CIS Benchmarks

CIS Amazon Linux 2 STIG Benchmark

v1.0.0 - 03-19-2020

Terms of Use

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

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

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Amazon Linux 2 systems running on AWS. This document was tested against Amazon Linux 2. It is based on the Amazon Linux 2 Benchmark Level 1 and Level 2 profile, and the Red Hat Enterprise Linux 7 Security Technical Implementation Guide: Version 2, Release: 3 Benchmark Date: 26 Apr 2019

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.

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 Amazon Linux 2.

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

Scoring Information

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

Scored

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

Not Scored

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

  This profile is intended for servers.

- **Level 2**

  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 3 - STIG**

  This profile extends the "Level 2 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

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

  This profile is intended for servers.

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
Rael Daruszka
Ron Colvin, Ron Colvin
Bill Erickson
Dave Billing
Dominic Pace
Elliot Anderson
Ely Pinto
Fredrik Silverskär
Joy Latten
Kirill Antonenko
Koen Laevens
Marcelo Cerri
Mark Birch
Martynas Brijunas
Michel Verbraak
Mike Thompson
Pradeep R B
Rakesh Jain
Robert Thomas
Tom Pietschmann
Vineetha Hari Pai
William E. Triest III
Anurag Pal
Bradley Hieber
Thomas Sjögren
James Trigg
Kenneth Karlsson

Editor
Jonathan Lewis Christopherson
Eric Pinnell

Greg Carpenter

Recommendations

1 Initial Setup

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

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

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

1.1.1 Disable unused filesystems

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

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

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

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v cramfs

install /bin/true

# lsmod | grep cramfs

<No output>
```

If the output shown does not match what is defined in the audit, refer to the remediation procedure below.

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 hfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v hfs

install /bin/true

# lsmod | grep hfs

<No output>
```

If the output shown does not match what is defined in the audit, refer to the remediation procedure below.

Remediation:

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

1.1.1.3 Ensure mounting of hfsplus filesystems is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v hfsplus

install /bin/true

# lsmod | grep hfsplus

<No output>
```

If the output shown does not match what is defined in the audit, refer to the remediation procedure below.

Remediation:

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

1.1.1.4 Ensure mounting of squashfs filesystems is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v squashfs

install /bin/true

# lsmod | grep squashfs

<No output>
```

If the output shown does not match what is defined in the audit, refer to the remediation procedure below.

Remediation:

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

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

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

```
# rmmod squashfs
```

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 udf filesystems is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# modprobe -n -v udf

install /bin/true

# lsmod | grep udf

<No output>
```

If the output shown does not match what is defined in the audit, refer to the remediation procedure below.

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /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 (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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.

Audit:

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

```
# mount | grep -E '\s/tmp\s'

tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Run the following command and verify that tmpfs has been mounted to, or a system partition has been created for `/tmp`

```
#  grep -E '\s/tmp\s' /etc/fstab | grep -E -v '^\s*#'

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

OR

```
# systemctl is-enabled tmp.mount

enabled
```

If the /tmp partition isn't mounted as defined above refer to the remediation procedure below.

Remediation:

Configure `/etc/fstab` as appropriate.
Example: `vim /etc/fstab`
and add the following line:

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

OR
Run the following commands to enable systemd `/tmp` mounting:

```
# systemctl unmask tmp.mount

# systemctl enable tmp.mount
```

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to configure the `/tmp` mount:

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

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

References:

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

Notes:

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

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 seperate file system for /tmp (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must use a separate file system for /tmp (or equivalent).

Rationale:

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

Audit:

Verify that a separate file system/partition has been created for `/tmp`.
Check that a file system/partition has been created for `/tmp` with the following command:

```
# systemctl is-enabled tmp.mount

enabled
```

If the `tmp.mount` service is not enabled, check to see if `/tmp` is defined in the `fstab` with a device and mount point:

```
# grep -i /tmp /etc/fstab

UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /tmp ext4
rw,relatime,discard,data=ordered,nosuid,noexec, 0 0
```

If `tmp.mount` service is not enabled and the `/tmp` directory is not defined in the `fstab` with a device and mount point, refer to the remediation procedure below.

Remediation:

Start the `tmp.mount` service with the following command:

```
# systemctl enable tmp.mount
```

OR
Edit the `/etc/fstab` file and ensure the `/tmp` directory is defined in the `fstab` with a device and mount point.
Example: `vim /etc/fstab`
Add, uncomment or update this line:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72065

Rule ID: SV-86689r3_rule

STIG ID: RHEL-07-021340

Severity: CAT III
```

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep -E '\s/tmp\s' | grep -v nodev
```

If the `/tmp` partition exists, and `nodev` is NOT set a vaule will be returned, refer to the remediation procedure below

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/tmp` partition. See the `fstab(5)` manual page for more information.
Example: `vim /etc/fstab`
Add the following line:
`tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`
Run the following command to remount `/tmp` :

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

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

```
[Mount]

Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to remount `/tmp` :

```
# mount -o remount,nodev /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 nosuid option set on /tmp partition (Scored)

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/tmp\s' | grep -v nosuid
```

If the `/tmp` partition exists, and `nosuid` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Add the following line:

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

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:
Example: `vim /etc/systemd/system/local-fs.target.wants/tmp.mount`

```
[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.

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep -E '\s/tmp\s' | grep -v noexec
```

If the `/tmp` partition exists, and `noexec` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Add the following line:
`tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`
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:
Example: `vim /etc/systemd/system/local-fs.target.wants/tmp.mount`

```
[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

1.1.7 Ensure separate partition exists for /var (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep -E '\s/var\s'

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

If the `/var` partition is not mounted as defined above, refer to the remediation procedure below

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var` .
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

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

References:

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

Notes:

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.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72061

Rule ID: SV-86685r2_rule

STIG ID: RHEL-07-021320

Severity: CAT III
```

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 separate partition exists for /var/tmp (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep /var/tmp

<device> on /var/tmp type ext4 (rw,nosuid,nodev,noexec,relatime)
```

If var/tmp is not mounted as defined above, refer to the remediation procedure below

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp` .
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

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

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

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/var/tmp\s' | grep -v nodev
```

If `var/tmp` partition exists, and `nodev` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/var/tmp` :

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

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

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/var/tmp\s' | grep -v nosuid
```

If `var/tmp` partition exists, and `nosuid` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/var/tmp` :

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

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

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/var/tmp\s' | grep -v noexec
```

If `var/tmp` partition exists, and `noexec' is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/var/tmp` :

```
# mount -o remount,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

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep /var/log

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

If a separate partition for `var/log` is not mounted as defined above, refer to the remediation procedure below

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log` .
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

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

References:

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

Notes:

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.

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep /var/log/audit

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

If a separate partition for `var/log/audit` is not mounted as defined above, refer to the remediation procedure below

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`.
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

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

References:

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

Notes:

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.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72063

Rule ID: SV-86687r6_rule

STIG ID: RHEL-07-021330

Severity: CAT III
```

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.

1.1.14 Ensure separate partition exists for /home (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

```
# mount | grep /home

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

If a separate partition for `/home` is not mounted as defined above, refer to the remediation procedure below

Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/home` .
For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact:

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

References:

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

CIS Controls:

Version 7

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

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

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/home\s' | grep -v nodev
```

If `/home` partition exists, and `nodev` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`

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

Notes:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

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

Profile Applicability:

- Level 1

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:

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

```
# mount | grep -E '\s/dev/shm\s' | grep -v nodev
```

If `/dev/shm` partition exists, and `nodev` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/dev/shm` :

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

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81009

Rule ID: SV-95721r2_rule

STIG ID: RHEL-07-021022

Severity: CAT III
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

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

Profile Applicability:

- Level 1

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:

Verify that the `nosuid` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nosuid
```

If `/dev/shm` partition exists, and `nosuid` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/dev/shm` :

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

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81011

Rule ID: SV-95723r2_rule

STIG ID: RHEL-07-021023

Severity: CAT III
```

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

Profile Applicability:

- Level 1

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:

Verify that the `noexec` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v noexec
```

If `/dev/shm` partition exists, and `noexec` is NOT set a value will be returned, refer to the remediation procedure below

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.
Example: `vim /etc/fstab`
Run the following command to remount `/dev/shm`:

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

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81013

Rule ID: SV-95725r2_rule

STIG ID: RHEL-07-021024

Severity: CAT III
```

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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 '{}'
```

Notes:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.1.20 Disable Automounting (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run one of the following commands to verify `autofs` is not enabled:
Verify all runlevels are listed as "off" or autofs is not available.

```
# systemctl is-enabled autofs

disabled
```

Verify result is not "enabled".

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

Verify no S* lines are returned.

Remediation:

Run the following command to disable `autofs` :

```
# systemctl disable autofs
```

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.

Notes:

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

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71985

Rule ID: SV-86609r2_rule

STIG ID: RHEL-07-020110

Severity: CAT II
```

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.

1.1.21 Ensure all world-writable directories are group-owned. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.

Rationale:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

Verify all world-writable directories are group-owned by `root`, `sys`, `bin`, or an `application group`.
Check the system for world-writable directories with the following command:
Note: The value after `-fstype` must be replaced with the filesystem type. `XFS` is used as an example.

```
# find / -xdev -perm -002 -type d -fstype xfs -exec ls -lLd {} \;

drwxrwxrwt 2 root root 40 Aug 26 13:07 /dev/mqueue
drwxrwxrwt 2 root root 220 Aug 26 13:23 /dev/shm
drwxrwxrwt 14 root root 4096 Aug 26 13:29 /tmp
```

Review list of the world-writable directories to ensure they are owned by `root`, `sys`, `bin`, or an `application group` associated with the directory and annotated in the system security plan. If any are discovered not associated correctly refer to the remediation procedure below.

Remediation:

Referring to the list obatined in in the Audit above, change the group of the world-writable directories to `root` with the following command:

```
# chgrp root <directory>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72047

Rule ID: SV-86671r4_rule

STIG ID: RHEL-07-021030

Severity: CAT II
```

1.2 Configure Software Updates

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

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

1.2.1 Ensure package manager repositories are configured (Not Scored)

Profile Applicability:

- Level 1

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 one of the following commands to verify repositories are configured correctly:

```
# yum repolist
```

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 (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
```

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.

1.2.3 Ensure gpgcheck is globally activated (Scored)

Profile Applicability:

- Level 1

Description:

The `gpgcheck` option, found in the main section of the `/etc/yum.conf` and individual `/etc/yum/repos.d/*` files determines if an RPM package's signature is checked prior to its installation.

Rationale:

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

Audit:

Run the following command and verify `gpgcheck` is set to ' `1` ':

```
# grep ^gpgcheck /etc/yum.conf

gpgcheck=1
```

Run the following command and verify that all instances of `gpgcheck` returned are set to ' `1` ':

```
# grep ^gpgcheck /etc/yum.repos.d/*
```

Remediation:

Edit `/etc/yum.conf` and set '`gpgcheck=1`' in the `[main]` section.
Example: `vim /etc/yum.conf`
Edit any failing files in `/etc/yum.repos.d/*` and set all instances of `gpgcheck` to '`1`'.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71977

Rule ID: SV-86601r2_rule

STIG ID: RHEL-07-020050

Severity: CAT I
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.2.4 Ensure software packages have been digitally signed by a Certificate Authority (CA) (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Audit:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components of local packages without verification that they have been digitally signed using a certificate that is recognized and approved by the Authorizing Official of the organization.
Check that `yum` verifies the signature of local packages prior to install with the following command:

```
# grep localpkg_gpgcheck /etc/yum.conf

localpkg_gpgcheck=1
```

If `localpkg_gpgcheck` is not set to `1`, or if options are missing or commented out, ask how the signatures of local packages and other operating system components are verified.
If there is no process to validate the signatures of local packages that is approved by the organization, refer to the remediation procedure below.

Remediation:

Configure the operating system to verify the signature of local packages prior to install by setting the following option in the `/etc/yum.conf` file:
Example: `vim /etc/yum.conf`
and add the following line:

```
localpkg_gpgcheck=1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71979

Rule ID: SV-86603r2_rule

STIG ID: RHEL-07-020060

Severity: CAT I
```

1.2.5 Ensure the version of the operating system is an active vendor supported release. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be a vendor supported release.

Rationale:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Audit:

Verify the version of the operating system is vendor supported.
Check the version of the operating system with the following command:

```
# cat /etc/system-release
```

Amazon Linux release 2 (Karoo)

```
Long-term support for Amazon Linux 2 only applies to core packages and
includes:
AWS will provide security updates and bug fixes for all packages in core
until June 30, 2023..
```

If the release is not supported by the vendor, refer to the remediation procedure below.

Remediation:

Upgrade to a supported version of the operating system.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71997

Rule ID: SV-86621r4_rule

STIG ID: RHEL-07-020250

Severity: CAT I
```

1.3 Filesystem Integrity Checking

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

1.3.1 Ensure AIDE is installed (Scored)

Profile Applicability:

- Level 1

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 command and verify `aide` is installed:

```
# rpm -q aide

aide-<version>
```

Remediation:

Install AIDE using the appropriate package manager or manual installation:

```
# yum install aide
```

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

```
# aide --init

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

References:

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

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71975

Rule ID: SV-86599r2_rule

STIG ID: RHEL-07-020040

Severity: CAT II
```

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 (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

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

Remediation:

Run the following command:

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

Add the following line to the crontab:

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

References:

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

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71973

Rule ID: SV-86597r2_rule

STIG ID: RHEL-07-020030

Severity: CAT II
```

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).

1.3.3 Ensure AIDE is configured to verify ACLs (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).

Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Audit:

Verify the file integrity tool is configured to verify ACLs.
Note: AIDE is highly configurable at install time. These commands assume the `aide.conf` file is under the `/etc` directory.
Use the following command to determine if the file is in another location:

```
# find / -name aide.conf
```

Check the `aide.conf` file to determine if the `acl` rule has been added to the rule list being applied to the files and directories selection lists.
An example rule that includes the `acl` rule is below:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

If the `acl` rule is not being used on all uncommented selection lines in the `/etc/aide.conf` file, or ACLs are not being checked by another file integrity tool, refer to the remediation procedure below.

Remediation:

Configure the file integrity tool to check file and directory ACLs.
If AIDE is installed, ensure the `acl` rule is present on all uncommented file and directory selection lists.
Example: `vim /etc/aide.conf`
add a rule that includes the `acl` example:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

Notes:

This checks for `aide.conf` in the default location. If `aide.conf` is in a different location, manually confirm that the setting(s) are correct.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72069

Rule ID: SV-86693r3_rule

STIG ID: RHEL-07-021600

Severity: CAT III
```

1.3.4 Ensure AIDE is configured to verify XATTRS (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the file integrity tool is configured to verify extended attributes.

Rationale:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Audit:

Verify the file integrity tool is configured to verify extended attributes.
Note: AIDE is highly configurable at install time. These commands assume the `aide.conf` file is under the `/etc` directory.
Use the following command to determine if the file is in another location:

```
# find / -name aide.conf
```

Check the `aide.conf` file to determine if the `xattrs` rule has been added to the rule list being applied to the files and directories selection lists.
An example rule that includes the `xattrs` rule follows:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

If the `xattrs` rule is not being used on all uncommented selection lines in the `/etc/aide.conf` file, or extended attributes are not being checked by another file integrity tool, refer to the remediation procedure below.

Remediation:

Configure the file integrity tool to check file and directory extended attributes.
If AIDE is installed, ensure the `xattrs` rule is present on all uncommented file and directory selection lists.
Example: `vim /etc/aide.conf`
add rule that includes the `xattrs` example:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72071

Rule ID: SV-86695r3_rule

STIG ID: RHEL-07-021610

Severity: CAT III
```

1.3.5 Ensure AIDE is configured to use FIPS 140-2 (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Rationale:

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Audit:

Verify the file integrity tool is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.
Note: AIDE is highly configurable at install time. These commands assume the `aide.conf` file is under the `/etc` directory.
Use the following command to determine if the file is in another location:

```
# find / -name aide.conf
```

Check the `aide.conf` file to determine if the `sha512` rule has been added to the rule list being applied to the files and directories selection lists.
An example rule that includes the `sha512` rule follows:

```
All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

If the `sha512` rule is not being used on all uncommented selection lines in the `/etc/aide.conf` file, or another file integrity tool is not using FIPS 140-2 approved cryptographic hashes for validating file contents and directories, refer to the remediation procedure below.

Remediation:

Configure the file integrity tool to use FIPS 140-2 cryptographic hashes for validating file and directory contents.
If AIDE is installed, ensure the `sha512` rule is present on all uncommented file and directory selection lists.
Example: `vim /etc/aide.conf`
add a rule that includes the `sha512` example:

```
All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72073

Rule ID: SV-86697r3_rule

STIG ID: RHEL-07-021620

Severity: CAT II
```

1.4 Secure Boot Settings

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

1.4.1 Ensure permissions on bootloader config are configured (Scored)

Profile Applicability:

- Level 1

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is `grub.cfg` stored in `/boot/grub2/`.

Rationale:

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

Audit:

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

```
# stat /boot/grub2/grub.cfg

Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

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

```
# chown root:root /boot/grub2/grub.cfg

# chmod og-rwx /boot/grub2/grub.cfg
```

Notes:

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

Replace `/boot/grub2/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.

1.4.2 Ensure authentication required for single user mode (Scored)

Profile Applicability:

- Level 1

Description:

Single user mode (rescue 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 (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Run the following commands and verify that `/sbin/sulogin` or `/usr/sbin/sulogin` is used as shown:

```
# grep /sbin/sulogin /usr/lib/systemd/system/rescue.service
ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"

# grep /sbin/sulogin /usr/lib/systemd/system/emergency.service
ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

Remediation:

Edit /usr/lib/systemd/system/rescue.service and /usr/lib/systemd/system/emergency.service and set ExecStart to use /sbin/sulogin or /usr/sbin/sulogin:

```
ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

Notes:

The systemctl option `--fail` is synonymous with `--job-mode=fail` . Using either is acceptable.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-77823

Rule ID: SV-92519r2_rule

STIG ID: RHEL-07-010481

Severity: CAT II
```

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 boot loader does not allow removable media (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not allow removable media to be used as the boot loader unless approved.

Rationale:

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Audit:

Verify the system is not configured to use a boot loader on removable media.
Note: GRUB 2 reads its configuration from the `/boot/grub2/grub.cfg` file on traditional BIOS-based machines and from the `/boot/efi/EFI/redhat/grub.cfg` file on UEFI machines.
Check for the existence of alternate boot loader configuration files with the following command:

```
# find / -name grub.cfg

/boot/grub2/grub.cfg
```

If a `grub.cfg` is found in any subdirectories other than `/boot/grub2` and `/boot/efi/EFI/redhat`, ask the Authorizing Official if there is documentation signed to approve the use of removable media as a boot loader.
Check that the grub configuration file has the set root command in each menu entry with the following commands:

```
# grep -c menuentry /boot/grub2/grub.cfg
1

# grep 'set root' /boot/grub2/grub.cfg
set root=(hd0,1)
```

If the system is using an alternate boot loader on removable media, and documentation does not exist approving the alternate configuration, refer to the remediation procedure below.

Remediation:

Remove alternate methods of booting the system from removable media or document the configuration to boot from removable media with the Authorizing Official.
Example: `vim /etc/default/grub`
Add this in the first menu entry

```
set root=(hd0,1)
```

Any changes made to `/etc/default/grub` require you to run `grub2-mkconfig` to re-generate the `/boot/grub2/grub.cfg` file.
Example:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72075

Rule ID: SV-86699r2_rule

STIG ID: RHEL-07-021700

Severity: CAT II
```

1.4.4 Ensure UEFI requires authentication for single-user and maintenance modes. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

If the operating system is using Unified Extensible Firmware Interface (UEFI) it must require authentication upon booting into single-user and maintenance modes.

Rationale:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use BIOS, this is Not Applicable.
Check to see if an encrypted `root` password is set. On systems that use `UEFI`, use the following command:

```
# grep -iw grub2_password /boot/efi/EFI/redhat/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the `root` password does not begin with `grub.pbkdf2.sha512`, this is a finding.
Verify that the `root` account is set as the `superusers`:

```
# grep -iw "superusers" /boot/efi/EFI/redhat/grub.cfg
set superusers="root"
export superusers
```

If `superusers` is not set to `root`, refer to the remediation procedure below.

