! -d "$dir" ]; then
    echo "User: \"$user\" home directory: \"$dir\" doesn't exist"
  else
    dirperm=$(stat -L -c "%A" "$dir")
    if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
      echo "User: \"$user\" home directory: \"$dir\" has permissions:
\"$(stat -L -c "%a" "$dir")\""
    fi
  fi
done
```

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.
The following script can be used to remove permissions is excess of `750` from users' home directories:

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) {print $6}' /etc/passwd | while read -r
dir; do
  if [ -d "$dir" ]; then
    dirperm=$(stat -L -c "%A" "$dir")
    if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
      chmod g-w,o-rwx "$dir"
    fi
  fi
done
```

CIS Controls:

Version 7

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

6.2.7 Ensure users' dot files are not group or world writable (Automated)

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

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $1 " " $6 }' /etc/passwd | while
read -r user dir; do
  if [ -d "$dir" ]; then
    for file in "$dir"/.*; do
      if [ ! -h "$file" ] && [ -f "$file" ]; then
        fileperm=$(stat -L -c "%A" "$file")
        if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
          echo "User: \"$user\" file: \"$file\" has permissions:
\"$fileperm\""
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.
The following script will remove excessive permissions on `dot` files within interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $1 " " $6 }' | while read -r
user dir; do
  if [ -d "$dir" ]; then
    for file in "$dir"/.*; do
      if [ ! -h "$file" ] && [ -f "$file" ]; then
        fileperm=$(stat -L -c "%A" "$file")
        if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
          chmod go-w "$file"
        fi
      fi
    done
  fi
done
```

CIS Controls:

Version 7

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

6.2.8 Ensure no users have .netrc files (Automated)

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.

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Note: While the complete removal of `.netrc` files is recommended, if any are required on the system secure permissions must be applied.

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.

If a `.netrc` file is required, and follows local site policy, it should have permissions of `600` or more restrictive.

Audit:

Run the following script. This script will return:

- `FAILED:` for any `.netrc` file with permissions less restrictive than `600`
- `WARNING:` for any `.netrc` files that exist in interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $1 " " $6 }' /etc/passwd | while
read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.netrc"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      if stat -L -c "%A" "$file" | cut -c4-10 |  grep -Eq '[^-]+'; then
        echo "FAILED: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file or excessive
permissions"
      else
        echo "WARNING: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file unless required"
      fi
    fi
  fi
done
```

Verify:

- Any lines beginning with `FAILED:` - File should be removed unless deemed necessary, in accordance with local site policy, and permissions are updated to be `600` or more restrictive
- Any lines beginning with `WARNING:` - File should be removed unless deemed necessary, and in accordance with local site policy

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 local site policy.
The following script will remove `.netrc` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/(halt|sync|shutdown)/ && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/
&& $7!~/(\/usr)?\/bin\/false(\/)?$/) { print $6 }'  /etc/passwd | while read
-r dir; do
  if [ -d "$dir" ]; then
    file="$dir/.netrc"
    [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
  fi
done
```

CIS Controls:

Version 7

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

6.2.9 Ensure no users have .forward files (Automated)

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 lines are returned:

```
#!/bin/bash

awk -F: '($1!~/(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.forward"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.
The following script will remove `.forward` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
  if [ -d "$dir" ]; then
    file="$dir/.forward"
    [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
  fi
done
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2.10 Ensure no users have .rhosts files (Automated)

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 lines are returned:

```
#!/bin/bash

awk -F: '($1!~/(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.rhosts"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.rhosts` files and determine the action to be taken in accordance with site policy.
The following script will remove `.rhosts` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/(root|halt|sync|shutdown)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/(\/usr)?\/bin\/false(\/)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
  if [ -d "$dir" ]; then
    file="$dir/.rhosts"
    [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
  fi
done
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.2.11 Ensure root is the only UID 0 account (Automated)

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:

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

root
```

Remediation:

Remove any users other than `root` with UID `0` or assign them a new UID if appropriate.