Remediation:

Create an encrypted password with `grub2-setpassword`:

```
# grub2-setpassword
Enter password: <password>
Confirm password: <password>
```

Edit the `/boot/efi/EFI/redhat/grub.cfg` file and add or modify the following lines in the `### BEGIN /etc/grub.d/01_users ###` section:

Example: `vim /boot/efi/EFI/redhat/grub.cfg`

```
set superusers="root"
export superusers
```

Run the following command to update the grub2 configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Impact:

This recommendation is only valid for Amazon Linux 2 when it is used on-premise.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81007

Rule ID: SV-95719r1_rule

STIG ID: RHEL-07-010491

Severity: CAT I
```

1.5 Additional Process Hardening

1.5.1 Ensure core dumps are restricted (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following commands and verify output matches:

```
# grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*
* hard core 0

# sysctl fs.suid_dumpable
fs.suid_dumpable = 0

# 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` 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.

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

Profile Applicability:

- Level 1

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 "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*

kernel.randomize_va_space = 2
```

Remediation:

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

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-77825

Rule ID: SV-92521r2_rule

STIG ID: RHEL-07-040201

Severity: CAT II
```

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 (Scored)

Profile Applicability:

- Level 1

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.
Run the following command:

```
# rpm -q prelink

package prelink is not installed
```

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

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

```
# yum remove prelink
```

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 the Ctrl-Alt-Delete key sequence is disabled. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the user will be prompted when Ctrl-Alt-Delete key sequence is entered.

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In the GNOME graphical environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Audit:

Verify the operating system is not configured to reboot the system when `Ctrl-Alt-Delete` is pressed.
Check that the `ctrl-alt-del.target` is masked and not active with the following command:

```
# systemctl status ctrl-alt-del.target

ctrl-alt-del.target

Loaded: masked (/dev/null; bad)

Active: inactive (dead)
```

If the `ctrl-alt-del.target` is not masked, or if the `ctrl-alt-del.target` is active, refer to the remediation procedure below.

Remediation:

Configure the system to disable the `Ctrl-Alt_Delete` sequence for the command line with the following command:

```
# systemctl mask ctrl-alt-del.target
```

If GNOME is active on the system, create a database to contain the system-wide setting (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/00-disable-CAD
```

Add the setting to disable the `Ctrl-Alt_Delete` sequence for GNOME:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71993

Rule ID: SV-86617r4_rule

STIG ID: RHEL-07-020230

Severity: CAT I
```

1.5.5 Ensure kernel core dumps are disabled. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must disable Kernel core dumps unless needed.

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

Audit:

Verify that kernel core dumps are disabled unless needed.
Check the status of the `kdump` service with the following command:

```
# systemctl status kdump.service

kdump.service - Crash recovery kernel arming
Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled)
Active: active (exited) since Wed 2015-08-26 13:08:09 EDT; 43min ago
Main PID: 1130 (code=exited, status=0/SUCCESS)
kernel arming.
```

If the `kdump` service is active, the use of the service must be documented with the Authorizing Official.
If the service is active and is not documented, refer to the remediation procedure below.

Remediation:

If kernel core dumps are not required, disable the `kdump` service with the following command:

```
# systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the Authorizing Official.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72057

Rule ID: SV-86681r2_rule

STIG ID: RHEL-07-021300

Severity: CAT II
```

1.5.6 Ensure NIST FIPS-validated cryptography is configured (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement NIST FIPS-validated cryptography for the following:

- provision digital signatures
- generate cryptographic hashes
- protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

Verify the operating system implements DoD-approved encryption to protect the confidentiality of remote access sessions.
Check to see if the `dracut-fips` package is installed with the following command:

```
# yum list installed dracut-fips

dracut-fips-033-360.el7_2.x86_64.rpm
```

If a `dracut-fips` package is installed, check to see if the kernel command line is configured to use FIPS mode with the following command:
Note: GRUB 2 reads its configuration from the `/boot/grub2/grub.cfg` file on traditional BIOS-based machines and from the `/boot/efi/EFI/redhat/grub.cfg` file on UEFI machines.

```
# grep fips /boot/grub2/grub.cfg
/vmlinuz-3.8.0-0.40.el7.x86_64 root=/dev/mapper/rhel-root ro rd.md=0 rd.dm=0
rd.lvm.lv=rhel/swap crashkernel=auto rd.luks=0 vconsole.keymap=us
rd.lvm.lv=rhel/root rhgb fips=1 quiet
```

If the kernel command line is configured to use FIPS mode, check to see if the system is in FIPS mode with the following command:

```
# cat /proc/sys/crypto/fips_enabled
1
```

If a `dracut-fips` package is not installed, the kernel command line does not have a FIPS entry, or the system has a value of `0` for `fips_enabled` in `/proc/sys/crypto`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement DoD-approved encryption by installing the `dracut-fips` package.
To enable strict FIPS compliance, the `fips=1` kernel option needs to be added to the kernel command line during system installation so key generation is done with FIPS- approved algorithms and continuous monitoring tests in place.
Configure the operating system to implement DoD-approved encryption by following the steps below:
The `fips=1` kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users should also ensure that the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is `256` and more. Less than `256` keystrokes may generate a non-unique key.
Install the `dracut-fips` package with the following command:

```
# yum install dracut-fips
```

Recreate the `initramfs` file with the following command:
Note: This command will overwrite the existing `initramfs` file.

```
# dracut -f
```

Modify the kernel command line of the current kernel in the `grub.cfg` file by adding the following option to the `GRUB_CMDLINE_LINUX` key in the `/etc/default/grub` file and then rebuild the `grub.cfg` file:

```
fips=1
```

Changes to `/etc/default/grub` require rebuilding the `grub.cfg` file as follows:
On BIOS-based machines, use the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

On UEFI-based machines, use the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

If `/boot` or `/boot/efi` reside on separate partitions, the kernel parameter `boot=<partition of /boot or /boot/efi>` must be added to the kernel command line. You can identify a partition by running the `df /boot` or `df /boot/efi` command:

```
# df /boot
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda1 495844 53780 416464 12% /boot
```

To ensure the `boot=` configuration option will work even if device naming changes occur between boots, identify the universally unique identifier (UUID) of the partition with the following command:

```
# blkid /dev/sda1
/dev/sda1: UUID="05c000f1-a213-759e-c7a2-f11b7424c797" TYPE="ext4"
```

For the example above, append the following string to the kernel command line:

```
boot=UUID=05c000f1-a213-759e-c7a2-f11b7424c797
```

Reboot the system for the changes to take effect.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72067

Rule ID: SV-86691r4_rule

STIG ID: RHEL-07-021350

Severity: CAT I
```

1.5.7 Ensure DNS is servers are configured (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating systems that are using DNS resolution, must have at least two name servers configured.

Rationale:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Audit:

Determine whether the system is using local or DNS name resolution with the following command:

```
# grep hosts /etc/nsswitch.conf
hosts: files dns
```

If the DNS entry is missing from the host's line in the `/etc/nsswitch.conf` file, the `/etc/resolv.conf` file must be empty.
Verify the `/etc/resolv.conf` file is empty with the following command:

```
# ls -al /etc/resolv.conf
-rw-r--r-- 1 root root 0 Aug 19 08:31 resolv.conf
```

If local host authentication is being used and the `/etc/resolv.conf` file is not empty, refer to the remediation procedure below.
If the DNS entry is found on the host's line of the `/etc/nsswitch.conf` file, verify the operating system is configured to use two or more name servers for DNS resolution.
Determine the name servers used by the system with the following command:

```
# grep nameserver /etc/resolv.conf
nameserver 192.168.1.2
nameserver 192.168.1.3
```

If less than two lines are returned that are not commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to use two or more name servers for DNS resolution. Edit the `/etc/resolv.conf` file to uncomment or add the two or more `nameserver` option lines with the IP address of local authoritative name servers. If local host resolution is being performed, the `/etc/resolv.conf` file must be empty. An empty `/etc/resolv.conf` file can be created as follows:

```
# echo -n > /etc/resolv.conf
```

And then make the file immutable with the following command:

```
# chattr +i /etc/resolv.conf
```

If the `/etc/resolv.conf` file must be mutable, the required configuration must be documented with the Authorizing Official and the file must be verified by the system file integrity tool.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72281

Rule ID: SV-86905r2_rule

STIG ID: RHEL-07-040600

Severity: CAT III
```

1.6 Mandatory Access Control

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

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

1.6.1 Configure SELinux

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

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

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

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

References:

1. NSA SELinux resources:
    1. http://www.nsa.gov/research/selinux
    2. http://www.nsa.gov/research/selinux/list.shtml
2. Fedora SELinux resources:
    1. FAQ: http://docs.fedoraproject.org/selinux-faq
    2. User Guide: http://docs.fedoraproject.org/selinux-user-guide
    3. Managing Services Guide: http://docs.fedoraproject.org/selinux-managing-confined-services-guide
3. SELinux Project web page and wiki:
    1. http://www.selinuxproject.org
4. Chapters 43-45 of Red Hat Enterprise Linux 5: Deployment Guide (Frank Mayer, Karl MacMillan and David Caplan),
5. SELinux by Example: Using Security Enhanced Linux (Prentice Hall, August 6, 2006)

1.6.1.1 Ensure SELinux is installed (Scored)

Profile Applicability:

- Level 2

Description:

SELinux provides Mandatory Access Control.

Rationale:

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

Audit:

Verify SELinux is installed.
Run the following command:

```
# rpm -q libselinux

libselinux-<version>
```

Remediation:

Install SELinux or apparmor using the appropriate package manager:
OR

```
# yum install libselinux
```

Impact:

SELinux has several package names in use on different distributions. Research the appropriate packages for your environment.

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 SELinux is not disabled in bootloader configuration (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Run the following command and verify that no linux line has the `selinux=0` or `enforcing=0` parameters set:

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -E "(selinux=0|enforcing=0)"
```

Nothing should be returned. If a value is returned, refer to the remediation procedure below

Remediation:

Edit `/etc/default/grub` and remove all instances of `selinux=0` and `enforcing=0` from all CMDLINE_LINUX parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet"

GRUB_CMDLINE_LINUX=""
```

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

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Notes:

This recommendation is designed around the grub 2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

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 the SELinux state is enforcing (Scored)

Profile Applicability:

- Level 2

Description:

Set SELinux to enable when the system is booted.

Rationale:

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

Audit:

Run the following commands and ensure output matches:

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

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

Remediation:

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

```
SELINUX=enforcing
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71989

Rule ID: SV-86613r3_rule

STIG ID: RHEL-07-020210

Severity: CAT I
```

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 SELinux policy is configured (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

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

SELINUXTYPE=targeted

# sestatus

Policy from config file: targeted
```

Remediation:

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

```
SELINUXTYPE=targeted
```

Notes:

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

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71991

Rule ID: SV-86615r4_rule

STIG ID: RHEL-07-020220

Severity: CAT I
```

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.

1.6.1.5 Ensure SETroubleshoot is not installed (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Verify `setroubleshoot` is not installed.
Run the following command:

```
# rpm -q setroubleshoot

package setroubleshoot is not installed
```

Remediation:

Uninstall `setroubleshoot` using the appropriate package manager:

```
# yum remove setroubleshoot
```

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.

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Verify `mcstrans` is not installed.
Run the following command:

```
# rpm -q mcstrans

package mcstrans is not installed
```

Remediation:

Uninstall `mcstrans` using the appropriate package manager:
OR

```
# yum remove mcstrans
```

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.

1.6.1.7 Ensure no unconfined daemons exist (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Run the following command and verify no output is produced:

```
# ps -eZ | grep -E "initrc" | grep -E -v -w "tr|ps|grep|bash|awk" | tr ':' '
' | awk '{ print $NF }'
```

Remediation:

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

Notes:

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

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.

1.7 Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

1.7.1 Command Line Warning Banners

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

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

Profile Applicability:

- Level 1

Description:

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

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

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

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

Run the following command and verify no results are returned:

```
#  grep -E -i '\\\v|\\\r|\\\m|\\\s|Amazon' /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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71863

Rule ID: SV-86487r3_rule

STIG ID: RHEL-07-010050

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.7.1.2 Ensure local login warning banner is configured properly (Scored)

Profile Applicability:

- Level 1

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|Amazon)' /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.

1.7.1.3 Ensure remote login warning banner is configured properly (Scored)

Profile Applicability:

- Level 1

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|Amazon)' /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.

1.7.1.4 Ensure permissions on /etc/motd are configured (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# stat /etc/motd

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

Remediation:

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

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

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

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

Profile Applicability:

- Level 1

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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.7.1.6 Ensure permissions on /etc/issue.net are configured (Scored)

Profile Applicability:

- Level 1

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
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

1.7.1.7 Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Audit:

Verify any publicly accessible connection to the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.
Check for the location of the banner file being used with the following command:

```
# grep -i banner /etc/ssh/sshd_config

banner /etc/issue
```

This command will return the banner keyword and the name of the file that contains the ssh banner (in this case `/etc/issue`).
If the line is commented out, refer to the remediation procedure below.
View the file specified by the banner keyword to check that it matches the text of the Standard Mandatory DoD Notice and Consent Banner:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, refer to the remediation procedure below.
If the text in the file does not match the Standard Mandatory DoD Notice and Consent Banner, refer to the remediation procedure below.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the ssh.
Edit the `/etc/ssh/sshd_config` file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).
Example: `vim /etc/sshd_config`
An example configuration line is:

```
banner /etc/issue
```

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DoD Notice and Consent Banner.
Example: `vim /etc/issue`
The DoD required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

The SSH service must be restarted for changes to take effect.
Examples:

```
Type the following command:
# /etc/init.d/sshd restart

or use the service command:
# service sshd restart

or with systemd enter:
$ sudo systemctl restart sshd
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72225

Rule ID: SV-86849r4_rule

STIG ID: RHEL-07-040170

Severity: CAT II
```

1.8 Ensure updates, patches, and additional security software are installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# yum check-update --security
```

Remediation:

Use your package manager to update all packages on the system according to site policy. The following command will install all available security updates:

```
# yum update --security
```

Notes:

Site policy may mandate a testing period before install onto production systems for available updates. The audit and remediation here only cover security updates. Non-security updates can be audited with and comparing against site policy:

```
# yum check-update
```

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71999

Rule ID: SV-86623r4_rule

STIG ID: RHEL-07-020260

Severity: CAT II
```

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.

1.9 Ensure anti-virus is installed and running (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must have virus scanning software installed.

Rationale:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Audit:

Verify an anti-virus solution is installed on the system. The anti-virus solution may be bundled with an approved host-based security solution.
If virus scanning software is not installed, refer to the remediation procedure below.

Remediation:

Install an antivirus solution on the system.
Document which solution is installed on the system with the ISSO.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72213

Rule ID: SV-86837r3_rule

STIG ID: RHEL-07-032000

Severity: CAT I
```

1.10 Ensure required packages for multifactor atuentication are installed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must have the required packages for multifactor authentication installed.

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Audit:

Verify the operating system has the packages required for multifactor authentication installed.
Check for the presence of the packages required to support multifactor authentication with the following commands:

```
# yum list installed esc
esc-1.1.0-26.el7.noarch.rpm

# yum list installed pam_pkcs11
pam_pkcs11-0.6.2-14.el7.noarch.rpm
```

If the `esc` and `pam_pkcs11` packages are not installed, refer to the remediation procedure below.

Remediation:

To configure the operating system to implement multifactor authentication by installing the required packages.
Install the `esc` and `pam_pkcs11` packages on the system with the following command:

```
# yum install esc pam_pkcs11
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72417

Rule ID: SV-87041r4_rule

STIG ID: RHEL-07-041001

Severity: CAT II
```

1.11 Ensure host-based intrusion detection tool is used (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must have a host-based intrusion detection tool installed.

Rationale:

Adding host-based intrusion detection tools can provide the capability to automatically take actions in response to malicious behavior, which can provide additional agility in reacting to network threats. These tools also often include a reporting capability to provide network awareness of the system, which may not otherwise exist in an organization's systems management regime.

Audit:

Ask if a host-based intrusion detection application is loaded on the system. Per OPORD 16-0080, the preferred intrusion detection system is McAfee HBSS available through the U.S. Cyber Command (USCYBERCOM).
If another host-based intrusion detection application is in use, such as SELinux, this must be documented and approved.
Procedure:
Examine the system to determine if the Host Intrusion Prevention System (HIPS) is installed:

```
# rpm -qa | grep MFEhiplsm
```

Verify that the McAfee HIPS module is active on the system:

```
# ps -ef | grep -i "hipclient"
```

If the MFEhiplsm package is not installed, check for another intrusion detection system:

```
# find / -name <daemon name>
```

Where <daemon name> is the name of the primary application daemon to determine if the application is loaded on the system.
Determine if the application is active on the system:

```
# ps -ef | grep -i <daemon name>
```

If the MFEhiplsm package is not installed and an alternate host-based intrusion detection application has not been documented for use, refer to the remediation procedure below.
If no host-based intrusion detection system is installed and running on the system, refer to the remediation procedure below.

Remediation:

Install and enable the latest `McAfee HIPS` package, available from USCYBERCOM.
Note: If the system does not support the McAfee HIPS package, install and enable a supported intrusion detection system application and document its use with the Authorizing Official.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-92255

Rule ID: SV-102357r1_rule

STIG ID: RHEL-07-020019

Severity: CAT II
```

2 Services

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

2.1 inetd Services

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

2.1.1 Ensure the rsh package has been removed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have the rsh-server package installed.

Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Audit:

Check to see if the `rsh-server` package is installed with the following command:

```
# yum list installed rsh-server
```

If the `rsh-server` package is installed, refer to the remediation procedure below.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the `rsh-server` package from the system with the following command:

```
# yum remove rsh-server
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71967

Rule ID: SV-86591r2_rule

STIG ID: RHEL-07-020000

Severity: CAT I
```

2.1.2 Ensure the ypserv package has been removed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have the ypserv package installed.

Rationale:

Removing the "ypserv" package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Audit:

The NIS service provides an unencrypted authentication service that does not provide for the confidentiality and integrity of user passwords or the remote session.
Check to see if the `ypserv` package is installed with the following command:

```
# yum list installed ypserv
```

If the `ypserv` package is installed, refer to the remediation procedure below.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the `ypserv` package from the system with the following command:

```
# yum remove ypserv
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71969

Rule ID: SV-86593r2_rule

STIG ID: RHEL-07-020010

Severity: CAT I
```

2.1.3 Ensure the TFTP server has not been installed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.

Rationale:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Audit:

Verify a TFTP server has not been installed on the system.
Check to see if a TFTP server has been installed with the following command:

```
# yum list installed tftp-server
tftp-server-0.49-9.el7.x86_64.rpm
```

If TFTP is installed and the requirement for TFTP is not documented with the Authorizing Official, refer to the remediation procedure below.

Remediation:

Remove the TFTP package from the system with the following command:

```
# yum remove tftp-server
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72301

Rule ID: SV-86925r2_rule

STIG ID: RHEL-07-040700

Severity: CAT I
```

2.1.4 Ensure TFTP daemon is configured to operate in secure mode. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.

Rationale:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Audit:

Verify the TFTP daemon is configured to operate in secure mode.
Check to see if a TFTP server has been installed with the following commands:

```
# yum list installed tftp-server
tftp-server.x86_64 x.x-x.el7 rhel-7-server-rpms
```

If a TFTP server is not installed, this is Not Applicable.
If a TFTP server is installed, check for the server arguments with the following command:

```
# grep server_args /etc/xinetd.d/tftp
server_args = -s /var/lib/tftpboot
```

If the `server_args` line does not have a `-s` option and a subdirectory is not assigned, refer to the remediation procedure below.

Remediation:

Configure the TFTP daemon to operate in secure mode by adding the following line to `/etc/xinetd.d/tftp` (or modify the line to have the required value):
`Example: vim /etc/xinetd.d/tftp`
Add this line.

```
server_args = -s /var/lib/tftpboot
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72305

Rule ID: SV-86929r3_rule

STIG ID: RHEL-07-040720

Severity: CAT II
```

2.2 Special Purpose Services

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

2.2.1 Time Synchronization

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

2.2.1.1 Ensure time synchronization is in use (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# rpm -q chrony
```

OR

```
# rpm -q 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 physical systems or virtual systems where host based time synchronization is not available install NTP or chrony using the appropriate package manager or manual installation:
To install chrony:
Run one of the folloing commands:

```
# yum install chrony
```

OR
To install ntp:
Run one of the following commands:

```
# yum install ntp
```

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

Notes:

systemd-timesyncd is part of systemd. Some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72269

Rule ID: SV-86893r4_rule

STIG ID: RHEL-07-040500

Severity: CAT II
```

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.

2.2.1.2 Ensure ntp is configured (Scored)

Profile Applicability:

- Level 1

Description:

`ntp` is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. `ntp` can be configured to be a client and/or a server.

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

Rationale:

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

Audit:

Run the following command and verify output matches:

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

The `-4` in the first line is optional and options after `default` can appear in any order. Additional restriction lines may exist.
Run the following command and verify remote server is configured properly:

```
# grep -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 one of the following commands as appropriate for your distribution and verifying output matches:

```
# grep "^OPTIONS" /etc/sysconfig/ntpd
OPTIONS="-u ntp:ntp"
# grep "^ExecStart" /usr/lib/systemd/system/ntpd.service
ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS
```

Additional options may be present.

Remediation:

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

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

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

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

Configure `ntp` to run as the `ntp` user by adding or editing one of the following file:
`/etc/sysconfig/ntpd`:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72269

Rule ID: SV-86893r4_rule

STIG ID: RHEL-07-040500

Severity: CAT II
```

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.

2.2.1.3 Ensure chrony is configured (Scored)

Profile Applicability:

- Level 1

Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on `chrony` can be found at http://chrony.tuxfamily.org/. `chrony` can be configured to be a client and/or a server.

Rationale:

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

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

Audit:

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

```
# grep -E "^(server|pool)" /etc/chrony.conf
server <remote-server>
```

Multiple servers may be configured.
Run the following command and verify the first field for the `chronyd` process is `chrony`:

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

Remediation:

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

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

Add or edit the `OPTIONS` in `/etc/sysconfig/chronyd` to include '`-u chrony`':

```
OPTIONS="-u 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.

2.2.1.4 Ensure NTP "maxpoll" is set. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

For networked systems, the operating system must synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Audit:

Check to see if NTP is running in continuous mode.

```
# ps -ef | grep ntp

aluser  4174  3375  0 01:18 pts/0    00:00:00 grep --color=auto ntp
```

If NTP is not running, this is a finding.
Check the `ntp.conf` file for the `maxpoll` option setting:

```
# grep maxpoll /etc/ntp.conf
server 0.amazon.pool.ntp.org iburst maxpoll 10
```

If the option is set to `17` or is not set, refer to the remediation procedure below.
If the file does not exist, check the `/etc/cron.daily` subdirectory for a crontab file controlling the execution of the `ntpd -q` command.

```
# grep -i "ntpd -q" /etc/cron.daily/*
# ls -al /etc/cron.* | grep ntp
ntp
```

If a crontab file does not exist in the `/etc/cron.daily` that executes the `ntpd -q` command, refer to the remediation procedure below.

Remediation:

Edit the `/etc/ntp.conf` file and add or update an entry to define `maxpoll` to `10` as follows:
`Example: vim /etc/ntp.conf`
Add the following line:

```
server 0.amazon.pool.ntp.org iburst maxpoll 10
```

If NTP was running and `maxpoll` was updated, the NTP service must be restarted:

```
# systemctl restart ntpd
```

If NTP was not running, it must be started:

```
# systemctl start ntpd
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72269

Rule ID: SV-86893r4_rule

STIG ID: RHEL-07-040500

Severity: CAT II
```

2.2.2 GNOME Configuration

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems. If the GDM service is installed these additional security recommendations should be applied.

2.2.2.1 Ensure the screen package is installed. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

If the GNOME display manager is being utilized than the screen package must be installed so the security recommendations outlined for GNOME can execute. The Red Hat Enterprise Linux operating system must have the screen package installed.

Rationale:

A session time-out (screen lock and screensaver) is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system and either logs out or does not log out because of the temporary nature of the absence.

The screen and tmux packages allow for a session lock to be implemented and configured.

Audit:

Verify the operating system has the screen package installed.
Check to see if the screen package is installed with the following command:

```
# yum list installed screen

screen-4.3.1-3-x86_64.rpm
```

If the screen package is not installed, check to see if the `tmux` package is installed with the following command:

```
# yum list installed tmux

tmux-1.8-4.el7.x86_64.rpm
```

If either the screen package or the `tmux` package is not installed, please follow the remediation procedure below.

Remediation:

Install the screen package to allow the initiation of a user screen lock or a screensaver lock after a 15-minute period of inactivity.
Install the screen program (if it is not on the system) with the following command:

```
# yum install screen
```

OR
Install the `tmux` program (if it is not on the system) with the following command:

```
#yum install tmux
```

Impact:

The information system initiates a session lock after the organization-defined time period of inactivity.

Notes:

This Benchmark Recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71897

Rule ID: SV-86521r3_rule

STIG ID: RHEL-07-010090

Severity: CAT II
```

2.2.2.2 Ensure GNOME Screen Lock is Enabled. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system should enable a user session lock until that user re-establishes access using established identification and authentication procedures.

A session lock is a temporary action taken that locks the screen when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

Rationale:

The screen lock should be implemented at the point where session activity can be determined.

Regardless of where the screen lock is determined and implemented, once invoked, the screen lock must remain in place until the user re-authenticates. No other activity aside from re-authentication must unlock the system.

Audit:

Verify the operating system enables a user's screen lock until that user re-establishes access using established identification and authentication procedures. The screen program must be installed to lock sessions on the console.
Note: If the system does not have GNOME installed, this requirement is Not Applicable.
Check to see if the screen lock is enabled with the following command:

```
grep -i lock-enabled /etc/dconf/db/local.d/locks/*

lock-enabled=true
```

If the `lock-enabled` setting is missing or is not set to `true`, refer to the remediation procedure below.

Remediation:

Configure the operating system to enable a user's screen lock until that user re-establishes access using established identification and authentication procedures.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
# touch /etc/dconf/db/local.d/locks/00-screensaver
```

Edit the `[org/gnome/desktop/screensaver]` section of the database file and add or update the following lines:
Set this to true to lock the screen when the screensaver activates

```
[org/gnome/desktop/screensaver]

lock-enabled=true
```

Update the system databases:

```
# dconf update
```

Users must log out and back in again before the system-wide settings take effect.

Impact:

Users must log out and back in again before the system-wide settings take effect.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71891

Rule ID: SV-86515r6_rule

STIG ID: RHEL-07-010060

Severity: CAT II
```

2.2.2.3 Ensure GNOME Screensaver period of inactivity is configured. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Rationale:

A session time-out lock with the screensaver is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The screensaver is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system initiates a screensaver after a 15-minute period of inactivity for graphical user interfaces.
The screen program must be installed to lock sessions on the console.
Note: If the system does not have GNOME installed, this requirement is Not Applicable.
Check to see if GNOME is configured to display a screensaver after a 15 minute delay with the following command:

```
# grep -i idle-delay /etc/dconf/db/local.d/locks/*

idle-delay=uint32 900
```

If the `idle-delay` setting is missing or is not set to `900` or less, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/locks/00-screensaver
```

Edit `/etc/dconf/db/local.d/locks/00-screensaver` and add or update the following lines:
Set the lock time out to `900` seconds before the session is considered idle
You must include the `uint32` along with the integer key values as shown.

```
[org/gnome/desktop/session]

idle-delay=uint32 900
```

Update the system databases:

```
# dconf update
```

Impact:

Users must log out and back in again before the system-wide settings take effect.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71893

Rule ID: SV-86517r5_rule

STIG ID: RHEL-07-010070

Severity: CAT II
```

2.2.2.4 Ensure GNOME Idle activation is set. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. As part of this configuration idle activation has to be configured.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

Audit:

Verify the idle activation setting is configured correctly for GNOME so that when the operating system initiates a session lock after a 15-minute period of inactivity the screensaver is invoked. The screen program must be installed to lock sessions on the console.
If it is installed, GNOME must be configured to enforce a session lock after a 15-minute delay. Check for the session lock settings with the following commands:

```
# grep -i idle-activation-enabled /etc/dconf/db/local.d/locks/*

idle-activation-enabled=true
```

If `idle-activation-enabled` is not set to `true`, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate a session lock after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d//locks/00-screensaver
```

Edit /etc/dconf/db/local.d/locks/00-screensaver and add or update the following lines:
Add the setting to enable screensaver locking after 15 minutes of inactivity:

```
[org/gnome/desktop/screensaver]

idle-activation-enabled=true
```

Update the system databases:

```
# dconf update
```

Impact:

Users must log out and back in again before the system-wide settings take effect.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71899

Rule ID: SV-86523r4_rule

STIG ID: RHEL-07-010100

Severity: CAT II
```

2.2.2.5 Ensure GNOME Lock Delay is configured (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. Please ensure the screensaver contains the lock delay system wide setting.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

Audit:

Verify the lock delay setting is included in the system wide screensaver setting for the operating system.
Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.
If GNOME is installed, check to see a session lock occurs when the screensaver is activated with the following command:

```
# grep -i lock-delay /etc/dconf/db/local.d/locks/*

lock-delay=uint32 5
```

If the `lock-delay` setting is missing, or is not set to `5` or less, and `uint32` is not included along with the integer key values as shown. Refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/locks/00-screensaver
```

Edit /etc/dconf/db/local.d/locks/00-screensaver and add or update the following lines:
Add the setting to enable session locking when a screensaver is activated:
The `uint32` must be included along with the integer key values as shown.

```
[org/gnome/desktop/screensaver]

lock-delay=uint32 5
```

Update the system databases:

```
# dconf update
```

Impact:

Users must log out and back in again before the system-wide settings take effect.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71901

Rule ID: SV-86525r3_rule

STIG ID: RHEL-07-010110

Severity: CAT II
```

2.2.2.6 Ensure automatic logon via GUI is not allowed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

Rationale:

Failure to restrict system unattended or automatic logon to the system negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.
Note: If the system does not have GNOME installed, this requirement is Not Applicable.
Check for the value of the `AutomaticLoginEnable` in the `/etc/gdm/custom.conf` file with the following command:

```
# grep -i automaticloginenable /etc/gdm/custom.conf

AutomaticLoginEnable=false
```

If the value of `AutomaticLoginEnable` is not set to `false`, refer to the remediation procedure below.

Remediation:

Configure the operating system to not allow an unattended or automatic logon to the system via a graphical user interface.
Add or edit the line for the `AutomaticLoginEnable` parameter in the [daemon] section of the `/etc/gdm/custom.conf` file to `false`:
Example: `vim /etc/gdm/custom.conf`

```
[daemon]
AutomaticLoginEnable=false
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71953

Rule ID: SV-86577r2_rule

STIG ID: RHEL-07-010440

Severity: CAT I
```

2.2.2.7 Ensure unrestricted logon is not allowed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not allow an unrestricted logon to the system.

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unrestricted logon to the system via a graphical user interface.
Note: If the system does not have GNOME installed, this requirement is Not Applicable.
Check for the value of the `TimedLoginEnable` parameter in `/etc/gdm/custom.conf` file with the following command:

```
# grep -i timedloginenable /etc/gdm/custom.conf

TimedLoginEnable=false
```

If the value of `TimedLoginEnable` is not set to `false`, refer to the remediation procedure below.

Remediation:

Configure the operating system to not allow an unrestricted account to log on to the system via a graphical user interface.
Add or edit the line for the `TimedLoginEnable` parameter in the [daemon] section of the `/etc/gdm/custom.conf` file to `false`:
Example: `vim /etc/gdm/custom.conf`

```
[daemon]
TimedLoginEnable=false
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71955

Rule ID: SV-86579r3_rule

STIG ID: RHEL-07-010450

Severity: CAT I
```

2.2.2.8 Ensure overriding the screensaver lock-delay setting is prevented (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system prevents a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.
Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.
Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user

system-db:local
```

Check for the lock delay setting with the following command:
Note: The example below is using the database `local` for the system, so the path is `/etc/dconf/db/local.d`. This path must be modified if a database other than `local` is being used.

```
# grep -i lock-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/lock-delay
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database `local` for the system, so if the system is using another database in `/etc/dconf/profile/user`, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver lock delay:

```
/org/gnome/desktop/screensaver/lock-delay
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-73155

Rule ID: SV-87807r4_rule

STIG ID: RHEL-07-010081

Severity: CAT II
```

2.2.2.9 Ensure session idle-delay settings is enforced (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system prevents a user from overriding session idle delay after a 15-minute period of inactivity for graphical user interfaces.
Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.
Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user

system-db:local
```

Check for the session idle delay setting with the following command:
Note: The example below is using the database `local` for the system, so the path is `/etc/dconf/db/local.d`. This path must be modified if a database other than `local` is being used.

```
# grep -i idle-delay /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/session/idle-delay
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a session lock after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database `local` for the system, so if the system is using another database in `/etc/dconf/profile/user`, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the session idle delay:

```
/org/gnome/desktop/session/idle-delay
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-73157

Rule ID: SV-87809r4_rule

STIG ID: RHEL-07-010082

Severity: CAT II
```

2.2.2.10 Ensure screensaver lock-enabled is set. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Audit:

Verify the operating system prevents a user from overriding the screensaver lock-enabled setting for the graphical user interface.
Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.
Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user

system-db:local
```

Check for the lock-enabled setting with the following command:
Note: The example below is using the database `local` for the system, so the path is `/etc/dconf/db/local.d`. This path must be modified if a database other than `local` is being used.

```
# grep -i lock-enabled /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/lock-enabled
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database `local` for the system, so if the system is using another database in `/etc/dconf/profile/user`, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver lock-enabled setting:

```
/org/gnome/desktop/screensaver/lock-enabled
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-78995

Rule ID: SV-93701r2_rule

STIG ID: RHEL-07-010062

Severity: CAT II
```

2.2.2.11 Ensure the screensaver idle-activation-enabled setting (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Audit:

Verify the operating system prevents a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.
Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.
Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user

system-db:local
```

Check for the idle-activation-enabled setting with the following command:
Note: The example below is using the database `local` for the system, so the path is `/etc/dconf/db/local.d`. This path must be modified if a database other than `local` is being used.

```
# grep -i idle-activation-enabled /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/screensaver/idle-activation-enabled
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database `local` for the system, so if the system is using another database in `/etc/dconf/profile/user`, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver idle-activation-enabled setting:

```
/org/gnome/desktop/screensaver/idle-activation-enabled
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-78997

Rule ID: SV-93703r2_rule

STIG ID: RHEL-07-010101

Severity: CAT II
```

2.2.3 Ensure X Window System is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to Verify X Windows System is not installed.

```
# rpm -qa xorg-x11*
```

Remediation:

Remove the X Windows System packages using the appropriate package manager.
OR

```
# yum remove xorg-x11*
```

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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72307

Rule ID: SV-86931r4_rule

STIG ID: RHEL-07-040730

Severity: CAT II
```

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 Avahi Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

Run the following command to disable `avahi-daemon`:

```
# systemctl disable avahi-daemon
```

Notes:

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

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.

2.2.5 Ensure CUPS is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

Run the following command to disable `cups` :

```
# systemctl disable cups
```

Impact:

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

References:

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

Notes:

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

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.

2.2.6 Ensure DHCP Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `dhcpd` is not enabled:

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

Remediation:

Run the following command to disable `dhcpd`:

```
# systemctl disable dhcpd
```

References:

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

Notes:

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

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.

2.2.7 Ensure LDAP server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

Run the following command to disable `slapd` :

```
# systemctl disable slapd
```

References:

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

Notes:

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

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.

2.2.8 Ensure NFS and RPC are not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

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

Run the following command and verify result is not "enabled":

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

Run the following command and verify result is not "enabled":

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

Remediation:

Run one of the following commands to disable nfs, nfs-server and rpcbind if it is reported enabled in the audit:

```
# systemctl disable nfs
# systemctl disable nfs-server
# systemctl disable rpcbind
```

Notes:

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

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.

2.2.9 Ensure DNS Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Unless a 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 `named` is not enabled:

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

Remediation:

Run the following command to disable `named` :

```
# systemctl disable named
```

Notes:

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

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.

2.2.10 Ensure FTP Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `vsftpd` is not enabled:

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

Remediation:

Run the following command to disable `vsftpd` :

```
# systemctl disable vsftpd
```

Notes:

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

Additional FTP servers also exist and should be audited.

```
This Benchmark recommendation maps to:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72299

Rule ID: SV-86923r3_rule

STIG ID: RHEL-07-040690

Severity: CAT I
```

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.

2.2.11 Ensure HTTP server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `httpd` is not enabled:

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

Remediation:

Run the following command to disable `httpd` :

```
# systemctl disable httpd
```

Notes:

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

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

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.

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `dovecot` is not enabled:

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

Remediation:

Run the following command to disable `dovecot` :

```
# systemctl disable dovecot
```

Notes:

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

Several IMAP/POP3 servers exist and can use other service names. `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.

2.2.13 Ensure Samba is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the 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 can be deleted to reduce the potential attack surface.

Audit:

Run the following command to verify `smb` is not enabled:

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

Remediation:

Run the following command to disable `smb` :

```
# systemctl disable smb
```

Notes:

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

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

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.

2.2.14 Ensure HTTP Proxy Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `squid` is not enabled:

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

Remediation:

Run the following command to disable `squid` :

```
# systemctl disable squid
```

Notes:

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

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

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.

2.2.15 Ensure SNMP Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

The SNMP server can communicate using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to disallow SNMP v1.

Audit:

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

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

Remediation:

Run the following command to disable `snmpd`:

```
# systemctl disable snmpd
```

Notes:

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

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.

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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'
```

If anything is return this will be an indication that the MTA is listening on a non-loopback address (`127.0.0.1` or `::1`), refer to the remediation procedure below.

Remediation:

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

```
inet_interfaces = loopback-only
```

Restart postfix with one of the following commands:

```
# systemctl restart postfix
```

Notes:

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

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.

2.2.17 Ensure rsync service is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `rsyncd` is not enabled:

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

Remediation:

Run the following command to disable `rsyncd` :

```
# systemctl disable rsyncd
```

Notes:

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

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

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.

2.2.18 Ensure NIS Server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to verify `ypserv` is not enabled:

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

Remediation:

Run the following command to disable `ypserv` :

```
# systemctl disable ypserv
```

Notes:

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

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

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.

2.2.19 Ensure rsh server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled rsh.socket
disabled
```

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled rlogin.socket
disabled
```

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled rexec.socket
disabled
```

Remediation:

Run the following commands to disable rsh , rlogin , and rexec :

```
# systemctl disable rsh.socket
# systemctl disable rlogin.socket
# systemctl disable rexec.socket
```

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.

2.2.20 Ensure telnet server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled telnet.socket
disabled
```

Remediation:

Run the following command to disable telnet:

```
# systemctl disable telnet.socket
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72077

Rule ID: SV-86701r2_rule

STIG ID: RHEL-07-021710

Severity: CAT I
```

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.

2.2.21 Ensure tftp server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled tftp.socket

disabled
```

Remediation:

Run the following command to disable tftp:

```
# systemctl disable tftp.socket
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72301

Rule ID: SV-86925r2_rule

STIG ID: RHEL-07-040700

Severity: CAT I
```

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.

2.2.22 Ensure rsync service is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled rsyncd

disabled
```

Remediation:

Run the following command to disable `rsync` :

```
# systemctl disable rsyncd
```

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.

2.2.23 Ensure talk server is not enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify result is not "enabled":

```
# systemctl is-enabled ntalk

disabled
```

Remediation:

Run the following command to disable talk:

```
# systemctl disable ntalk
```

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.

2.2.24 Ensure default SNMP community strings don't exist (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

SNMP community strings must be changed from the default values.

Rationale:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Audit:

Verify that a system using SNMP is not using default community strings.
Check to see if the `/etc/snmp/snmpd.conf` file exists with the following command:

```
# ls -al /etc/snmp/snmpd.conf
-rw------- 1 root root 52640 Mar 12 11:08 snmpd.conf
```

If the file does not exist, this is Not Applicable.
If the file does exist, check for the default community strings with the following commands:

```
# grep public /etc/snmp/snmpd.conf
# grep private /etc/snmp/snmpd.conf
```

If either of these commands returns any output, refer to the remediation procedure below.

Remediation:

If the `/etc/snmp/snmpd.conf` file exists, modify any lines that contain a community string value of `public` or `private` to another string value.
`Example: vim /etc/snmp/snmpd.conf`
Example of changing the `public` and `private` string value:

```
snmp-server community nEV8rM1ndthi$ RO
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72313

Rule ID: SV-86937r2_rule

STIG ID: RHEL-07-040800

Severity: CAT I
```

2.2.25 Ensure unrestricted mail relaying is prevented. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured to prevent unrestricted mail relaying.

Rationale:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Audit:

Verify the system is configured to prevent unrestricted mail relaying.
Determine if `postfix` is installed with the following commands:

```
# yum list installed postfix
postfix-2.6.6-6.el7.x86_64.rpm
```

If `postfix` is not installed, this is Not Applicable.
If `postfix` is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

```
# postconf -n smtpd_client_restrictions
smtpd_client_restrictions = permit_mynetworks, reject
```

If the `smtpd_client_restrictions` parameter contains any entries other than `permit_mynetworks` and `reject`, refer to the remediation procedure below.