CIS Controls:

Version 7

4.6 Use of Dedicated Machines For All Administrative Tasks
Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.

6.2.12 Ensure root PATH Integrity (Automated)

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

RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"
echo "$RPCV" | grep -q "::" && echo "root's path contains a empty directory
(::)"
echo "$RPCV" | grep -q ":$" && echo "root's path contains a trailing (:)"
for x in $(echo "$RPCV" | tr ":" " "); do
   if [ -d "$x" ]; then
      ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working
directory (.)"}
      $3 != "root" {print $9, "is not owned by root"}
      substr($1,6,1) != "-" {print $9, "is group writable"}
      substr($1,9,1) != "-" {print $9, "is world writable"}'
   else
      echo "$x is not a directory"
   fi
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

6.2.13 Ensure no duplicate UIDs exist (Automated)

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

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    users=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs)
    echo "Duplicate UID ($2): $users"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.2.14 Ensure no duplicate GIDs exist (Automated)

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

cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.2.15 Ensure no duplicate user names exist (Automated)

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

cut -d: -f1 /etc/passwd | sort | uniq -d | while read -r x; do
  echo "Duplicate login name $x in /etc/passwd"
done
```

Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.2.16 Ensure no duplicate group names exist (Automated)

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

cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
  echo "Duplicate group name $x in /etc/group"
done
```

Remediation:

Based on the results of the 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.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.2.17 Ensure shadow group is empty (Automated)

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: -v GID="$(awk -F: '($1=="shadow") {print $3}' /etc/group)"
'($4==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.

CIS Controls:

Version 7

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

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 (Automated)	□	□
1.1.1.2	Ensure mounting of freevxfs filesystems is disabled (Automated)	□	□
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Automated)	□	□
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Automated)	□	□
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Automated)	□	□
1.1.1.6	Ensure mounting of udf filesystems is disabled (Automated)	□	□
1.1.2	Ensure /tmp is configured (Automated)	□	□
1.1.3	Ensure nodev option set on /tmp partition (Automated)	□	□
1.1.4	Ensure nosuid option set on /tmp partition (Automated)	□	□
1.1.5	Ensure noexec option set on /tmp partition (Automated)	□	□
1.1.6	Ensure /dev/shm is configured (Automated)	□	□
1.1.7	Ensure nodev option set on /dev/shm partition (Automated)	□	□
1.1.8	Ensure nosuid option set on /dev/shm partition (Automated)	□	□
1.1.9	Ensure noexec option set on /dev/shm partition (Automated)	□	□
1.1.10	Ensure separate partition exists for /var (Automated)	□	□
1.1.11	Ensure separate partition exists for /var/tmp (Automated)	□	□
1.1.12	Ensure /var/tmp partition includes the nodev option (Automated)	□	□
1.1.13	Ensure /var/tmp partition includes the nosuid option (Automated)	□	□
1.1.14	Ensure /var/tmp partition includes the noexec option (Automated)	□	□
1.1.15	Ensure separate partition exists for /var/log (Automated)	□	□
1.1.16	Ensure separate partition exists for /var/log/audit (Automated)	□	□
1.1.17	Ensure separate partition exists for /home (Automated)	□	□

1.1.18	Ensure /home partition includes the nodev option (Automated)	□	□
1.1.19	Ensure nodev option set on removable media partitions (Manual)	□	□
1.1.20	Ensure nosuid option set on removable media partitions (Manual)	□	□
1.1.21	Ensure noexec option set on removable media partitions (Manual)	□	□
1.1.22	Ensure sticky bit is set on all world-writable directories (Automated)	□	□
1.1.23	Disable Automounting (Automated)	□	□
1.1.24	Disable USB Storage (Automated)	□	□
1.2	**Configure Software Updates**		
1.2.1	Ensure package manager repositories are configured (Manual)	□	□
1.2.2	Ensure GPG keys are configured (Manual)	□	□
1.3	**Filesystem Integrity Checking**		
1.3.1	Ensure AIDE is installed (Automated)	□	□
1.3.2	Ensure filesystem integrity is regularly checked (Automated)	□	□
1.4	**Secure Boot Settings**		
1.4.1	Ensure permissions on bootloader config are not overridden (Automated)	□	□
1.4.2	Ensure bootloader password is set (Automated)	□	□
1.4.3	Ensure permissions on bootloader config are configured (Automated)	□	□
1.4.4	Ensure authentication required for single user mode (Automated)	□	□
1.5	**Additional Process Hardening**		
1.5.1	Ensure XD/NX support is enabled (Manual)	□	□
1.5.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	□	□
1.5.3	Ensure prelink is disabled (Automated)	□	□
1.5.4	Ensure core dumps are restricted (Automated)	□	□
1.6	**Mandatory Access Control**		
1.6.1	**Configure AppArmor**		
1.6.1.1	Ensure AppArmor is installed (Automated)	□	□
1.6.1.2	Ensure AppArmor is enabled in the bootloader configuration (Automated)	□	□
1.6.1.3	Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	□	□
1.6.1.4	Ensure all AppArmor Profiles are enforcing (Automated)	□	□
1.7	**Command Line Warning Banners**		