Remediation:

If `postfix` is installed, modify the `/etc/postfix/main.cf` file to restrict client connections to the local network with the following command:

```
# postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

Or you can manually add this line by editing the file:
`Example: vim /etc/postfix/main.cf`
Add this line:

```
smtpd_client_restrictions = permit_mynetworks,reject
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72297

Rule ID: SV-86921r3_rule

STIG ID: RHEL-07-040680

Severity: CAT II
```

2.2.26 Ensure ldap_tls_cacert is set for LDAP. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications is set for ldap_tls_cacert.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

If LDAP is not being utilized, this requirement is Not Applicable.
Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.
To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset:
disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sssd.service` is `active`, then LDAP is being used.
Check that the path to the X.509 certificate for peer authentication with the following command:

```
# grep -i tls_cacert /etc/sssd/sssd.conf

ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

Verify the `ldap_tls_cacert` option points to a file that contains the trusted CA certificate. If this file does not exist, or the option is commented out or missing, refer to the remediation procedure.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.
Add or modify the following line in `/etc/sssd/sssd.conf`:
Example: `vim /etc/sssd/sssd.conf`
Add, uncomment or update the following line:

```
ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72231

Rule ID: SV-86855r3_rule

STIG ID: RHEL-07-040200

Severity: CAT II
```

2.2.27 Ensure ldap_id_use_start_tls is set for LDAP. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications setting ldap_id_use_start_tls.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

NOTE *** If LDAP is not being utilized, this requirement is Not Applicable.
Verify the operating system implements cryptography to protect the integrity of remote LDAP authentication sessions.
To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset:
disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sssd.service` is `active`, then LDAP is being used. To see if LDAP is configured to use TLS, use the following command:

```
# grep -i "start_tls" /etc/sssd/sssd.conf

ldap_id_use_start_tls = true
```

If the `ldap_id_use_start_tls` option is not `true`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP authentication sessions.
Add or modify the following line in `/etc/sssd/sssd.conf`:
Example: `vim /etc/sssd/sssd.conf`
Add, uncomment or update the following line:

```
ldap_id_use_start_tls = true
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72227

Rule ID: SV-86851r3_rule

STIG ID: RHEL-07-040180

Severity: CAT II
```

2.2.28 Ensure ldap_tls_reqcert is set for LDAP (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications by setting ldap_tls_reqcert.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

NOTE*** If LDAP is not being utilized, this requirement is Not Applicable.
Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.
To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset:
disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sssd.service` is `active`, then LDAP is being used.
Verify that the sssd service is configured to require the use of certificates:

```
# grep -i tls_reqcert /etc/sssd/sssd.conf

ldap_tls_reqcert = demand
```

If the `ldap_tls_reqcert` setting is missing, commented out, or does not exist, refer to the remediation procedure below.
If the `ldap_tls_reqcert` setting is not set to `demand` or `hard`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.
Add or modify the following line in `/etc/sssd/sssd.conf`:
Example: `vim /etc/sssd/sssd.conf`
Add, uncomment or update the following line:

```
ldap_tls_reqcert = demand
```

Notes:

This Benchmark Recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72229

Rule ID: SV-86853r3_rule

STIG ID: RHEL-07-040190

Severity: CAT II
```

2.2.29 Ensure nosuid option is set for NFS (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).

Rationale:

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that are being NFS imported are configured with the `nosuid` option. Find the file system(s) that contain the directories being exported with the following command:

```
# more /etc/fstab | grep nfs

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid 0 0
```

If a file system found in `/etc/fstab` refers to NFS and it does not have the `nosuid` option set, this is a finding.
Verify the NFS is mounted with the `nosuid` option:

```
# mount | grep nfs | grep nosuid
```

If no results are returned, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `nosuid` option on file systems that are being imported via NFS.
Example: `vim /etc/fstab`
Add, uncomment or update the NFS file systems identified in the Audit:

```
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid 0 0
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72045

Rule ID: SV-86669r2_rule

STIG ID: RHEL-07-021020

Severity: CAT II
```

2.2.30 Ensure NFS is configured to use RPCSEC_GSS. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

Rationale:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Audit:

Verify `AUTH_GSS` is being used to authenticate NFS mounts.
To check if the system is importing an NFS file system, look for any entries in the `/etc/fstab` file that have a file system type of `nfs` with the following command:

```
# cat /etc/fstab | grep nfs

192.168.21.5:/mnt/export /data1 nfs4 rw,sync ,soft,sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and has the sec option without the `krb5:krb5i:krb5p` settings, the `sec` option has the `sys` setting, or the `sec` option is missing, refer to the remediation procedure below.

Remediation:

Update the `/etc/fstab` file so the option `sec` is defined for each NFS mounted file system and the `sec` option does not have the `sys` setting.
Example: `vim /etc/fstab`
Ensure the `sec` option is defined as `krb5:krb5i:krb5p`.

```
192.168.21.5:/mnt/export /data1 nfs4 rw,sync ,soft,sec=krb5:krb5i:krb5p
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72311

Rule ID: SV-86935r4_rule

STIG ID: RHEL-07-040750

Severity: CAT II
```

2.2.31 Ensure noexec option is configured for NFS. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).

Rationale:

The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that are being NFS imported are configured with the `noexec` option. Find the file system(s) that contain the directories being imported with the following command:

```
# more /etc/fstab | grep nfs

UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,noexec 0 0
```

If a file system found in `/etc/fstab` refers to NFS and it does not have the `noexec` option set, and use of NFS imported binaries is not documented with the Authorizing Official as an operational requirement, refer to the remediation procedure below.
Verify the NFS is mounted with the `noexec`option:

```
# mount | grep nfs | grep noexec
```

If no results are returned and use of NFS imported binaries is not documented with the Authorizing Official as an operational requirement, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `noexec` option on file systems that are being imported via NFS.
Example: `vim /etc/fstab`
Add, or update any NFS file systems found in the Audit to include the `noexec` option:

```
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,noexec 0 0
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-73161

Rule ID: SV-87813r2_rule

STIG ID: RHEL-07-021021

Severity: CAT II
```

2.3 Service Clients

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

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

2.3.1 Ensure NIS Client is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Verify `ypbind` is not installed.
Run the following command:

```
# rpm -q ypbind

package ypbind is not installed
```

Remediation:

Uninstall `ypbind` using the appropriate package manager:
OR

```
# yum remove ypbind
```

Impact:

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

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

2.3.2 Ensure rsh client is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Verify `rsh` is not installed.
Run the following command:

```
# rpm -q rsh

package rsh is not installed
```

Remediation:

Uninstall `rsh` using the appropriate package manager:
OR

```
# yum remove rsh
```

Impact:

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

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.

2.3.3 Ensure talk client is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Verify `talk` is not installed.
Run the following command:

```
# rpm -q talk

package talk is not installed
```

Remediation:

Uninstall `talk` using the appropriate package manager:
OR

```
# yum remove talk
```

Impact:

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

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

2.3.4 Ensure telnet client is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Verify `telnet` is not installed.
Run the following command:

```
# rpm -q telnet

package telnet is not installed
```

Remediation:

Uninstall `telnet` using the appropriate package manager.
OR

```
# yum remove telnet
```

Impact:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72077

Rule ID: SV-86701r2_rule

STIG ID: RHEL-07-021710

Severity: CAT I
```

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.

2.3.5 Ensure LDAP client is not installed (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Verify openldap-clients is not installed.
Run the following command:

```
# rpm -q openldap-clients

package openldap-clients is not installed
```

Remediation:

Uninstall `openldap-clients` using the appropriate package manager.
OR

```
# yum remove openldap-clients
```

Impact:

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

Notes:

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

CIS Controls:

Version 7

2.6 Address unapproved software

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

3 Network Configuration

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

3.1 Network Parameters (Host Only)

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

3.1.1 Ensure IP forwarding is disabled (Scored)

Profile Applicability:

- Level 1

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 command and verify output matches:

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

# grep "net\.ipv4\.ip_forward" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.ip_forward = 0

# sysctl net.ipv6.conf.all.forwarding
net.ipv6.conf.all.forwarding = 0

# grep "net\.ipv6\.conf\.all\.forwarding" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv6.conf.all.forwarding = 0
```

Remediation:

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

```
net.ipv4.ip_forward = 0
net.ipv6.conf.all.forwarding = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.ip_forward=0
# sysctl -w net.ipv6.conf.all.forwarding=0
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72309

Rule ID: SV-86933r2_rule

STIG ID: RHEL-07-040740

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.1.2 Ensure packet redirect sending is disabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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 "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*
net.ipv4.conf.all.send_redirects = 0

# grep "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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72293

Rule ID: SV-86917r3_rule

STIG ID: RHEL-07-040660

Severity: CAT II



Vul ID: V-72291

Rule ID: SV-86915r4_rule

STIG ID: RHEL-07-040650

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.1.3 Ensure network interfaces are not in promiscuous mode (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

Network interfaces configured on the operating system must not be in promiscuous mode.

Rationale:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow then to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Audit:

Verify network interfaces are not in promiscuous mode unless approved and documented. Check for the status with the following command:

```
# ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved and documented, refer to the remediation procedure below.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved and documented.
Set the promiscuous mode of an interface to off with the following command:

```
#ip link set dev <devicename> multicast off promisc off
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72295

Rule ID: SV-86919r2_rule

STIG ID: RHEL-07-040670

Severity: CAT II
```

3.2 Network Parameters (Host and Router)

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

3.2.1 Ensure source routed packets are not accepted (Scored)

Profile Applicability:

- Level 1

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

# 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
```

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
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.ipv4.conf.all.accept_source_route=0
# sysctl -w net.ipv4.conf.default.accept_source_route=0
# sysctl -w net.ipv6.conf.all.accept_source_route=0
# sysctl -w net.ipv6.conf.default.accept_source_route=0
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72283

Rule ID: SV-86907r2_rule

STIG ID: RHEL-07-040610

Severity: CAT II


Vul ID: V-72285

Rule ID: SV-86909r2_rule

STIG ID: RHEL-07-040620

Severity: CAT II


Vul ID: V-72319

Rule ID: SV-86943r2_rule

STIG ID: RHEL-07-040830

Severity: CAT II
```

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 ICMP redirects are not accepted (Scored)

Profile Applicability:

- Level 1

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects` 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

# 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
```

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
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.ipv4.conf.all.accept_redirects=0
# sysctl -w net.ipv4.conf.default.accept_redirects=0
# sysctl -w net.ipv6.conf.all.accept_redirects=0
# sysctl -w net.ipv6.conf.default.accept_redirects=0
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72289

Rule ID: SV-86913r3_rule

STIG ID: RHEL-07-040640

Severity: CAT II



Vul ID: V-73175

Rule ID: SV-87827r4_rule

STIG ID: RHEL-07-040641

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.2.3 Ensure secure ICMP redirects are not accepted (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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.

3.2.4 Ensure suspicious packets are logged (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

3.2.5 Ensure broadcast ICMP requests are ignored (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72287

Rule ID: SV-86911r2_rule

STIG ID: RHEL-07-040630

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.2.6 Ensure bogus ICMP responses are ignored (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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.

3.2.7 Ensure Reverse Path Filtering is enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Setting these flags is a good way to deter attackers from sending your 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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-92251

Rule ID: SV-102353r1_rule

STIG ID: RHEL-07-040611

Severity: CAT II



Vul ID: V-92253

Rule ID: SV-102355r1_rule

STIG ID: RHEL-07-040612

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.2.8 Ensure TCP SYN Cookies is enabled (Scored)

Profile Applicability:

- Level 1

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the 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.

3.2.9 Ensure IPv6 router advertisements are not accepted (Scored)

Profile Applicability:

- Level 1

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:

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
```

Remediation:

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.

3.2.10 Ensure rate limiting measures are set. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

Verify the operating system protects against or limits the effects of DoS attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

```
# grep 'net.ipv4.tcp_invalid_ratelimit' /etc/sysctl.conf /etc/sysctl.d/*

/etc/sysctl.conf:net.ipv4.tcp_invalid_ratelimit = 500
```

If `net.ipv4.tcp_invalid_ratelimit` is not configured in the `/etc/sysctl.conf` file or in the `/etc/sysctl.d/` directory, is commented out refer to the remediation procedure below.
Check that the operating system implements the value of the `tcp_invalid_ratelimit` variable with the following command:

```
# /sbin/sysctl -a | grep 'net.ipv4.tcp_invalid_ratelimit'
net.ipv4.tcp_invalid_ratelimit = 500
```

If `net.ipv4.tcp_invalid_ratelimit` has a value of `0`, refer to the remediation procedure below.
If `net.ipv4.tcp_invalid_ratelimit` has a value greater than `1000` and is not documented, refer to the remediation procedure below.

Remediation:

Set the system to implement rate-limiting measures by adding the following line to `/etc/sysctl.conf` or a configuration file in the `/etc/sysctl.d/` directory (or modify the line to have the required value):
Example: `vim /etc/sysctl.conf`

```
net.ipv4.tcp_invalid_ratelimit = 500
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72271

Rule ID: SV-86895r3_rule

STIG ID: RHEL-07-040510

Severity: CAT II
```

3.3 TCP Wrappers

3.3.1 Ensure TCP Wrappers is installed (Scored)

Profile Applicability:

- Level 1

Description:

Many Linux distributions provide value-added firewall solutions which provide easy, advanced management of network traffic into and out of the local system. When these solutions are available and appropriate for an environment they should be used.

In cases where a value-added firewall is not provided by a distribution, TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. Services that are called from `inetd` and `xinetd` support the use of TCP wrappers. Any service that can support TCP wrappers will have the `libwrap.so` library attached to it.

Rationale:

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

Audit:

Run the following command and verify TCP Wrappers is installed:

```
# rpm -q tcp_wrappers

tcp_wrappers-<version>
```

Run the following command and verify libwrap.so is installed:

```
# rpm -q tcp_wrappers-libs

tcp_wrappers-libs-<version>
```

Remediation:

Run the following command to install TCP Wrappers:

```
# yum install tcp_wrappers
```

Impact:

Some Linux distributions have deprecated the use of TCP Wrappers in favor of value-added firewall solutions. In these cases the provided firewall solution should be used.

Notes:

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

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

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

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.

3.3.2 Ensure /etc/hosts.allow is configured (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
# cat /etc/hosts.allow
```

Remediation:

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

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

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

Notes:

Contents of the `/etc/hosts.allow` file will vary depending on your network configuration.

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.

3.3.3 Ensure /etc/hosts.deny is configured (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command and verify the contents of the `/etc/hosts.deny` file:

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

Remediation:

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

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

Notes:

Contents of the `/etc/hosts.deny` file may include additional options depending on your network configuration.

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.

3.3.4 Ensure permissions on /etc/hosts.allow are configured (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

Run the following commands to set permissions on `/etc/hosts.allow`:

```
# chown root:root /etc/hosts.allow
# chmod 644 /etc/hosts.allow
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

3.3.5 Ensure permissions on /etc/hosts.deny are configured (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

Run the following commands to set permissions on `/etc/hosts.deny` :

```
# chown root:root /etc/hosts.deny
# chmod 644 /etc/hosts.deny
```

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 (Scored)

Profile Applicability:

- Level 2

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: `vim /etc/modprobe.d/dccp.conf`
and add the following line:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-77821

Rule ID: SV-92517r2_rule

STIG ID: RHEL-07-020101

Severity: CAT II
```

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 (Scored)

Profile Applicability:

- Level 2

Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

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

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

# lsmod | grep sctp
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /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 (Scored)

Profile Applicability:

- Level 2

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: `vim /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 (Scored)

Profile Applicability:

- Level 2

Description:

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Audit:

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

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

# lsmod | grep tipc
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /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 Provides defense against external and internal threats by refusing unauthorized connections, to stop intrusion and provide a strong method of access control policy.

this section is intended only to ensure the resulting firewall rules are in place, not how they are configured.

3.5.1 Configure iptables

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.

3.5.1.1 Ensure Firewall software is installed

In order to configure Firewall protection for you system, a Firewall software package needs to be installed

3.5.1.1.1 Ensure iptables is installed (Scored)

Profile Applicability:

- Level 1

Description:

`iptables` allows configuration of the IPv4 and IPv6 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to `iptables`.

Rationale:

iptables is required for firewall management and configuration.

Audit:

Run the following command and verify iptables is installed:

```
# rpm -q iptables

iptables-<version>
```

Remediation:

Run the following command to install `iptables`:

```
# yum install iptables
```

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 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
```

3.5.1.2.1 Ensure default deny firewall policy (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the `INPUT` , `OUTPUT` , and `FORWARD` chains is `DROP` or `REJECT` :

```
# iptables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

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.

3.5.1.2.2 Ensure loopback traffic is configured (Scored)

Profile Applicability:

- Level 1

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       127.0.0.0/8          0.0.0.0/0

 # iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

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.

3.5.1.2.3 Ensure outbound and established connections are configured (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure the firewall rules for new outbound, and established connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

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.

3.5.1.2.4 Ensure firewall rules exist for all open ports (Scored)

Profile Applicability:

- Level 1

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# 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
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72219

Rule ID: SV-86843r2_rule

STIG ID: RHEL-07-040100

Severity: CAT II
```

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.

3.5.1.3 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
```

3.5.1.3.1 Ensure IPv6 default deny firewall policy (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

OR
If IPv6 is disabled:
Run the following command and verify that no lines are returned.

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

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.

3.5.1.3.2 Ensure IPv6 loopback traffic is configured (Scored)

Profile Applicability:

- Level 1

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

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
If IPv6 is disabled:
Run the following command and verify that no lines are returned.

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1
```

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
```

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.

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.

3.5.1.3.3 Ensure IPv6 outbound and established connections are configured (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# ip6tables -L -v -n
```

OR
If IPv6 is disabled:
Run the following command and verify that no lines are returned.

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1
```

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
```

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.

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.

3.5.1.3.4 Ensure IPv6 firewall rules exist for all open ports (Not Scored)

Profile Applicability:

- Level 1

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# 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
If IPv6 is disabled:
Run the following command and verify that no lines are returned.

```
# grep "^\s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1
```

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
```

Notes:

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

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

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.

3.6 Disable IPv6 (Not Scored)

Profile Applicability:

- Level 2

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.

Audit:

Depending or your distribution, run the appropriate following command and verify no lines should be returned.

```
#  grep "^\s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disabled=1
```

or

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

Remediation:

Edit `/etc/default/grub` and add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

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

Depending or your distribution, run the appropriate following command to update the `grub2` configuration:

```
# grub2-mkconfig –o /boot/grub2/grub.cfg
```

or

```
# update-grub
```

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.

3.7 Ensure IP tunnels are not configured. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have unauthorized IP tunnels configured.

Rationale:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the the Authorizing Official of the organization.

Audit:

Verify the system does not have unauthorized IP tunnels configured.
Check to see if `libreswan` is installed with the following command:

```
# yum list installed libreswan
libreswan.x86-64 3.20-5.el7_4
```

If `libreswan` is installed, check to see if the `IPsec` service is active with the following command:

```
# systemctl status ipsec
ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled)
Active: inactive (dead)
```

If the `IPsec` service is active, check to see if any tunnels are configured in `/etc/ipsec.conf` and `/etc/ipsec.d/` with the following commands:

```
# grep -iw conn /etc/ipsec.conf /etc/ipsec.d/*.conf
```

If there are indications that a `conn` parameter is configured for a tunnel, ask if the tunnel is documented.
If `libreswan` is installed, `IPsec` is active, and an undocumented tunnel is active, refer to the remediation procedure below.

Remediation:

Remove all unapproved tunnels from the system, or document them with the Authorizing Official.
To remove them edit the `/etc/ipsec.conf` and `/etc/ipsec.d/*.conf` files removing any lines indicating a `conn` parameter is configured.
Example: `vim /etc/ipsec.conf`

```
Remove and lines with a "conn" parameter set.
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72317

Rule ID: SV-86941r2_rule

STIG ID: RHEL-07-040820

Severity: CAT II
```

4 Logging and Auditing

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

It is recommended that `rsyslog`be used for logging (with `logwatch`providing summarization) and `auditd` be used for auditing (with `aureport`providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the `ntpd(8)` manual page for more information on configuring NTP.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640`where `securegrp`is the defined security group (in some cases `wheel`).

4.1 Configure System Accounting (auditd)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, auditd will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations. **Note:** For 64 bit systems that have arch as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems. For 32 bit systems, only one rule is needed.

Note: Several recommendations in this section filter based off of `auid>=500` for unprivileged non-system users. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

Note: Once all configuration changes have been made to `/etc/audit/rules.d/audit.rules`, the auditd configuration must be reloaded with the following command:

```
# service auditd reload
```

4.1.1 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

4.1.1.1 Ensure audit log storage size is configured (Scored)

Profile Applicability:

- Level 2

Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

Audit:

Run the following command and ensure output is in compliance with site policy:

```
# grep max_log_file /etc/audit/auditd.conf

max_log_file = <MB>
```

Remediation:

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

Notes:

The max_log_file parameter is measured in megabytes.

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.

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.

4.1.1.2 Ensure system is disabled when audit logs are full (Scored)

Profile Applicability:

- Level 2

Description:

The `auditd` daemon can be configured to halt the system when the audit logs are full.

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Audit:

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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72091

Rule ID: SV-86715r2_rule

STIG ID: RHEL-07-030340

Severity: CAT II



Vul ID: V-72093

Rule ID: SV-86717r3_rule

STIG ID: RHEL-07-030350

Severity: CAT II
```

CIS Controls:

Version 7

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

4.1.1.3 Ensure audit logs are not automatically deleted (Scored)

Profile Applicability:

- Level 2

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

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

4.1.1.4 Ensure audit logs are stored on a different system. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must off-load audit records onto a different system or media from the system being audited.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Verify the operating system off-loads audit records onto a different system or media from the system being audited.
To determine the remote server that the records are being sent to, use the following command:

```
# grep -i remote_server /etc/audisp/audisp-remote.conf
remote_server = 10.0.21.1
```

If a remote server is not configured, or the line is commented out, ask how the audit logs are off-loaded to a different system or media.
If there is no evidence that the audit logs are being off-loaded to another system or media, refer to the remediation procedure below.

Remediation:

Configure the operating system to off-load audit records onto a different system or media from the system being audited.
Set the remote server option in `/etc/audisp/audisp-remote.conf` with the IP address of the log aggregation server.
Example: `vim /etc/audisp/audisp-remote.conf`
Add, uncomment or update the following line:
Note: The ip address listed is just for an example. Replace it with the IP address or the log aggregation server in your environment.

```
remote_server = 10.0.21.1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72083

Rule ID: SV-86707r2_rule

STIG ID: RHEL-07-030300

Severity: CAT II
```

4.1.1.5 Ensure audit logs on seperate system are encrypted. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited and encrypted the records.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading and encrypting is a common process in information systems with limited audit storage capacity.

Audit:

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited.
To determine if the transfer is encrypted, use the following command:

```
# grep -i enable_krb5 /etc/audisp/audisp-remote.conf
enable_krb5 = yes
```

If the value of the `enable_krb5` option is not set to `yes` or the line is commented out, ask how the audit logs are off-loaded to a different system or media.
If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, refer to the remediation procedure below.

Remediation:

Configure the operating system to encrypt the transfer of off-loaded audit records onto a different system or media from the system being audited.
Add or update the `/etc/audisp/audisp-remote.conf` and set it with the following line:
Example: `vim /etc/audisp/audisp-remote.conf`
Add, uncomment or update the following line:

```
enable_krb5 = yes
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72085

Rule ID: SV-86709r2_rule

STIG ID: RHEL-07-030310

Severity: CAT II
```

4.1.2 Configure audit of commands

When auditing, it is important to configure successful and unsuccessful attempts to run certain commands. By default, auditd does not monitor these commands and their actions. In order to recreate negligent actions audit files must be kept for the commands listed in this sub-section so that it can be determined what was attempted on the system.

4.1.2.1 Ensure all uses of the passwd command are audited. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the passwd command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `passwd` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/passwd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/passwd -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `passwd` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, update or uncomment this line below

```
-a always,exit -F path=/usr/bin/passwd -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72149

Rule ID: SV-86773r5_rule

STIG ID: RHEL-07-030630

Severity: CAT II
```

4.1.2.2 Ensure auditing of the unix_chkpwd command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the unix_chkpwd command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `unix_chkpwd` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -iw /usr/sbin/unix_chkpwd /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/unix_chkpwd -F auid>=1000 -F
auid!=4294967295 -k privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unix_chkpwd` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update this line:

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F auid>=1000 -F
auid!=4294967295 -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72151

Rule ID: SV-86775r5_rule

STIG ID: RHEL-07-030640

Severity: CAT II
```

4.1.2.3 Ensure audit of the gpasswd command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the gpasswd command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `gpasswd` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/gpasswd /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/gpasswd -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `gpasswd` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/gpasswd -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72153

Rule ID: SV-86777r5_rule

STIG ID: RHEL-07-030650

Severity: CAT II
```

4.1.2.4 Ensure audit all uses of chage (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the chage command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chage` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/chage /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chage -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chage` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the line:

```
-a always,exit -F path=/usr/bin/chage -F auid>=1000 -F auid!=4294967295 -k
privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72155

Rule ID: SV-86779r5_rule

STIG ID: RHEL-07-030660

Severity: CAT II
```

4.1.2.5 Ensure audit all uses of the newgrp command. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the newgrp command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `newgrp` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -i /usr/bin/newgrp /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/newgrp -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `newgrp` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/newgrp -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72165

Rule ID: SV-86789r4_rule

STIG ID: RHEL-07-030710

Severity: CAT II
```

4.1.2.6 Ensure audit all uses of the chsh command. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the chsh command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chsh` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -i /usr/bin/chsh /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chsh -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chsh` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/chsh -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72167

Rule ID: SV-86791r4_rule

STIG ID: RHEL-07-030720

Severity: CAT II
```

4.1.2.7 Ensure audit the umount command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the umount command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `umount` command occur.
Check that the following system call is being audited by performing the following series of commands to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw "/usr/bin/umount" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/umount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `umount` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/umount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark Recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72173

Rule ID: SV-86797r5_rule

STIG ID: RHEL-07-030750

Severity: CAT II
```

4.1.2.8 Ensure audit of postdrop command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the postdrop command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `postdrop` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/sbin/postdrop /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postdrop -F auid>=1000 -F auid!=4294967295 -
k privileged-postfix
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `postdrop` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/postdrop -F auid>=1000 -F auid!=4294967295 -
k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendations maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72175

Rule ID: SV-86799r4_rule

STIG ID: RHEL-07-030760

Severity: CAT II
```

4.1.2.9 Ensure audit of postqueue command. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the postqueue command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `postqueue` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/sbin/postqueue /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postqueue -F auid>=1000 -F auid!=4294967295
-k privileged-postfix
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `postqueue` command occur.
Add or update the following rule in /etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/postqueue -F auid>=1000 -F auid!=4294967295
-k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72177

Rule ID: SV-86801r3_rule

STIG ID: RHEL-07-030770

Severity: CAT II
```

4.1.2.10 Enusre audit ssh-keysign command. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the ssh-keysign command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `ssh-keysign` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/libexec/openssh/ssh-keysign /etc/audit/audit.rules

-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F auid>=1000 -F
auid!=4294967295 -k privileged-ssh
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `ssh-keysign` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F auid>=1000 -F
auid!=4294967295 -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72179

Rule ID: SV-86803r3_rule

STIG ID: RHEL-07-030780

Severity: CAT II
```

4.1.2.11 Ensure audit of crontab command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the crontab command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `crontab` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/bin/crontab /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/crontab -F auid>=1000 -F auid!=4294967295 -k
privileged-cron
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `crontab` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/crontab -F auid>=1000 -F auid!=4294967295 -k
privileged-cron
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72183

Rule ID: SV-86807r3_rule

STIG ID: RHEL-07-030800

Severity: CAT II
```

4.1.2.12 Ensure audit pam_timestamp_check command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the pam_timestamp_check command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `pam_timestamp_check` command occur.
Check the auditing rules in `/etc/audit/audit.rules` with the following command:

```
# grep -iw "/usr/sbin/pam_timestamp_check" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/pam_timestamp_check -F auid>=1000 -F
auid!=4294967295 -k privileged-pam
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `pam_timestamp_check` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F auid>=1000 -F
auid!=4294967295 -k privileged-pam
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72185

Rule ID: SV-86809r4_rule

STIG ID: RHEL-07-030810

Severity: CAT II
```

4.1.2.13 Ensure audit of kmod command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the kmod command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `kmod` command occur.
Check the auditing rules in `/etc/audit/audit.rules` with the following command:

```
# grep -iw kmod /etc/audit/audit.rules

-w /usr/bin/kmod -p x -F auid!=4294967295 -k module-change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `kmod` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-w /usr/bin/kmod -p x -F auid!=4294967295 -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72191

Rule ID: SV-86815r5_rule

STIG ID: RHEL-07-030840

Severity: CAT II
```

4.1.2.14 Ensure audit of the rmdir syscall (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the rmdir syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `rmdir` syscall occur.
Check the file system rules in `/etc/audit/audit.rules` with the following commands:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw rmdir /etc/audit/audit.rules

-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete
```

If there are no audit rules defined for the `rmdir` syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `rmdir` syscall occur.
Add the following rules in `/etc/audit/rules.d/audit.rules`:
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line that fits your system architecture:

```
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete

-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72203

Rule ID: SV-86827r4_rule

STIG ID: RHEL-07-030900

Severity: CAT II
```

4.1.2.15 Ensure audit of unlink syscall (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the unlink syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `unlink` syscall occur.
Check the file system rules in `/etc/audit/audit.rules` with the following commands:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw unlink /etc/audit/audit.rules

-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=4294967295 -k
delete
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=4294967295 -k
delete
```

If there are no audit rules defined for the `unlink` syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unlink` syscall occur.
Add the following rules in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line depending on your system architecture:
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=4294967295 -k
delete

-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=4294967295 -k
delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72205

Rule ID: SV-86829r4_rule

STIG ID: RHEL-07-030910

Severity: CAT II
```

4.1.2.16 Ensure audit unlinkat syscall (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the unlinkat syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `unlinkat` syscall occur.
Check the file system rules in `/etc/audit/audit.rules` with the following commands:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw unlinkat /etc/audit/audit.rules

-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete
```

If there are no audit rules defined for the `unlinkat` syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unlinkat` syscall occur.
Add the following rules in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment, update the following line for the appropriate system architecture.
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete

-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72207

Rule ID: SV-86831r4_rule

STIG ID: RHEL-07-030920

Severity: CAT II
```

4.1.2.17 Ensure audit of the create_module syscall. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the create_module syscall.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `create_module` syscall occur.
Check the auditing rules in `/etc/audit/audit.rules` with the following command:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
# grep -iw create_module /etc/audit/audit.rules

-a always,exit -F arch=b32 -S create_module -k module-change
-a always,exit -F arch=b64 -S create_module -k module-change
```

If there are no audit rules defined for `create_module`, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `create_module` syscall occur.
Add or update the following rules in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.
Add, uncomment or update the following line appropriate for the architecture you are running.

```
-a always,exit -F arch=b32 -S create_module -k module-change

-a always,exit -F arch=b64 -S create_module -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-78999

Rule ID: SV-93705r2_rule

STIG ID: RHEL-07-030819

Severity: CAT II
```

4.1.2.18 Ensure audit of the finit_module syscall (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the finit_module syscall.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `finit_module` syscall occur.
Check the auditing rules in `/etc/audit/audit.rules` with the following command:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
# grep -iw finit_module /etc/audit/audit.rules

-a always,exit -F arch=b32 -S finit_module -k module-change
-a always,exit -F arch=b64 -S finit_module -k module-change
```

If there are no audit rules defined for `finit_module`, refer to the remediation below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `finit_module` syscall occur.
Add or update the following rules in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.
Add, uncomment or update the following line for the appropriate architecture:

```
-a always,exit -F arch=b32 -S finit_module -k module-change

-a always,exit -F arch=b64 -S finit_module -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-79001

Rule ID: SV-93707r2_rule

STIG ID: RHEL-07-030821

Severity: CAT II
```

4.1.2.19 Ensure audit of semanage command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the semanage command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `semanage` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/semanage /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/semanage -F auid>=1000 -F auid!=4294967295 -
k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `semanage` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/semanage -F auid>=1000 -F auid!=4294967295 -
k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72135

Rule ID: SV-86759r4_rule

STIG ID: RHEL-07-030560

Severity: CAT II
```

4.1.2.20 Ensure audit of the setsebool command. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the setsebool command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `setsebool` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/setsebool /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setsebool -F auid>=1000 -F auid!=4294967295
-k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `setsebool` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/setsebool -F auid>=1000 -F auid!=4294967295
-k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72137

Rule ID: SV-86761r4_rule

STIG ID: RHEL-07-030570

Severity: CAT II
```

4.1.2.21 Ensure audit of the chcon command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the chcon command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chcon`` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/chcon /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chcon -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chcon` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/chcon -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72139

Rule ID: SV-86763r4_rule

STIG ID: RHEL-07-030580

Severity: CAT II
```

4.1.2.22 Ensure audit of setfiles command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the setfiles command.

Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `setfiles` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -iw /usr/sbin/setfiles /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setfiles -F auid>=1000 -F auid!=4294967295 -
k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `setfiles` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/setfiles -F auid>=1000 -F auid!=4294967295 -
k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72141

Rule ID: SV-86765r5_rule

STIG ID: RHEL-07-030590

Severity: CAT II
```

4.1.2.23 Ensure audit of the userhelper command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the userhelper command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `userhelper` command occur.
Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/userhelper /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/userhelper -F auid>=1000 -F auid!=4294967295
-k privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `userhelper` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/userhelper -F auid>=1000 -F auid!=4294967295
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72157

Rule ID: SV-86781r5_rule

STIG ID: RHEL-07-030670

Severity: CAT II
```

4.1.2.24 Ensure audit of the su command (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the su command.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `su` command occur.
Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/bin/su /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/su -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `su` command occur.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Add the following line:

```
-a always,exit -F path=/usr/bin/su -F auid>=1000 -F auid!=4294967295 -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72159

Rule ID: SV-86783r5_rule

STIG ID: RHEL-07-030680

Severity: CAT II
```

4.1.2.25 Ensure audit of the mount command and syscall (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all uses of the mount command and syscall.

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `mount` command and syscall occur.
Check that the following system call is being audited by performing the following series of commands to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw "mount" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F path=/usr/bin/mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

If all uses of the `mount` command and syscall are not being audited, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `mount` command and syscall occur.
Add or update the following rules in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.
Add the following lines appropriate for the architecture:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F path=/usr/bin/mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72171

Rule ID: SV-86795r6_rule

STIG ID: RHEL-07-030740

Severity: CAT II
```

4.1.3 Ensure auditd service is enabled (Scored)

Profile Applicability:

- Level 2

Description:

Turn on the `auditd` daemon to record system events.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd

enabled
```

Remediation:

Run the following command to enable `auditd` :

```
# systemctl --now enable auditd
```

Notes:

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.

4.1.4 Ensure auditing for processes that start prior to auditd is enabled (Scored)

Profile Applicability:

- Level 2

Description:

Configure `grub` so that processes that are capable of being audited can be audited even if they start up prior to `auditd` startup.

Rationale:

Audit events need to be captured on processes that start up prior to `auditd`, so that potential malicious activity cannot go undetected.

Audit:

For `grub2` based systems run the following command and verify that each linux line has the `audit=1` parameter set:

```
# grep "^\s*linux" /boot/grub2/grub.cfg
```

Remediation:

For `grub2` based systems edit `/etc/default/grub` and add `audit=1` to `GRUB_CMDLINE_LINUX`:

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

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

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

Notes:

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

Replace `/boot/grub2/grub.cfg` or `/boot/grub/menu.lst` with the appropriate grub configuration file for your environment.

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.

4.1.5 Ensure events that modify date and time information are collected (Scored)

Profile Applicability:

- Level 2

Description:

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the `adjtimex` (tune kernel clock), `settimeofday` (Set time, using timeval and timezone structures) `stime` (using seconds since 1/1/1970) or `clock_settime` (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the `/var/log/audit.log` file upon exit, tagging the records with the identifier "time-change"

Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Audit:

On a 32 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules

# auditctl -l | grep time-change
```

Verify output of both 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
```

On a 64 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules

# auditctl -l | grep time-change
```

Verify output of both 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
```

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/audit.rules`
and 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/audit.rules`
and 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
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

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 user/group information are collected (Scored)

Profile Applicability:

- Level 2

Description:

Record events affecting the `group` , `passwd` (user IDs), `shadow` and `gshadow` (passwords) or `/etc/security/opasswd` (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Audit:

Run the following commands:

```
# grep identity /etc/audit/rules.d/*.rules

# auditctl -l | grep identity
```

Verify output of both 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/audit.rules`
and 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
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72197

Rule ID: SV-86821r5_rule

STIG ID: RHEL-07-030870

Severity: CAT II



Vul ID: V-73165

Rule ID: SV-87817r3_rule

STIG ID: RHEL-07-030871

Severity: CAT II



Vul ID: V-73167

Rule ID: SV-87819r4_rule

STIG ID: RHEL-07-030872

Severity: CAT II
```

```
Vul ID: V-73171

Rule ID: SV-87823r4_rule

STIG ID: RHEL-07-030873

Severity: CAT II


Vul ID: V-73173

Rule ID: SV-87825r5_rule

STIG ID: RHEL-07-030874

Severity: CAT II
```

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.

4.1.7 Ensure events that modify the system's network environment are collected (Scored)

Profile Applicability:

- Level 2

Description:

Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the `/etc/issue` and `/etc/issue.net` files (messages displayed pre-login), `/etc/hosts` (file containing host names and associated IP addresses) and `/etc/sysconfig/network` (directory containing network interface scripts and configurations) files.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Audit:

On a 32 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules

# auditctl -l | grep system-locale
```

Verify output of both 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/sysconfig/network -p wa -k system-locale
```

On a 64 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules

# auditctl -l | grep system-locale
```

Verify output of both 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/sysconfig/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/audit.rules`
and 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/sysconfig/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/audit.rules`
and 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/sysconfig/network -p wa -k system-locale
```

Notes:

`/etc/sysconfig/network` is common to Red Hat and SUSE based distributions.

You should expand or replace this coverage to any network configuration files on your system such as `/etc/network` on Debian based distributions.

Reloading the auditd config to set active settings may require a system reboot.

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.

4.1.8 Ensure events that modify the system's Mandatory Access Controls are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor SELinux/AppArmor mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or /etc/apparmor and /etc/apparmor.d directories.

Rationale:

Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit:

On systems using SELinux run the following commands:

```
# grep MAC-policy /etc/audit/rules.d/*.rules

# auditctl -l | grep MAC-policy
```

Verify output of both matches:

```
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
```

Remediation:

On systems using SELinux Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/audit.rules`
and add the following lines:

```
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

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.

4.1.9 Ensure login and logout events are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file `/var/log/faillog` tracks failed events from login. The file `/var/log/lastlog` maintain records of the last time a user successfully logged in. The file `/var/log/tallylog` maintains records of failures via the `pam_tally2` module

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

Run the following commands:

```
# grep logins /etc/audit/rules.d/*.rules

# auditctl -l | grep logins
```

Verify output of both includes:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock/ -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/audit.rules`
and add the following lines:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock/ -p wa -k logins
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72145

Rule ID: SV-86769r4_rule

STIG ID: RHEL-07-030610

Severity: CAT II


Vul ID: V-72147

Rule ID: SV-86771r3_rule

STIG ID: RHEL-07-030620

Severity: CAT II
```

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.

4.1.10 Ensure session initiation information is collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file `/var/run/utmp` 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."