1.7.1	Ensure message of the day is configured properly (Automated)	□	□
1.7.2	Ensure permissions on /etc/issue.net are configured (Automated)	□	□
1.7.3	Ensure permissions on /etc/issue are configured (Automated)	□	□
1.7.4	Ensure permissions on /etc/motd are configured (Automated)	□	□
1.7.5	Ensure remote login warning banner is configured properly (Automated)	□	□
1.7.6	Ensure local login warning banner is configured properly (Automated)	□	□
1.8	**GNOME Display Manager**		
1.8.1	Ensure GNOME Display Manager is removed (Manual)	□	□
1.8.2	Ensure GDM login banner is configured (Automated)	□	□
1.8.3	Ensure disable-user-list is enabled (Automated)	□	□
1.8.4	Ensure XDCMP is not enabled (Automated)	□	□
1.9	Ensure updates, patches, and additional security software are installed (Manual)	□	□
2	**Services**		
2.1	**Special Purpose Services**		
2.1.1	**Time Synchronization**		
2.1.1.1	Ensure time synchronization is in use (Automated)	□	□
2.1.1.2	Ensure systemd-timesyncd is configured (Manual)	□	□
2.1.1.3	Ensure chrony is configured (Automated)	□	□
2.1.1.4	Ensure ntp is configured (Automated)	□	□
2.1.2	Ensure X Window System is not installed (Automated)	□	□
2.1.3	Ensure Avahi Server is not installed (Automated)	□	□
2.1.4	Ensure CUPS is not installed (Automated)	□	□
2.1.5	Ensure DHCP Server is not installed (Automated)	□	□
2.1.6	Ensure LDAP server is not installed (Automated)	□	□
2.1.7	Ensure NFS is not installed (Automated)	□	□
2.1.8	Ensure DNS Server is not installed (Automated)	□	□
2.1.9	Ensure FTP Server is not installed (Automated)	□	□
2.1.10	Ensure HTTP server is not installed (Automated)	□	□
2.1.11	Ensure IMAP and POP3 server are not installed (Automated)	□	□
2.1.12	Ensure Samba is not installed (Automated)	□	□
2.1.13	Ensure HTTP Proxy Server is not installed (Automated)	□	□
2.1.14	Ensure SNMP Server is not installed (Automated)	□	□
2.1.15	Ensure mail transfer agent is configured for local-only mode (Automated)	□	□
2.1.16	Ensure rsync service is not installed (Automated)	□	□
2.1.17	Ensure NIS Server is not installed (Automated)	□	□

2.2	**Service Clients**		
2.2.1	Ensure NIS Client is not installed (Automated)	□	□
2.2.2	Ensure rsh client is not installed (Automated)	□	□
2.2.3	Ensure talk client is not installed (Automated)	□	□
2.2.4	Ensure telnet client is not installed (Automated)	□	□
2.2.5	Ensure LDAP client is not installed (Automated)	□	□
2.2.6	Ensure RPC is not installed (Automated)	□	□
2.3	Ensure nonessential services are removed or masked (Manual)	□	□
3	**Network Configuration**		
3.1	**Disable unused network protocols and devices**		
3.1.1	Disable IPv6 (Manual)	□	□
3.1.2	Ensure wireless interfaces are disabled (Automated)	□	□
3.2	**Network Parameters (Host Only)**		
3.2.1	Ensure packet redirect sending is disabled (Automated)	□	□
3.2.2	Ensure IP forwarding is disabled (Automated)	□	□
3.3	**Network Parameters (Host and Router)**		
3.3.1	Ensure source routed packets are not accepted (Automated)	□	□
3.3.2	Ensure ICMP redirects are not accepted (Automated)	□	□
3.3.3	Ensure secure ICMP redirects are not accepted (Automated)	□	□
3.3.4	Ensure suspicious packets are logged (Automated)	□	□
3.3.5	Ensure broadcast ICMP requests are ignored (Automated)	□	□
3.3.6	Ensure bogus ICMP responses are ignored (Automated)	□	□
3.3.7	Ensure Reverse Path Filtering is enabled (Automated)	□	□
3.3.8	Ensure TCP SYN Cookies is enabled (Automated)	□	□
3.3.9	Ensure IPv6 router advertisements are not accepted (Automated)	□	□
3.4	**Uncommon Network Protocols**		
3.4.1	Ensure DCCP is disabled (Automated)	□	□
3.4.2	Ensure SCTP is disabled (Automated)	□	□
3.4.3	Ensure RDS is disabled (Automated)	□	□
3.4.4	Ensure TIPC is disabled (Automated)	□	□
3.5	**Firewall Configuration**		
3.5.1	**Configure UncomplicatedFirewall**		
3.5.1.1	Ensure ufw is installed (Automated)	□	□
3.5.1.2	Ensure iptables-persistent is not installed with ufw (Automated)	□	□
3.5.1.3	Ensure ufw service is enabled (Automated)	□	□
3.5.1.4	Ensure ufw loopback traffic is configured (Automated)	□	□
3.5.1.5	Ensure ufw outbound connections are configured (Manual)	□	□
3.5.1.6	Ensure ufw firewall rules exist for all open ports (Manual)	□	□
3.5.1.7	Ensure ufw default deny firewall policy (Automated)	□	□
3.5.2	**Configure nftables**		