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 commands:

```
# grep -E '(session|logins)' /etc/audit/rules.d/*.rules

# auditctl -l | grep -E '(session|logins)'
```

Verify output of both 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/audit.rules`
and 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
```

Notes:

The `last` command can be used to read `/var/log/wtmp` (`last` with no parameters) and `/var/run/utmp` (`last -f /var/run/utmp`)

Reloading the auditd config to set active settings may require a system reboot.

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.

4.1.11 Ensure discretionary access control permission modification events are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The `chmod` , `fchmod` and `fchmodat` system calls affect the permissions associated with a file. The `chown` , `fchown` , `fchownat` and `lchown` system calls affect owner and group attributes on a file. The `setxattr` , `lsetxattr` , `fsetxattr` (set extended file attributes) and `removexattr` , `lremovexattr` , `fremovexattr` (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 500) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier "perm_mod."

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

On a 32 bit system run the following commands:

```
# 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>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod

# auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=-1 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=-1 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=-1 -k
perm_mod
```

On a 64 bit system run the following commands:

```
# grep auditctl -l | 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>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod

# auditctl -l | grep auditctl -l | grep perm_mod
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=-1 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=-1 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=-1 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=-1 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=-1 -k
perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=-1 -k
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/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295
-k perm_mod
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:
Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72097
Rule ID: SV-86721r4_rule
STIG ID: RHEL-07-030370
Severity: CAT II


Vul ID: V-72099
Rule ID: SV-86723r4_rule
STIG ID: RHEL-07-030380
Severity: CAT II


Vul ID: V-72101
Rule ID: SV-86725r4_rule
STIG ID: RHEL-07-030390
Severity: CAT II


Vul ID: V-72103
Rule ID: SV-86727r4_rule
STIG ID: RHEL-07-030400
Severity: CAT II


Vul ID: V-72105
```

```
Rule ID: SV-86729r4_rule

STIG ID: RHEL-07-030410

Severity: CAT II


Vul ID: V-72107

Rule ID: SV-86731r4_rule

STIG ID: RHEL-07-030420

Severity: CAT II


Vul ID: V-72109

Rule ID: SV-86733r4_rule

STIG ID: RHEL-07-030430

Severity: CAT II


Vul ID: V-72111

Rule ID: SV-86735r4_rule

STIG ID: RHEL-07-030440

Severity: CAT II


Vul ID: V-72113

Rule ID: SV-86737r4_rule

STIG ID: RHEL-07-030450

Severity: CAT II


Vul ID: V-72115

Rule ID: SV-86739r4_rule

STIG ID: RHEL-07-030460

Severity: CAT II
```

```
Vul ID: V-72117

Rule ID: SV-86741r4_rule

STIG ID: RHEL-07-030470

Severity: CAT II


Vul ID: V-72119

Rule ID: SV-86743r4_rule

STIG ID: RHEL-07-030480

Severity: CAT II


Vul ID: V-72121

Rule ID: SV-86745r4_rule

STIG ID: RHEL-07-030490

Severity: CAT II
```

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.

4.1.12 Ensure unsuccessful unauthorized file access attempts are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (`creat`), opening (`open` , `openat`) and truncation (`truncate` , `ftruncate`) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 500), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access."

Rationale:

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Audit:

On a 32 bit system run the following commands:

```
# 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>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=-1 -k access
```

On a 64 bit system run the following commands:

```
# 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>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=-1 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=-1 -k 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/audit.rules`
and 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>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/audit.rules`
and 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>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72123

Rule ID: SV-86747r4_rule

STIG ID: RHEL-07-030500

Severity: CAT II



Vul ID: V-72125

Rule ID: SV-86749r4_rule
```

```
STIG ID: RHEL-07-030510

Severity: CAT II


Vul ID: V-72127

Rule ID: SV-86751r4_rule

STIG ID: RHEL-07-030520

Severity: CAT II


Vul ID: V-72129

Rule ID: SV-86753r4_rule

STIG ID: RHEL-07-030530

Severity: CAT II


Vul ID: V-72131

Rule ID: SV-86755r4_rule

STIG ID: RHEL-07-030540

Severity: CAT II


Vul ID: V-72133

Rule ID: SV-86757r4_rule

STIG ID: RHEL-07-030550

Severity: CAT II
```

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).

4.1.13 Ensure use of privileged commands is collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing `<partition>` with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk
'{print "-a always,exit -F path=" $1 " -F perm=x -F auid>='"$(awk
'/^\s*UID_MIN/{print $2}' /etc/login.defs)"' -F auid!=4294967295 -k
privileged" }'
```

Verify all resulting lines are in 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 "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.

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72161

Rule ID: SV-86785r4_rule

STIG ID: RHEL-07-030690

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

4.1.14 Ensure successful file system mounts are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user

Rationale:

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open` , `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Audit:

On a 32 bit system run the following command:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

Then run this command:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=-1 -k mounts
```

On a 64 bit system run the following command:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

Then run this command:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=-1 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=-1 -k 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/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b32 -S mount -F auid>=500 -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/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

Notes:

This tracks successful and unsuccessful mount commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).

Reloading the auditd config to set active settings may require a system reboot.

CIS Controls:

Version 7

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

4.1.15 Ensure file deletion events by users are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the `unlink` (remove a file), `unlinkat` (remove a file attribute), `rename` (rename a file) and `renameat` (rename a file attribute) system calls and tags them with the identifier "delete".

Rationale:

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Audit:

On a 32 bit system run the following command:

```
# 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>=500 -F auid!=4294967295 -k delete
```

Then run this command:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
```

On a 64 bit system run the following command:

```
# 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>=500 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
```

Then run this command:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=-1 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=-1 -k 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/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/audit.rules`
and add the following lines:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
```

Notes:

At a minimum, configure the audit system to collect file deletion events for all users and root.

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72199

Rule ID: SV-86823r4_rule

STIG ID: RHEL-07-030880

Severity: CAT II


Vul ID: V-72201

Rule ID: SV-86825r4_rule

STIG ID: RHEL-07-030890

Severity: CAT II
```

CIS Controls:

Version 7

13 Data Protection
Data Protection

4.1.16 Ensure changes to system administration scope (sudoers) is collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers` will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier "scope."

Rationale:

Changes in the `/etc/sudoers` file can indicate that an unauthorized change has been made to scope of system administrator activity.

Audit:

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/audit.rules`
and add the following lines:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72163

Rule ID: SV-86787r5_rule

STIG ID: RHEL-07-030700

Severity: CAT II
```

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.

4.1.17 Ensure system administrator actions (sudolog) are collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log` . Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

Rationale:

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

Audit:

Run the following commands:

```
# grep actions /etc/audit/rules.d/*.rules

# auditctl -l | grep actions
```

Verify output of both matches:

```
-w /var/log/sudo.log -p wa -k actions
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`
Example: `vi /etc/audit/rules.d/audit.rules`
and add the following lines:

```
-w /var/log/sudo.log -p wa -k actions
```

Notes:

The system must be configured with `su`disabled (See Item 5.6 Ensure access to the su command is restricted) to force all command execution through `sudo`. This will not be effective on the console, as administrators can log in as root.

Reloading the auditd config to set active settings may require a system reboot.

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.

4.1.18 Ensure the audit configuration is immutable (Scored)

Profile Applicability:

- Level 2

Description:

Set system audit so that audit rules cannot be modified with `auditctl` . Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

Rationale:

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Audit:

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

Notes:

This setting will ensure reloading the auditd config to set active settings requires a system reboot.

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.

4.1.19 Ensure kernel module loading and unloading is collected (Scored)

Profile Applicability:

- Level 2

Description:

Monitor the loading and unloading of kernel modules. The programs `insmod` (install a kernel module), `rmmod` (remove a kernel module), and `modprobe` (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The `init_module` (load a module) and `delete_module` (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules".

Rationale:

Monitoring the use of `insmod` , `rmmod` and `modprobe` could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the `init_module` and `delete_module` system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Audit:

On a 32 bit system run the following commands:

```
# grep modules /etc/audit/rules.d/*.rules

# auditctl -l | grep modules
```

Verify output of both 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
```

On a 64 bit system run the following commands:

```
# grep modules /etc/audit/rules.d/*.rules

# auditctl -l | grep modules
```

Verify output of both 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
```

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/audit.rules`
and 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/audit.rules`
and 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
```

Notes:

Reloading the auditd config to set active settings may require a system reboot.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72187

Rule ID: SV-86811r4_rule

STIG ID: RHEL-07-030820

Severity: CAT II


Vul ID: V-72189

Rule ID: SV-86813r4_rule

STIG ID: RHEL-07-030830

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

4.1.20 Ensure the auditing processing failures are handled. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff in the event of an audit processing failure.

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Confirm the audit configuration regarding how auditing processing failures are handled. Check to see what level `auditctl` is set to with following command:

```
# auditctl -s | grep -i "fail"

failure 2
```

If the value of `failure` is set to `2`, the system is configured to panic (shut down) in the event of an auditing failure.
If the value of `failure` is set to `1`, the system is configured to only send information to the kernel log regarding the failure.
If the `failure` setting is not set, this is a CAT I finding, refer to the remediation procedure below.
If the `failure` setting is set to any value other than `1` or `2`, this is a CAT II finding, refer to the remediation procedure below.
If the `failure` setting is set to `1` but the availability concern is not documented or there is no monitoring of the kernel log, this is a CAT III finding, refer to the remediation procedure below.

Remediation:

Configure the operating system to shut down or notify staff in the event of an audit processing failure.
To add or correct the option to shut down the operating system use the following command:

```
# auditctl -f 2
```

Edit the `/etc/audit/rules.d/audit.rules` file and add the following line:
Example: `vim /etc/audit/rules.d/audit.rules`
Add this line:

```
-f 2
```

If availability has been determined to be more important, and this decision is documented with the Authorizing Official, configure the operating system to notify the appropriate staff in the event of an audit processing failure with the following command:

```
# auditctl -f 1
```

Edit the `/etc/audit/rules.d/audit.rules` file and add the following line:
Example: `vim /etc/audit/rules.d/audit.rules`
Add this line:

```
-f 1
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

Impact:

Kernel log monitoring must also be configured to properly alert designated staff.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72081

Rule ID: SV-86705r4_rule

STIG ID: RHEL-07-030010

Severity: CAT II
```

4.1.21 Ensure auditing of all privileged functions (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must audit all executions of privileged functions.

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Audit:

Verify the operating system audits the execution of privileged functions using the following command:
Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures.
Only the lines appropriate for the system architecture must be present.

```
# grep -iw execve /etc/audit/audit.rules

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

If the audit rule for `SUID` files is not defined, refer to the remediation procedure below.
If the audit rule for `SGID` files is not defined, refer to the remediation procedure below.

Remediation:

Configure the operating system to audit the execution of privileged functions.
Add or update the following rule in `/etc/audit/rules.d/audit.rules`:
Example: `vim /etc/audit/rules.d/audit.rules`
Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72095

Rule ID: SV-86719r6_rule

STIG ID: RHEL-07-030360

Severity: CAT II
```

4.1.22 Ensure auditd service is active (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.

Rationale:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds; or identifying an improperly configured operating system.

Audit:

Verify the operating system produces audit records containing information to establish when (date and time) the events occurred.
Check to see if `auditing` is active by issuing the following command:

```
# systemctl is-active auditd.service

active
```

If the `auditd` status is not active, refer to the remediation procedure below.

Remediation:

Configure the operating system to produce audit records containing information to establish when (date and time) the events occurred.
Enable the `auditd` service with the following command:

```
# service auditd start
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72079

Rule ID: SV-86703r3_rule

STIG ID: RHEL-07-030000

Severity: CAT I
```

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 Ensure the correct logging software is installed

The rsyslog and syslog-ng software are recommended replacements to the original syslogd daemon which provide improvements over syslogd , such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

4.2.1.1 Ensure rsyslog or syslog-ng is installed (Scored)

Profile Applicability:

- Level 1

Description:

The `rsyslog` and `syslog-ng` software are recommended replacements to the original `syslogd` daemon which provide improvements over `syslogd` , such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Rationale:

The security enhancements of `rsyslog` and `syslog-ng` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit:

Run the following commands and verify at least one indicates the package is installed:

```
# rpm -q rsyslog
# rpm -q syslog-ng
```

Remediation:

Install `rsyslog` or `syslog-ng` using one of the following commands:

```
# yum install rsyslog
# yum install syslog-ng
```

Notes:

The `syslog-ng` package requires the EPEL7 and Optional repositories be enabled. See https://czanik.blogs.balabit.com/2015/09/installing-syslog-ng-ose-3-7-1-on-rhel6-and-centos6/ 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.

4.2.2 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.

4.2.2.1 Ensure rsyslog Service is enabled (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

If the `rsyslog` service is not activated the system 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
enabled
```

Remediation:

Run one of the following commands to enable `rsyslog` :

```
# systemctl enable rsyslog
```

Notes:

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

Some distributions may configure syslog daemon selection via a setting in a configuration file such as `/etc/sysconfig/syslog` and a centralized init script.

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.

4.2.2.2 Ensure logging is configured (Not Scored)

Profile Applicability:

- Level 1

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/secure
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 `rsyslogd` configuration:

```
# pkill -HUP rsyslogd
```

References:

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

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72051

Rule ID: SV-86675r2_rule

STIG ID: RHEL-07-021100

Severity: CAT II
```

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.

4.2.2.3 Ensure rsyslog default file permissions configured (Scored)

Profile Applicability:

- Level 1

Description:

rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that `$FileCreateMode` is `0640` or more restrictive:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

References:

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

Notes:

You should also ensure this is not overridden with less restrictive settings in any `/etc/rsyslog.d/*` conf file.

CIS Controls:

Version 7

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

4.2.2.4 Ensure rsyslog is configured to send logs to a remote log host (Scored)

Profile Applicability:

- Level 1

Description:

The `rsyslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

```
# grep "^*.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf

*.* @@loghost.example.com
```

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host).

```
*.* @@loghost.example.com
```

Run the following command to reload the `rsyslogd` configuration:

```
# pkill -HUP rsyslogd
```

References:

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

Notes:

The double "at" sign (`@@`) directs `rsyslog`to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72209

Rule ID: SV-86833r2_rule

STIG ID: RHEL-07-031000

Severity: CAT II
```

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.

4.2.2.5 Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)

Profile Applicability:

- Level 1

Description:

By default, `rsyslog` does not listen for log messages coming in from remote systems. The `ModLoad` tells `rsyslog` to load the `imtcp.so` module so it can listen over a network via TCP. The `InputTCPServerRun` option instructs `rsyslogd` to listen on the specified TCP port.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `rsyslog` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `rsyslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Run the following commands and verify the resulting lines are uncommented on designated log hosts and commented or removed on all others:

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$ModLoad imtcp

# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$InputTCPServerRun 514
```

Remediation:

For hosts that are designated as log hosts, edit the `/etc/rsyslog.conf` file and un-comment or add the following lines:

```
$ModLoad imtcp
$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:

```
# pkill -HUP rsyslogd
```

References:

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

Notes:

The `$MoadLoad imtcp` line can have the `.so` extension added to the end of the module, or use the full path to the module.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72211

Rule ID: SV-86835r2_rule

STIG ID: RHEL-07-031010

Severity: CAT II
```

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.

4.2.2.6 Ensure rsyslog imudp and imrelp aren't loaded. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.

Rationale:

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the system's logs, or could fill the system's storage leading to a Denial of Service.

If the system is intended to be a log aggregation server its use must be documented with the Authorizing Official.

Audit:

Verify that the system is not accepting `rsyslog` messages from other systems unless it is documented as a log aggregation server.
Check the configuration of `rsyslog` with the following commands:

```
# grep imudp /etc/rsyslog.conf
$ModLoad imudp
# grep imrelp /etc/rsyslog.conf
$ModLoad imrelp
```

If any of the above modules are being loaded in the `/etc/rsyslog.conf` file, ask to see the documentation for the system being used for log aggregation.
If the documentation does not exist, or does not specify the server as a log aggregation system, refer to the remediation procedure below.

Remediation:

Modify the `/etc/rsyslog.conf` file to remove the `ModLoad imudp`, and `ModLoad imrelp` configuration lines, or document the system as being used for log aggregation.
Example: `vim /etc/rsyslog.conf`
Remove or comment out these following configuration lines:

```
#ModLoad imudp
#ModLoad imrelp
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72211

Rule ID: SV-86835r2_rule

STIG ID: RHEL-07-031010

Severity: CAT II
```

4.2.3 Configure syslog-ng

The `syslog-ng` software is recommended as a replacement for the `syslogd` daemon and provides improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server. **NOTE**: This section only applies if `syslog-ng` is installed on the system.

4.2.3.1 Ensure syslog-ng service is enabled (Scored)

Profile Applicability:

- Level 1

Description:

Once the `syslog-ng` package is installed it needs to be activated.

Rationale:

If the `syslog-ng` service is not activated the system may default to the `syslogd` service or lack logging instead.

Audit:

Run the following command and verify result is "enabled":

```
# systemctl is-enabled syslog-ng
enabled
```

Remediation:

Run the following command to enable `syslog-ng` :

```
# systemctl enable syslog-ng
```

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.

4.2.3.2 Ensure logging is configured (Not Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/syslog-ng/syslog-ng.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via `syslog-ng` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the `/etc/syslog-ng/syslog-ng.conf` file to ensure appropriate logging is set. In addition, run the following command and ensure that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the log lines in the `/etc/syslog-ng/syslog-ng.conf` file as appropriate for your environment:

```
log { source(src); source(chroots); filter(f_console); destination(console);
};
log { source(src); source(chroots); filter(f_console); destination(xconsole);
};
log { source(src); source(chroots); filter(f_newscrit);
destination(newscrit); };
log { source(src); source(chroots); filter(f_newserr); destination(newserr);
};
log { source(src); source(chroots); filter(f_newsnotice);
destination(newsnotice); };
log { source(src); source(chroots); filter(f_mailinfo);
destination(mailinfo); };
log { source(src); source(chroots); filter(f_mailwarn);
destination(mailwarn); };
log { source(src); source(chroots); filter(f_mailerr);  destination(mailerr);
};
log { source(src); source(chroots); filter(f_mail); destination(mail); };
log { source(src); source(chroots); filter(f_acpid); destination(acpid);
flags(final); };
log { source(src); source(chroots); filter(f_acpid_full);
destination(devnull); flags(final); };
log { source(src); source(chroots); filter(f_acpid_old); destination(acpid);
flags(final); };
log { source(src); source(chroots); filter(f_netmgm); destination(netmgm);
flags(final); };
log { source(src); source(chroots); filter(f_local);
destination(localmessages); };
log { source(src); source(chroots); filter(f_messages);
destination(messages); };
log { source(src); source(chroots); filter(f_iptables);
destination(firewall); };
log { source(src); source(chroots); filter(f_warn); destination(warn); };
```

Run the following command to reload the `syslog-ng` configuration:

```
# pkill -HUP syslog-ng
```

References:

1. See the syslog-ng 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.

4.2.3.3 Ensure syslog-ng default file permissions configured (Scored)

Profile Applicability:

- Level 1

Description:

syslog-ng will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `syslog-ng` data is archived and protected.

Audit:

Run the following command and verify the `perm` option is `0640` or more restrictive:

```
# grep ^options /etc/syslog-ng/syslog-ng.conf
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600);
threaded(yes); };
```

Remediation:

Edit the `/etc/syslog-ng/syslog-ng.conf` and set `perm` option to `0640` or more restrictive:

```
options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600);
threaded(yes); };
```

References:

1. See the syslog-ng man pages for more information.

CIS Controls:

Version 7

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

4.2.3.4 Ensure syslog-ng is configured to send logs to a remote log host (Not Scored)

Profile Applicability:

- Level 1

Description:

The `syslog-ng` utility supports the ability to send logs it gathers to a remote log host or to receive messages from remote hosts, reducing administrative overhead.

Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Audit:

Review the `/etc/syslog-ng/syslog-ng.conf` file and verify that logs are sent to a central host (where `logfile.example.com` is the name of your central log host):

```
destination logserver { tcp("logfile.example.com" port(514)); };
log { source(src); destination(logserver); };
```

Remediation:

Edit the `/etc/syslog-ng/syslog-ng.conf` file and add the following lines (where `logfile.example.com` is the name of your central log host).

```
destination logserver { tcp("logfile.example.com" port(514)); };
log { source(src); destination(logserver); };
```

Run the following command to reload the `syslog-ng` configuration:

```
# pkill -HUP syslog-ng
```

References:

1. See the syslog-ng.conf(5) man page for more information.

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.

4.2.3.5 Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)

Profile Applicability:

- Level 1

Description:

By default, `syslog-ng` does not listen for log messages coming in from remote systems.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `syslog-ng` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `syslog-ng` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Review the /etc/syslog-ng/syslog-ng.conf file and verify the following lines are configured appropriately on designated log hosts:

```
source net{ tcp(); };
destination remote { file("/var/log/remote/${FULLHOST}-log"); };
log { source(net); destination(remote); };
```

Remediation:

On designated log hosts edit the `/etc/syslog-ng/syslog-ng.conf` file and configure the following lines are appropriately:

```
source net{ tcp(); };
destination remote { file("/var/log/remote/${FULLHOST}-log"); };
log { source(net); destination(remote); };
```

On non designated log hosts edit the `/etc/syslog-ng/syslog-ng.conf` file and remove or edit any sources that accept network sourced log messages.
Run the following command to reload the `syslog-ng` configuration:

```
# pkill -HUP syslog-ng
```

References:

1. See the syslog-ng(8) man page for more information.

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.

4.2.4 Ensure permissions on all logfiles are configured (Scored)

Profile Applicability:

- Level 1

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log -type f -ls
```

Remediation:

Run the following 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 "{}" +
```

Notes:

You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

4.3 Ensure logrotate is configured (Not Scored)

Profile Applicability:

- Level 1

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Review `/etc/logrotate.conf` and `/etc/logrotate.d/*` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/*` to ensure logs are rotated according to site policy.

Notes:

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.

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 audit system is set to single when the disk is full. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

Rationale:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Audit:

Verify the action the operating system takes if the disk the audit records are written to becomes full.
To determine the action that takes place if the disk is full on the remote server, is set to `syslog`, `single`, or `halt` using the following command:

```
# grep -i disk_full_action /etc/audisp/audisp-remote.conf

disk_full_action = single
```

If the value of the `disk_full_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure the action the operating system takes if the disk the audit records are written to becomes full.
Uncomment or edit the `disk_full_action` option in `/etc/audisp/audisp-remote.conf`.
Example: `vim /etc/audisp/audisp-remote.conf`
Set it to `syslog`, `single`, or `halt`, such as the following example:

```
disk_full_action = single
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72087

Rule ID: SV-86711r3_rule

STIG ID: RHEL-07-030320

Severity: CAT II
```

4.5 Ensure system notification is sent out when voume is 75% full (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must initiate an action to notify the Authorizing Official, at a minimum, when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the operating system initiates an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.
Check the system configuration to determine the partition the audit records are being written to with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Check the size of the partition that audit records are written to (with the example being `/var/log/audit/`):

```
# df -h /var/log/audit/

0.9G /var/log/audit
```

If the audit records are not being written to a partition specifically created for audit records (in this example `/var/log/audit` is a separate partition), determine the amount of space other files in the partition are currently occupying with the following command:

```
# du -sh <partition>

1.8G /var
```

Determine what the threshold is for the system to take action when 75 percent of the repository maximum audit record storage capacity is reached:

```
# grep -iw space_left /etc/audit/auditd.conf

space_left = 225
```

If the value of the `space_left` keyword is not set to 75 percent of the total partition size, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate an action to notify the Authorizing Official (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.
Check the system configuration to determine the partition the audit records are being written to:

```
# grep -iw log_file /etc/audit/auditd.conf
```

Determine the size of the partition that audit records are written to (with the example being `/var/log/audit/`):

```
# df -h /var/log/audit/
```

Set the value of the `space_left` keyword in `/etc/audit/auditd.conf` to 75 percent of the partition size.
Example: `vim /etc/audit/auditd.conf`
Add the line with space_left set to `75%` or the partition size.
Example:

```
space_left = 225
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72089

Rule ID: SV-86713r3_rule

STIG ID: RHEL-07-030330

Severity: CAT II
```

4.6 Ensure audit system action is defined for sending errors (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the audit system takes appropriate action when there is an error sending audit records to a remote system.

Rationale:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Audit:

Verify the action the operating system takes if there is an error sending audit records to a remote system.
Check the action that takes place if there is an error sending audit records to a remote system is set to `syslog`, `single`, or `halt` with the following command:

```
# grep -i network_failure_action /etc/audisp/audisp-remote.conf

network_failure_action = syslog
```

If the value of the `network_failure_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation below.

Remediation:

Configure the action the operating system takes if there is an error sending audit records to a remote system.
Uncomment the `network_failure_action` option in `/etc/audisp/audisp-remote.conf` and set it to `syslog`, `single`, or `halt`.
Example: `vim /etc/audisp/audisp-remote.conf`
Add the line as shown in below

```
network_failure_action = syslog
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-73163

Rule ID: SV-87815r3_rule

STIG ID: RHEL-07-030321

Severity: CAT II
```

4.7 Enable use of the au-remote plugin (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured to use the au-remote plugin.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the "au-remote" plugin, the audisp-remote daemon will not off-load the logs from the system being audited.

Audit:

Verify the `au-remote` plugin is active on the system:

```
# grep "active" /etc/audisp/plugins.d/au-remote.conf

active = yes
```

If the `active` setting is not set to `yes`, or the line is commented out, refer to the remediation below.

Remediation:

Edit the `/etc/audisp/plugins.d/au-remote.conf` file and change the value of `active` to `yes`.
Example: `vim /etc/audisp/plugins.d/au-remote.conf`
Add this line:

```
active = yes
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81015

Rule ID: SV-95727r1_rule

STIG ID: RHEL-07-030200

Severity: CAT II
```

4.8 Enure off-load of audit logs. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Without the configuration of the "au-remote" plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Audit:

Verify the `au-remote` plugin is configured to always off-load audit logs using the audisp-remote daemon:

```
# cat /etc/audisp/plugins.d/au-remote.conf | grep -v "^#"

active = yes
direction = out
path = /sbin/audisp-remote
type = always
format = string
```

If the `direction` setting is not set to `out`, or the line is commented out, refer to the remediation procedure below.
If the `path` setting is not set to `/sbin/audisp-remote`, or the line is commented out, refer to the remediation procedure below.
If the `type` setting is not set to `always`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audisp/plugins.d/au-remote.conf` file and add, uncomment or update the following values:
Example: `vim /etc/audisp/plugins.d/au-remote.conf`
Add uncomment or update the following lines:

```
direction = out
path = /sbin/audisp-remote
type = always
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81017

Rule ID: SV-95729r1_rule

STIG ID: RHEL-07-030201

Severity: CAT II
```

4.9 Ensure action is taken when audisp-remote buffer is full (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must take appropriate action when the audisp-remote buffer is full.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Audit:

Verify the audisp daemon is configured to take an appropriate action when the internal queue (audisp-remote buffer) is full:

```
# grep "overflow_action" /etc/audisp/audispd.conf

overflow_action = syslog
```

If the `overflow_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audisp/audispd.conf` file and add or update the `overflow_action` option:
Example: `vim /etc/audisp/audispd.conf`
Add, update or uncomment the following line:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81019

Rule ID: SV-95731r1_rule

STIG ID: RHEL-07-030210

Severity: CAT II
```

4.10 Ensure off-loaded audit logs are labeled. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must label all off-loaded audit logs before sending them to the central log server.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Audit:

Verify the audisp daemon is configured to label all off-loaded audit logs by checking that the name_format `hostname`, `fqd`, or `numeric`:

```
# grep "name_format" /etc/audisp/audispd.conf

name_format = hostname
```

If the `name_format` option is not `hostname`, `fqd`, or `numeric`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audisp/audispd.conf` file and add or update the `name_format` option:
Example: `vim /etc/audisp/audispd.conf`
Add the name format to include `hostname`, `fqd`, or `numeric`.
Example:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81021

Rule ID: SV-95733r1_rule

STIG ID: RHEL-07-030211

Severity: CAT II
```

5 Access, Authentication and Authorization

5.1 Configure cron

5.1.1 Ensure cron daemon is enabled (Scored)

Profile Applicability:

- Level 1

Description:

The `cron` daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

Audit:

Based on your system configuration, run the appropriate one of the following commands to verify `cron` is enabled:

```
# systemctl is-enabled crond

enabled
```

Verify result is "enabled".

Remediation:

Run the following command to enable `cron` :

```
# systemctl --now enable crond
```

Notes:

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

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.1.2 Ensure permissions on /etc/crontab are configured (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

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

5.1 Establish Secure Configurations

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

5.1.3 Ensure permissions on /etc/cron.hourly are configured (Scored)

Profile Applicability:

- Level 1

Description:

This directory contains system `cron` jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

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 `/etc/cron.hourly` :

```
# chown root:root /etc/cron.hourly

# chmod og-rwx /etc/cron.hourly
```

CIS Controls:

Version 7

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

5.1.4 Ensure permissions on /etc/cron.daily are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

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 `/etc/cron.daily` :

```
# chown root:root /etc/cron.daily

# chmod og-rwx /etc/cron.daily
```

CIS Controls:

Version 7

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

5.1.5 Ensure permissions on /etc/cron.weekly are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

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 `/etc/cron.weekly` :

```
# chown root:root /etc/cron.weekly

# chmod og-rwx /etc/cron.weekly
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.1.6 Ensure permissions on /etc/cron.monthly are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

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 `/etc/cron.monthly` :

```
# chown root:root /etc/cron.monthly

# chmod og-rwx /etc/cron.monthly
```

CIS Controls:

Version 7

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

5.1.7 Ensure permissions on /etc/cron.d are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab` , but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Audit:

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 `/etc/cron.d`:

```
# chown root:root /etc/cron.d

# chmod og-rwx /etc/cron.d
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.1.8 Ensure at/cron is restricted to authorized users (Scored)

Profile Applicability:

- Level 1

Description:

Configure `/etc/cron.allow` and `/etc/at.allow` to allow specific users to use these services. If `/etc/cron.allow` or `/etc/at.allow` do not exist, then `/etc/at.deny` and `/etc/cron.deny` are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in `/etc/cron.allow` and `/etc/at.allow` are allowed to use at and cron. Note that even though a given user is not listed in `cron.allow` , cron jobs can still be run as that user. The `cron.allow` file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale:

On many systems, only the system administrator is authorized to schedule `cron` jobs. Using the `cron.allow` file to control who can run `cron` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Audit:

Run the following commands and ensure `/etc/cron.deny` and `/etc/at.deny` do not exist:

```
# stat /etc/cron.deny
stat: cannot stat `/etc/cron.deny': No such file or directory

# stat /etc/at.deny
stat: cannot stat` /etc/at.deny': No such file or directory
```

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

```
# stat /etc/cron.allow
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)

# stat /etc/at.allow
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to remove `/etc/cron.deny` and `/etc/at.deny` and create and set permissions and ownership for `/etc/cron.allow` and `/etc/at.allow` :

```
# rm /etc/cron.deny
# rm /etc/at.deny

# touch /etc/cron.allow
# touch /etc/at.allow

# chmod og-rwx /etc/cron.allow
# chmod og-rwx /etc/at.allow

# chown root:root /etc/cron.allow
# chown root:root /etc/at.allow
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72055

Rule ID: SV-86679r2_rule

STIG ID: RHEL-07-021120

Severity: CAT II



Vul ID: V-72053

Rule ID: SV-86677r3_rule

STIG ID: RHEL-07-021110

Severity: CAT II
```

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

5.2 SSH Server Configuration

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note: The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is not required the SSH daemon can be removed and this section skipped.

Note: Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:

```
# systemctl reload sshd
```

5.2.1 Ensure SSH is installed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all networked systems have SSH installed.

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Audit:

Check to see if `sshd` is installed with the following command:

```
# yum list installed \*ssh\*
libssh2.x86_64 1.4.3-8.el7 @anaconda/7.1
openssh.x86_64 6.6.1p1-11.el7 @anaconda/7.1
openssh-server.x86_64 6.6.1p1-11.el7 @anaconda/7.1
```

If the `SSH server` package is not installed, refer to the remediation procedure below.

Remediation:

Install SSH packages onto the host with the following commands:

```
# yum install openssh-server.x86_64
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72233

Rule ID: SV-86857r3_rule

STIG ID: RHEL-07-040300

Severity: CAT II
```

5.2.2 Ensure SSH is running (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Audit:

Verify `SSH` is loaded and active with the following command:

```
# systemctl status sshd

sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)
Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days
ago
Main PID: 1348 (sshd)
CGroup: /system.slice/sshd.service
1053 /usr/sbin/sshd -D
```

If `sshd` does not show a status of `active` and `running`, refer to the remediation procedure below.

Remediation:

Configure the SSH service to start and automatically start after reboot with the following command:

```
# systemctl --now enable sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72235

Rule ID: SV-86859r3_rule

STIG ID: RHEL-07-040310

Severity: CAT II
```

5.2.3 Ensure permissions on /etc/ssh/sshd_config are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to root.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-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
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71903

Rule ID: SV-86527r3_rule

STIG ID: RHEL-07-010120

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.2.4 Ensure permissions on SSH private host key files are configured (Scored)

Profile Applicability:

- Level 1

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 and Gid is 0/root. Ensure group and other do not have permissions

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;

  File: ‘/etc/ssh/ssh_host_rsa_key’
  Size: 1679            Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8628138     Links: 1
Access: (0600/-rw-------)  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 18:24:56.873750616 +0000
 Birth: -
  File: ‘/etc/ssh/ssh_host_ecdsa_key’
  Size: 227             Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631760     Links: 1
Access: (0600/-rw-------)  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 18:24:56.905750616 +0000
 Birth: -
  File: ‘/etc/ssh/ssh_host_ed25519_key’
  Size: 387             Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631762     Links: 1
Access: (0600/-rw-------)  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 18:24:56.957750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set ownership and permissions on the private SSH host key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {} \;

# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod 0600 {} \;
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72257

Rule ID: SV-86881r3_rule

STIG ID: RHEL-07-040420

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.2.5 Ensure permissions on SSH public host key files are configured (Scored)

Profile Applicability:

- Level 1

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 {} \;

  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 0644 {}
\;

#find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root
{} \;
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72255

Rule ID: SV-86879r2_rule

STIG ID: RHEL-07-040410

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.2.6 Ensure SSH Protocol is set to 2 (Scored)

Profile Applicability:

- Level 1

Description:

Older versions of SSH support two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

Run the following command and verify that output matches:

```
# grep ^Protocol /etc/ssh/sshd_config

Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:
Example: `vim /etc/ssh/sshd_config`

```
Protocol 2
```

Notes:

This command not longer exists in newer versions of SSH. This check is still being included for systems that may be running an older version of SSH. As of openSSH version 7.4 this parameter will not cause an issue when included.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72251

Rule ID: SV-86875r4_rule

STIG ID: RHEL-07-040390

Severity: CAT I
```

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.

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.2.7 Ensure SSH LogLevel is appropriate (Scored)

Profile Applicability:

- Level 1

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:

```
# sshd -T | grep loglevel

LogLevel VERBOSE

OR

loglevel INFO
```

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.

5.2.8 Ensure SSH X11 forwarding is disabled (Scored)

Profile Applicability:

- Level 2

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep x11forwarding

X11Forwarding no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running

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

5.2.9 Ensure SSH MaxAuthTries is set to 4 or less (Scored)

Profile Applicability:

- Level 1

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# sshd -T | grep maxauthtries

MaxAuthTries 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

MaxAuthTries 6

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.

5.2.10 Ensure SSH IgnoreRhosts is enabled (Scored)

Profile Applicability:

- Level 1

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with ssh.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep ignorerhosts

IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

IgnoreRhosts yes

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72243

Rule ID: SV-86867r3_rule

STIG ID: RHEL-07-040350

Severity: CAT II
```

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.

5.2.11 Ensure SSH HostbasedAuthentication is disabled (Scored)

Profile Applicability:

- Level 1

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep hostbasedauthentication

HostbasedAuthentication no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

HostbasedAuthentication no

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71959

Rule ID: SV-86583r3_rule

STIG ID: RHEL-07-010470

Severity: CAT II
```

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.

5.2.12 Ensure SSH root login is disabled (Scored)

Profile Applicability:

- Level 1

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` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep permitrootlogin

PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

PermitRootLogin without-password

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72247

Rule ID: SV-86871r3_rule

STIG ID: RHEL-07-040370

Severity: CAT II
```

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.

5.2.13 Ensure SSH PermitEmptyPasswords is disabled (Scored)

Profile Applicability:

- Level 1

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 | grep permitemptypasswords

PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

PermitEmptyPasswords no

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71939

Rule ID: SV-86563r3_rule

STIG ID: RHEL-07-010300

Severity: CAT I
```

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.

5.2.14 Ensure SSH PermitUserEnvironment is disabled (Scored)

Profile Applicability:

- Level 1

Description:

The `PermitUserEnvironment` option allows users to present environment options to the `ssh` daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has `ssh` executing trojan'd programs)

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep permituserenvironment

PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71957

Rule ID: SV-86581r3_rule

STIG ID: RHEL-07-010460

Severity: CAT II
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.2.15 Ensure only strong Ciphers are used (Scored)

Profile Applicability:

- Level 1

Description:

This variable limits the ciphers that SSH can use during communication.

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

The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

Audit:

Run the following command and verify that output does not contain any of the listed weak ciphers

```
# sshd -T | grep ciphers
```

Weak Ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

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,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc

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)

Notes:

Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

The only "strong" ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr

CVE-2013-4548 referenced above applies to OpenSSH versions 6.2 and 6.3. If running these versions of Open SSH, Please upgrade to version 6.4 or later to fix the vulnerability, or disable AES-GCM in the server configuration.

The Following are the supported ciphers in openSSH:

```
3des-cbc

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

aes128-gcm@openssh.com

aes256-gcm@openssh.com

arcfour

arcfour128

arcfour256

blowfish-cbc

cast128-cbc

rijndael-cbc@lysator.liu.se

chacha20-poly1305@openssh.com
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.2.16 Ensure only strong MAC algorithms are used (Scored)

Profile Applicability:

- Level 1

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Audit:

Run the following command and verify that output does not contain any of the listed weak MAC algorithms:

```
# sshd -T | grep -i "MACs"
```

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
```

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,hmac-sha1-etm@openssh.com

References:

1. More information on SSH downgrade attacks can be found here: http://www.mitls.org/pages/attacks/SLOTH
2. SSHD_CONFIG(5)

Notes:

Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.

The only "strong" MACs currently FIPS 140-2 approved are hmac-sha2-256 and hmac-sha2-512

The Supported MACs are:

```
hmac-md5

hmac-md5-96

hmac-ripemd160

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-ripemd160-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
```

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.

5.2.17 Ensure only strong Key Exchange algorithms are used (Scored)

Profile Applicability:

- Level 1

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 that output does not contain any of the listed weak Key Exchange algorithms

```
# sshd -T | grep kexalgorithms
```

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

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,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Default Value:

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

Notes:

Kex algorithms have a higher preference the earlier they appear in the list

Some organizations may have stricter requirements for approved Key exchange algorithms. Ensure that Key exchange algorithms used are in compliance with site policy.

The only Key Exchange Algorithms currently FIPS 140-2 approved are: 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

The Key Exchange algorithms supported by OpenSSH 7 are:

```
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
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

5.2.18 Ensure SSH Idle Timeout Interval is configured (Scored)

Profile Applicability:

- Level 1

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions. When the `ClientAliveInterval` variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, `sshd` will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response from the client, the `ssh` session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client `ssh` session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's `ssh` session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Audit:

Run the following commands and verify `ClientAliveInterval` is between 1 and 300 and `ClientAliveCountMax` is 3 or less:

```
# sshd -T | grep clientaliveinterval

ClientAliveInterval 300

# sshd -T | grep clientalivecountmax

ClientAliveCountMax 0
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters according to site policy:

```
ClientAliveInterval 300

ClientAliveCountMax 0
```

Default Value:

ClientAliveInterval 300

ClientAliveCountMax 0

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72241

Rule ID: SV-86865r4_rule

STIG ID: RHEL-07-040340

Severity: CAT II


Vul ID: V-72237

Rule ID: SV-86861r4_rule

STIG ID: RHEL-07-040320

Severity: CAT II
```

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

5.2.19 Ensure SSH LoginGraceTime is set to one minute or less (Scored)

Profile Applicability:

- Level 1

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:

```
# sshd -T | grep logingracetime

LoginGraceTime 60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

LoginGraceTime 120

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.2.20 Ensure SSH access is limited (Scored)

Profile Applicability:

- Level 1

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

`AllowUsers`

The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of 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 commands and verify that output matches for at least one:

```
# sshd -T | grep allowusers

AllowUsers <userlist>

# sshd -T | grep allowgroups

AllowGroups <grouplist>

# sshd -T | grep denyusers
DenyUsers <userlist>

# sshd -T | grep denygroups

DenyGroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>

AllowGroups <grouplist>

DenyUsers <userlist>

DenyGroups <grouplist>
```

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.

5.2.21 Ensure SSH warning banner is configured (Scored)

Profile Applicability:

- Level 1

Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. 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 | grep banner

Banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /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.

5.2.22 Ensure only FIPS 140-2 ciphers are used for SSH (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general purpose computing system.

Audit:

Verify the operating system uses mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.
Note: If Benchmark recommendation 1.5.7 fails, this is automatically a finding as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.
The location of the `sshd_config` file may vary if a different daemon is in use. The command below utilizes this path `/etc/ssh/sshd_config`.
Inspect the `Ciphers` configuration with the following command:

```
# grep -i ciphers /etc/ssh/sshd_config
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

If any ciphers other than `aes128-ctr`, `aes192-ctr`, or `aes256-ctr` are listed, the `Ciphers` keyword is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Configure SSH to use FIPS 140-2 approved cryptographic algorithms.
Add the following line (or modify the line to have the required value) to the `/etc/ssh/sshd_config` file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Impact:

The only "strong" ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72221

Rule ID: SV-86845r3_rule

STIG ID: RHEL-07-040110

Severity: CAT II
```

5.2.23 Ensure RSA rhosts authentication is not allowed (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using RSA rhosts authentication. To determine how the SSH daemon's `RhostsRSAAuthentication` option is set, run the following command:

```
# grep RhostsRSAAuthentication /etc/ssh/sshd_config

RhostsRSAAuthentication no
```

If the value is returned as `yes`, the returned line is commented out, or no output is returned, refer to the remediation procedure below.