3.5.2.1	Ensure nftables is installed (Automated)	□	□
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables (Automated)	□	□
3.5.2.3	Ensure iptables are flushed with nftables (Manual)	□	□
3.5.2.4	Ensure a nftables table exists (Automated)	□	□
3.5.2.5	Ensure nftables base chains exist (Automated)	□	□
3.5.2.6	Ensure nftables loopback traffic is configured (Automated)	□	□
3.5.2.7	Ensure nftables outbound and established connections are configured (Manual)	□	□
3.5.2.8	Ensure nftables default deny firewall policy (Automated)	□	□
3.5.2.9	Ensure nftables service is enabled (Automated)	□	□
3.5.2.10	Ensure nftables rules are permanent (Automated)	□	□
3.5.3	**Configure iptables**		
3.5.3.1	**Configure iptables software**		
3.5.3.1.1	Ensure iptables packages are installed (Automated)	□	□
3.5.3.1.2	Ensure nftables is not installed with iptables (Automated)	□	□
3.5.3.1.3	Ensure ufw is uninstalled or disabled with iptables (Automated)	□	□
3.5.3.2	**Configure IPv4 iptables**		
3.5.3.2.1	Ensure iptables default deny firewall policy (Automated)	□	□
3.5.3.2.2	Ensure iptables loopback traffic is configured (Automated)	□	□
3.5.3.2.3	Ensure iptables outbound and established connections are configured (Manual)	□	□
3.5.3.2.4	Ensure iptables firewall rules exist for all open ports (Automated)	□	□
3.5.3.3	**Configure IPv6 ip6tables**		
3.5.3.3.1	Ensure ip6tables default deny firewall policy (Automated)	□	□
3.5.3.3.2	Ensure ip6tables loopback traffic is configured (Automated)	□	□
3.5.3.3.3	Ensure ip6tables outbound and established connections are configured (Manual)	□	□
3.5.3.3.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	□	□
4	**Logging and Auditing**		
4.1	**Configure System Accounting (auditd)**		
4.1.1	**Ensure auditing is enabled**		
4.1.1.1	Ensure auditd is installed (Automated)	□	□
4.1.1.2	Ensure auditd service is enabled (Automated)	□	□
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	□	□
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	□	□
4.1.2	**Configure Data Retention**		
4.1.2.1	Ensure audit log storage size is configured (Automated)	□	□

4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	□	□
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	□	□
4.1.3	Ensure events that modify date and time information are collected (Automated)	□	□
4.1.4	Ensure events that modify user/group information are collected (Automated)	□	□
4.1.5	Ensure events that modify the system's network environment are collected (Automated)	□	□
4.1.6	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	□	□
4.1.7	Ensure login and logout events are collected (Automated)	□	□
4.1.8	Ensure session initiation information is collected (Automated)	□	□
4.1.9	Ensure discretionary access control permission modification events are collected (Automated)	□	□
4.1.10	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	□	□
4.1.11	Ensure use of privileged commands is collected (Automated)	□	□
4.1.12	Ensure successful file system mounts are collected (Automated)	□	□
4.1.13	Ensure file deletion events by users are collected (Automated)	□	□
4.1.14	Ensure changes to system administration scope (sudoers) is collected (Automated)	□	□
4.1.15	Ensure system administrator command executions (sudo) are collected (Automated)	□	□
4.1.16	Ensure kernel module loading and unloading is collected (Automated)	□	□
4.1.17	Ensure the audit configuration is immutable (Automated)	□	□
4.2	**Configure Logging**		
4.2.1	**Configure rsyslog**		
4.2.1.1	Ensure rsyslog is installed (Automated)	□	□
4.2.1.2	Ensure rsyslog Service is enabled (Automated)	□	□
4.2.1.3	Ensure logging is configured (Manual)	□	□
4.2.1.4	Ensure rsyslog default file permissions configured (Automated)	□	□
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host (Automated)	□	□
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	□	□
4.2.2	**Configure journald**		

4.2.2.1	Ensure journald is configured to send logs to rsyslog (Automated)	□	□
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	□	□
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	□	□
4.2.3	Ensure permissions on all logfiles are configured (Automated)	□	□
4.3	Ensure logrotate is configured (Manual)	□	□
4.4	Ensure logrotate assigns appropriate permissions (Automated)	□	□
5	**Access, Authentication and Authorization**		
5.1	**Configure time-based job schedulers**		
5.1.1	Ensure cron daemon is enabled and running (Automated)	□	□
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	□	□
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	□	□
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	□	□
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	□	□
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	□	□
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	□	□
5.1.8	Ensure cron is restricted to authorized users (Automated)	□	□
5.1.9	Ensure at is restricted to authorized users (Automated)	□	□
5.2	**Configure sudo**		
5.2.1	Ensure sudo is installed (Automated)	□	□
5.2.2	Ensure sudo commands use pty (Automated)	□	□
5.2.3	Ensure sudo log file exists (Automated)	□	□
5.3	**Configure SSH Server**		
5.3.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	□	□
5.3.2	Ensure permissions on SSH private host key files are configured (Automated)	□	□
5.3.3	Ensure permissions on SSH public host key files are configured (Automated)	□	□
5.3.4	Ensure SSH access is limited (Automated)	□	□
5.3.5	Ensure SSH LogLevel is appropriate (Automated)	□	□
5.3.6	Ensure SSH X11 forwarding is disabled (Automated)	□	□
5.3.7	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	□	□

5.3.8	Ensure SSH IgnoreRhosts is enabled (Automated)	□	□
5.3.9	Ensure SSH HostbasedAuthentication is disabled (Automated)	□	□
5.3.10	Ensure SSH root login is disabled (Automated)	□	□
5.3.11	Ensure SSH PermitEmptyPasswords is disabled (Automated)	□	□
5.3.12	Ensure SSH PermitUserEnvironment is disabled (Automated)	□	□
5.3.13	Ensure only strong Ciphers are used (Automated)	□	□
5.3.14	Ensure only strong MAC algorithms are used (Automated)	□	□
5.3.15	Ensure only strong Key Exchange algorithms are used (Automated)	□	□
5.3.16	Ensure SSH Idle Timeout Interval is configured (Automated)	□	□
5.3.17	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	□	□
5.3.18	Ensure SSH warning banner is configured (Automated)	□	□
5.3.19	Ensure SSH PAM is enabled (Automated)	□	□
5.3.20	Ensure SSH AllowTcpForwarding is disabled (Automated)	□	□
5.3.21	Ensure SSH MaxStartups is configured (Automated)	□	□
5.3.22	Ensure SSH MaxSessions is limited (Automated)	□	□
5.4	**Configure PAM**		
5.4.1	Ensure password creation requirements are configured (Automated)	□	□
5.4.2	Ensure lockout for failed password attempts is configured (Automated)	□	□
5.4.3	Ensure password reuse is limited (Automated)	□	□
5.4.4	Ensure password hashing algorithm is SHA-512 (Automated)	□	□
5.5	**User Accounts and Environment**		
5.5.1	**Set Shadow Password Suite Parameters**		
5.5.1.1	Ensure minimum days between password changes is configured (Automated)	□	□
5.5.1.2	Ensure password expiration is 365 days or less (Automated)	□	□
5.5.1.3	Ensure password expiration warning days is 7 or more (Automated)	□	□
5.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	□	□
5.5.1.5	Ensure all users last password change date is in the past (Automated)	□	□
5.5.2	Ensure system accounts are secured (Automated)	□	□
5.5.3	Ensure default group for the root account is GID 0 (Automated)	□	□

5.5.4	Ensure default user umask is 027 or more restrictive (Automated)	□	□
5.5.5	Ensure default user shell timeout is 900 seconds or less (Automated)	□	□
5.6	Ensure root login is restricted to system console (Manual)	□	□
5.7	Ensure access to the su command is restricted (Automated)	□	□
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Audit system file permissions (Manual)	□	□
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	□	□
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	□	□
6.1.4	Ensure permissions on /etc/group are configured (Automated)	□	□
6.1.5	Ensure permissions on /etc/group- are configured (Automated)	□	□
6.1.6	Ensure permissions on /etc/shadow are configured (Automated)	□	□
6.1.7	Ensure permissions on /etc/shadow- are configured (Automated)	□	□
6.1.8	Ensure permissions on /etc/gshadow are configured (Automated)	□	□
6.1.9	Ensure permissions on /etc/gshadow- are configured (Automated)	□	□
6.1.10	Ensure no world writable files exist (Automated)	□	□
6.1.11	Ensure no unowned files or directories exist (Automated)	□	□
6.1.12	Ensure no ungrouped files or directories exist (Automated)	□	□
6.1.13	Audit SUID executables (Manual)	□	□
6.1.14	Audit SGID executables (Manual)	□	□
6.2	**User and Group Settings**		
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords (Automated)	□	□
6.2.2	Ensure password fields are not empty (Automated)	□	□
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	□	□
6.2.4	Ensure all users' home directories exist (Automated)	□	□
6.2.5	Ensure users own their home directories (Automated)	□	□
6.2.6	Ensure users' home directories permissions are 750 or more restrictive (Automated)	□	□
6.2.7	Ensure users' dot files are not group or world writable (Automated)	□	□
6.2.8	Ensure no users have .netrc files (Automated)	□	□

6.2.9	Ensure no users have .forward files (Automated)	□	□
6.2.10	Ensure no users have .rhosts files (Automated)	□	□
6.2.11	Ensure root is the only UID 0 account (Automated)	□	□
6.2.12	Ensure root PATH Integrity (Automated)	□	□
6.2.13	Ensure no duplicate UIDs exist (Automated)	□	□
6.2.14	Ensure no duplicate GIDs exist (Automated)	□	□
6.2.15	Ensure no duplicate user names exist (Automated)	□	□
6.2.16	Ensure no duplicate group names exist (Automated)	□	□
6.2.17	Ensure shadow group is empty (Automated)	□	□

Appendix: Change History

Date	Version	Changes for this version
Feb 18, 2021	2.1.0	Proposal for addition to 1.8.2 or new 1.8.3 (Ticket 11218)
Feb 18, 2021	2.1.0	nftables.conf file is in the /etc/nftables.conf path (Ticket 11692)
Feb 18, 2021	2.1.0	ADD - Subsection "Disable network protocols and devices" (Ticket 10670)
Feb 18, 2021	2.1.0	Audit fails if service is masked instead of disabled (Ticket 10982)
Feb 19, 2021	2.1.0	No need for "for" loop (Ticket 10221)
Feb 22, 2021	2.1.0	1.4.1 Ensure permissions on bootloader config are configured (Ticket 6993)
Feb 22, 2021	2.1.0	Cant change grub.cfg permissions (Ticket 10210)
Mar 1, 2021	2.1.0	Wrong chrony file (Ticket 10270)
Mar 1, 2021	2.1.0	Use newer command for finding if tmp is mounted (Ticket 10962)
Mar 1, 2021	2.1.0	Audit differs from Remediation (Ticket 10201)
Mar 2, 2021	2.1.0	Rule 6.1.6, 6.1.7 remediation section needs to be updated for 18.04 Ubuntu (Ticket 6414)
Mar 2, 2021	2.1.0	5.6 Ensure access to su command. No wheel group on ubuntu by default (Ticket 6409)
Mar 2, 2021	2.1.0	Contents of '/etc/bashrc' have no effects Ubuntu 18 (Ticket 9818)
Mar 2, 2021	2.1.0	5.2.11 umac-128@openssh.com not supported but umac128-etm@openssh.com is (Ticket 7988)

Mar 2, 2021	2.1.0	DELETE - Ensure mounting of squashfs filesystems is disabled (Ticket 12300)
Mar 15, 2021	2.1.0	Removing ufw fails "Ensure loopback traffic is configured" (Ticket 12217)
Mar 17, 2021	2.1.0	CIS_Ubuntu_Linux_18.04_LTS_Benchmark_v2.0.1-oval.xml is break (Ticket 10710)
Mar 17, 2021	2.1.0	Update list of FIPS-140-2 compliant MACs to include ETM modes (Ticket 12440)
Mar 22, 2021	2.1.0	TYPO - Audit Procedure (Ticket 12482)