Remediation:

Configure the SSH daemon to not allow authentication using RSA rhosts authentication.
Add the following line in `/etc/ssh/sshd_config`, or uncomment the line and set the value to `no`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
RhostsRSAAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72239

Rule ID: SV-86863r4_rule

STIG ID: RHEL-07-040330

Severity: CAT II
```

5.2.24 Ensure Printlastlog is enabled (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must display the date and time of the last successful account logon upon an SSH logon.

Rationale:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify SSH provides users with feedback on when account accesses last occurred.
Check that `PrintLastLog` keyword in the sshd daemon configuration file is used and set to `yes` with the following command:

```
# grep -i printlastlog /etc/ssh/sshd_config

PrintLastLog yes
```

If the `PrintLastLog` keyword is set to `no`, is missing, or is commented out, refer to the remediation procedure below.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in `/etc/pam.d/sshd` or in the `sshd_config` file used by the system (`/etc/ssh/sshd_config` will be used in the example) (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).
Modify the `PrintLastLog` line in `/etc/ssh/sshd_config` to match the following:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
PrintLastLog yes
```

The SSH service must be restarted for changes to `sshd_config` to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72245

Rule ID: SV-86869r3_rule

STIG ID: RHEL-07-040360

Severity: CAT II
```

5.2.25 Ensure SSH setting for "IgnoreUserKnownHosts" is enabled. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known hosts authentication. To determine how the SSH daemon's `IgnoreUserKnownHosts` option is set, run the following command:

```
# grep -i IgnoreUserKnownHosts /etc/ssh/sshd_config

IgnoreUserKnownHosts yes
```

If the value is returned as `no`, the returned line is commented out, or no output is returned, refer to the remediation procedure below.

Remediation:

Configure the SSH daemon to not allow authentication using known hosts authentication.
Add the following line in `/etc/ssh/sshd_config`, or uncomment the line and set the value to `yes`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment, or update the following line.

```
IgnoreUserKnownHosts yes
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72249

Rule ID: SV-86873r3_rule

STIG ID: RHEL-07-040380

Severity: CAT II
```

5.2.26 Ensure only FIPS 140-2 MACs are used for SSH (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

Rationale:

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

Audit:

Verify the SSH daemon is configured to only use MACs employing FIPS 140-2-approved ciphers.
Note: If Benchmark recommendation 1.5.7 fails, this is automatically a finding as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.
Check that the SSH daemon is configured to only use MACs employing FIPS 140-2-approved ciphers with the following command:

```
# grep -i macs /etc/ssh/sshd_config

MACs hmac-sha2-256,hmac-sha2-512
```

If any ciphers other than `hmac-sha2-256` or `hmac-sha2-512` are listed or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/ssh/sshd_config` file to uncomment or add the line for the `MACs` keyword and set its value to `hmac-sha2-256` and/or `hmac-sha2-512` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line.

```
MACs hmac-sha2-256,hmac-sha2-512
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72253

Rule ID: SV-86877r3_rule

STIG ID: RHEL-07-040400

Severity: CAT II
```

5.2.27 Ensure SSH does not permit GSSAPI (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Rationale:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Audit:

Verify the SSH daemon does not permit GSSAPI authentication unless approved.
Check that the SSH daemon does not permit GSSAPI authentication with the following command:

```
# grep -i gssapiauth /etc/ssh/sshd config

GSSAPIAuthentication no
```

If the `GSSAPIAuthentication` keyword is missing, is set to `yes` and is not documented with the Authorizing Official, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `GSSAPIAuthentication` keyword in `/etc/ssh/sshd_config` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to `no`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
GSSAPIAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

If GSSAPI authentication is required, it must be documented, to include the location of the configuration file.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72259

Rule ID: SV-86883r3_rule

STIG ID: RHEL-07-040430

Severity: CAT II
```

5.2.28 Ensure SSH does not permit Kerberos authentication (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

Rationale:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Audit:

Verify the SSH daemon does not permit Kerberos to authenticate passwords unless approved.
Check that the SSH daemon does not permit Kerberos to authenticate passwords with the following command:

```
# grep -i kerberosauth /etc/ssh/sshd_config

KerberosAuthentication no
```

If the `KerberosAuthentication` keyword is missing, or is set to `yes` and is not documented with the Authorizing Official, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `KerberosAuthentication` keyword in `/etc/ssh/sshd_config` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to `no`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
KerberosAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

If Kerberos authentication is required, it must be documented, to include the location of the configuration file.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72261

Rule ID: SV-86885r3_rule

STIG ID: RHEL-07-040440

Severity: CAT II
```

5.2.29 Ensrue SSH performs checks of home directory configuration files. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Audit:

Verify the SSH daemon performs strict mode checking of home directory configuration files.
The location of the `sshd_config` file may vary if a different daemon is in use.
Inspect the `sshd_config` file with the following command:

```
# grep -i strictmodes /etc/ssh/sshd_config

StrictModes yes
```

If `StrictModes` is set to `no`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `StrictModes` keyword in `/etc/ssh/sshd_config` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to `yes`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
StrictModes yes
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72263

Rule ID: SV-86887r3_rule

STIG ID: RHEL-07-040450

Severity: CAT II
```

5.2.30 Ensure SSH uses privilege seperation (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the SSH daemon uses privilege separation.

Rationale:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Audit:

Verify the SSH daemon performs privilege separation.
Check that the SSH daemon performs privilege separation with the following command:

```
# grep -i usepriv /etc/ssh/sshd_config

UsePrivilegeSeparation sandbox
```

If the `UsePrivilegeSeparation` keyword is set to `no`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `UsePrivilegeSeparation` keyword in `/etc/ssh/sshd_config` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to `sandbox` or `yes`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
UsePrivilegeSeparation sandbox
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72265

Rule ID: SV-86889r3_rule

STIG ID: RHEL-07-040460

Severity: CAT II
```

5.2.31 Ensure SSH compressions setting is delayed. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

Teh operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

Rationale:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Audit:

Verify the SSH daemon performs compression after a user successfully authenticates. Check that the SSH daemon performs compression after a user successfully authenticates with the following command:

```
# grep -i compression /etc/ssh/sshd_config

Compression delayed
```

If the `Compression` keyword is set to `yes`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `Compression` keyword in `/etc/ssh/sshd_config` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) on the system and set the value to `delayed` or `no`:
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
Compression no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72267

Rule ID: SV-86891r3_rule

STIG ID: RHEL-07-040470

Severity: CAT II
```

5.2.32 Ensure no ".shosts" files exist on the system (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not contain .shosts files.

Rationale:

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no `.shosts` files on the system.
Check the system for the existence of these files with the following command:

```
# find / -name '*.shosts'
```

If any `.shosts` files are found on the system, refer to the remediation procedure below.

Remediation:

Remove any found `.shosts` files from the system.
Refer to the list found in the Audit section and apply the path to the file in the example below:

```
# rm /[path]/[to]/[file]/.shosts
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72277

Rule ID: SV-86901r2_rule

STIG ID: RHEL-07-040540

Severity: CAT I
```

5.2.33 Ensure no "shosts.equiv" files exist on the system (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not contain shosts.equiv files.

Rationale:

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no `shosts.equiv` files on the system.
Check the system for the existence of these files with the following command:

```
# find / -name shosts.equiv
```

If any `shosts.equiv` files are found on the system, refer to the remediation below.

Remediation:

Remove any found `shosts.equiv` files from the system.
Refer to the list found in the Audit section and apply the path to the file in the example below:

```
# rm /[path]/[to]/[file]/shosts.equiv
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72279

Rule ID: SV-86903r2_rule

STIG ID: RHEL-07-040550

Severity: CAT I
```

5.2.34 Ensure remote X connections are encrypted. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that remote X connections for interactive users are encrypted.

Rationale:

Open X displays allow an attacker to capture keystrokes and execute commands remotely.

Audit:

Verify remote X connections for interactive users are encrypted.
Check that remote X connections are encrypted with the following command:

```
# grep -i x11forwarding /etc/ssh/sshd_config | grep -v "^#"

X11Forwarding yes
```

If the `X11Forwarding` keyword is set to `no` or is missing, refer to the remediation procedure below.

Remediation:

Configure SSH to encrypt connections for interactive users.
Edit the `/etc/ssh/sshd_config` file to uncomment or add the line for the `X11Forwarding` keyword and set its value to `yes` (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):
Example: `vim /etc/ssh/sshd_config`
Add, uncomment or update the following line:

```
X11Forwarding yes
```

The SSH service must be restarted for changes to take effect:

```
# systemctl restart sshd
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72303

Rule ID: SV-86927r4_rule

STIG ID: RHEL-07-040710

Severity: CAT I
```

5.3 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

5.3.1 Ensure password creation requirements are configured (Scored)

Profile Applicability:

- Level 1

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.

```
try_first_pass - retrieve the password from a previous stacked PAM module. If
not available, then prompt the user for a password.

retry=3 - Allow 3 tries before sending back a failure.
```

The following options are set in the /etc/security/pwquality.conf file:

```
minlen = 14 - password must be 14 characters or more

dcredit = -1 - provide at least one digit

ucredit = -1 - provide at least one uppercase character

ocredit = -1 - provide at least one special character

lcredit = -1 - provide at least one lowercase character
```

The 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:

Run the following commands and verify all password requirements conform to organization policy and minlen is 14 or more:

```
# grep pam_pwquality.so /etc/pam.d/password-auth
password requisite pam_pwquality.so try_first_pass retry=3

# grep pam_pwquality.so /etc/pam.d/system-auth
password requisite pam_pwquality.so try_first_pass retry=3

# grep ^minlen /etc/security/pwquality.conf
minlen = 14

# grep ^dcredit /etc/security/pwquality.conf
dcredit = -1

# grep ^lcredit /etc/security/pwquality.conf
lcredit = -1

# grep ^ocredit /etc/security/pwquality.conf
ocredit = -1

# grep ^ucredit /etc/security/pwquality.conf
ucredit = -1
```

Remediation:

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the appropriate options for pam_pwquality.so and to conform to site policy:

```
password requisite pam_pwquality.so try_first_pass retry=3
```

Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy:

```
minlen = 14
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation 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.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:
Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71903
Rule ID: SV-86527r3_rule
STIG ID: RHEL-07-010120
Severity: CAT II


Vul ID: V-71905
Rule ID: SV-86529r5_rule
STIG ID: RHEL-07-010130
Severity: CAT II


Vul ID: V-71907
Rule ID: SV-86531r3_rule
STIG ID: RHEL-07-010140
Severity: CAT II


Vul ID: V-71909
Rule ID: SV-86533r2_rule
STIG ID: RHEL-07-010150
```

```
Severity: CAT II



Vul ID: V-73159

Rule ID: SV-87811r4_rule

STIG ID: RHEL-07-010119

Severity: CAT II
```

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.

5.3.2 Ensure lockout for failed password attempts is configured (Scored)

Profile Applicability:

- Level 1

Description:

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

Set the lockout number to the policy in effect at your site.

Rationale:

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Review the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files and verify the following `pam_faillock.so` lines appear surrounding a `pam_unix.so` line and the `pam_unix.so` is `[success=1 default=bad]` as listed in both:

```
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth [success=1 default=bad] pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
```

Remediation:

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files and add the following `pam_faillock.so` lines surrounding a `pam_unix.so` line modify the `pam_unix.so` is `[success=1 default=bad]` as listed in both:

```
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth [success=1 default=bad] pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_tally2.so` or `pam_faillock.so` module, the user can be unlocked by issuing the command `pam_tally2 -u <username> --reset` or `faillock -u --reset` respectively. This command sets the failed count to 0, effectively unlocking the user.

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.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71943

Rule ID: SV-86567r4_rule

STIG ID: RHEL-07-010320

Severity: CAT II
```

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.

5.3.3 Ensure password reuse is limited (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

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

Audit:

Run the following commands and ensure the `remember` option is '5' or more and included in all results:

```
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/password-auth
password sufficient pam_unix.so remember=5
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/system-auth
password sufficient pam_unix.so remember=5
```

Or run the following commands and ensure the remember option is '5' or more and included in all results:

```
# egrep '^password\s+required\s+pam_pwhistory.so' /etc/pam.d/password-auth
password required pam_pwhistory.so remember=5
# egrep '^password\s+required\s+pam_pwhistory.so' /etc/pam.d/system-auth
password required pam_pwhistory.so remember=5
```

Remediation:

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the remember option and conform to site policy as shown:

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

or

```
password required pam_pwhistory.so remember=5
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

5.3.4 Ensure password hashing algorithm is SHA-512 (Scored)

Profile Applicability:

- Level 1

Description:

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

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

Audit:

Verify password hashing algorithm is `sha512`. This setting is commonly configured with the `pam_unix.so sha512` option found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`.
Run the following commands and ensure the `sha512` option is included in all results:

```
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/password-auth
password sufficient pam_unix.so sha512
# egrep '^password\s+sufficient\s+pam_unix.so' /etc/pam.d/system-auth
password sufficient pam_unix.so sha512
```

Remediation:

Set password hashing algorithm to sha512. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_unix.so` lines to include the sha512 option:
Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the `sha512` option for `pam_unix.so` as shown:

```
password sufficient pam_unix.so sha512
```

Notes:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# cat /etc/passwd | awk -F: '( $3 >= 500 && $1 != "nfsnobody" ) { print $1 }'
| xargs -n 1 chage -d 0
```

This command assumes a system UID split at 500. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71919

Rule ID: SV-86543r3_rule

STIG ID: RHEL-07-010200

Severity: CAT II
```

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

5.3.5 Ensure minimum and maximum requirements are set for password changes (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that when passwords are changed a minimum of `8` of the total number of characters must be changed and a minimum of `4` character classes must be changed. The operating system must also be configured so that when passwords are changed the number of repeating consecutive characters must not be more than `3` characters and the number of repeating characters of the same character class must not be more than `4` characters. The operating system must be configured so that passwords are a minimum of `15` characters in length.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

The `difok` option sets the number of characters in a password that must not be present in the old password. The `minclass` option sets the minimum number of required classes of characters for the new password `(digits, upper-case, lower-case, others)`. The `maxrepeat` option sets the maximum number of allowed same consecutive characters in a new password. The `maxclassrepeat` option sets the maximum number of allowed same consecutive characters in the same class in the new password. The `minlen` option sets the minimum number of characters in a new password.

Check for the value of the `difok` option in `/etc/security/pwquality.conf` with the following command:

```
# grep difok /etc/security/pwquality.conf

difok = 8
```

Check for the value of the `minclass` option in `/etc/security/pwquality.conf` with the following command:

```
# grep minclass /etc/security/pwquality.conf

minclass = 4
```

Check for the value of the `maxrepeat` option in `/etc/security/pwquality.conf` with the following command:

```
# grep maxrepeat /etc/security/pwquality.conf

maxrepeat = 3
```

Check for the value of the `maxclassrepeat` option in `/etc/security/pwquality.conf` with the following command:

```
# grep maxclassrepeat /etc/security/pwquality.conf

maxclassrepeat = 4
```

Check for the value of the `minlen` option in `/etc/security/pwquality.conf` with the following command:

```
# grep minlen /etc/security/pwquality.conf

minlen = 15
```

If the value of `difok` is set to less than `8` and/or `minclass` is set to less than `4`, and/or the value of `maxrepeat` is set to more than `3`, and/or the value of `maxclassrepeat` is set to more than `4`, and/or it does not return a `minlen` value of `15` or greater, please refer to the remediation procedure below.

Remediation:

Configure the operating system to require the change of at least `8` of the total number of characters when passwords are changed by setting the `difok` option and the `minclass` option and the `maxrepeat` option and the `maxclassrepeat` and the `minlen` option as defined below.
Add the following lines to `/etc/security/pwquality.conf` (or modify the line to have the required value):
Example: `vim /etc/security/pwquality.conf`

```
difok = 8
minclass = 4
maxrepeat = 3
maxclassrepeat = 4
minlen = 15
```

Impact:

Consult your documentation for the appropriate PAM file and module. 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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71911

Rule ID: SV-86535r2_rule

STIG ID: RHEL-07-010160

Severity: CAT II



Vul ID: V-71913

Rule ID: SV-86537r2_rule

STIG ID: RHEL-07-010170
```

```
Severity: CAT II


Vul ID: V-71915

Rule ID: SV-86539r3_rule

STIG ID: RHEL-07-010180

Severity: CAT II


Vul ID: V-71917

Rule ID: SV-86541r2_rule

STIG ID: RHEL-07-010190

Severity: CAT II


Vul ID: V-71935

Rule ID: SV-86559r2_rule

STIG ID: RHEL-07-010280

Severity: CAT II
```

5.3.6 Ensure no accounts are configured with blank or null passwords (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have accounts configured with `blank` or `null` passwords.

Rationale:

If an account has an `blank` password, anyone could log on and run commands with the privileges of that account. Accounts with 'blank' passwords should never be used in operational environments.

Audit:

To verify that `null` or `blank` passwords cannot be used, run the following command:

```
# grep nullok /etc/pam.d/system-auth /etc/pam.d/password-auth

password           sufficient             pam_unix.so    sha=512   shadow
nullok   try_first_pass  use_authtok
```

If this produces any output, it may be possible to log on with accounts with 'blank' passwords.
If `null` or `blank' passwords can be used, please refer to the remediation procedure below.

Remediation:

If an account is configured for password authentication but does not have an assigned password, it may be possible to log on to the account without authenticating.
Remove any instances of the `nullok` option in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` to prevent logons with `empty` or `blank` passwords.
Example: `vim /etc/pam.d/system-auth`
Remove `nullok` from the line show below:

```
password            sufficient              pam_unix.so     sha=512    shadow
nullok    try_first_pass   use_authtok
```

Impact:

Note: Manual changes to the listed files may be overwritten by the `authconfig` program. The `authconfig` program should not be used to update the configurations listed in this requirement.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71937

Rule ID: SV-86561r3_rule

STIG ID: RHEL-07-010290

Severity: CAT I
```

5.3.7 Ensure lockout for unsuccessful root logon attempts (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must lock the associated account after `3` unsuccessful `root` logon attempts are made within a `15-minute` period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Audit:

Verify the operating system automatically locks the `root` account until it is released by an administrator when `3` unsuccessful logon attempts in `15` minutes are made.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the `even_deny_root` setting is not defined on both lines with the `pam_faillock.so` module, is commented out, or is missing from a line, refer to the remediation procedure below.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the `even_deny_root` setting is not defined on both lines with the `pam_faillock.so` module, is commented out, or is missing from a line, refer to the remediation procedure below.

Remediation:

To configure the operating system to lock automatically the `root` account until the locked account is released by an administrator when `3` unsuccessful logon attempts in `15` minutes are made.
Modify the first `3` lines of the `auth` section and the first line of the `account` section of the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files to match the following lines:
Example: `vim /etc/pam.d/system-auth`
Add, uncomment or update the following lines in each file:

```
auth required pam_faillock.so preauth silent audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
auth sufficient pam_unix.so try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

Impact:

Note: Manual changes to the listed files may be overwritten by the "authconfig" program. The "authconfig" program should not be used to update the configurations listed in this requirement.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71945

Rule ID: SV-86569r4_rule

STIG ID: RHEL-07-010330

Severity: CAT II
```

5.3.8 Ensure date and time of last successful logon. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must display the `date` and `time` of the last successful account logon upon logon.

Rationale:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify users are provided with feedback on when account accesses last occurred.
Check that `pam_lastlog` is used and not silent with the following command:

```
# grep pam_lastlog /etc/pam.d/postlogin

session required pam_lastlog.so showfailed
```

If `pam_lastlog` is missing from `/etc/pam.d/postlogin` file, or the silent option is present, refer to the remediation procedure below.

Remediation:

Configure the operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in `/etc/pam.d/postlogin`.
Example: `vim /etc/pam.d/postlogin`
Add the following line to the top of the file:

```
session required pam_lastlog.so showfailed
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72275

Rule ID: SV-86899r4_rule

STIG ID: RHEL-07-040530

Severity: CAT III
```

5.3.9 Ensure multifactor authentication for access to privileged accounts (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules `(PAM)`.

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Audit:

Verify the operating system implements multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).
Check the /etc/sssd/sssd.conf file for the authentication services that are being used with the following command:

```
# grep services /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf

services = nss, pam
```

If the pam service is not present on all services lines, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement multifactor authentication for remote access to privileged accounts via PAM.
Modify all of the services lines in /etc/sssd/sssd.conf or in configuration files found under /etc/sssd/conf.d to include pam.
Example: vim /etc/sssd/sssd.conf
Add pam to the service line as shown here:

```
services = nss, pam
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72427

Rule ID: SV-87051r4_rule

STIG ID: RHEL-07-041002

Severity: CAT II
```

5.3.10 Ensure certificate status checking for PKI authentication. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must implement certificate status checking for `PKI authentication`.

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

Audit:

Verify the operating system implements certificate status checking for `PKI authentication`.
Check to see if Online Certificate Status Protocol `(OCSP)` is enabled on the system with the following command:

```
# grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -v "^#"

cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
```

There should be at least `3` lines returned.
If `ocsp_on` is not present in all uncommented `cert_policy` lines in `/etc/pam_pkcs11/pam_pkcs11.conf`, refer to the remediation procedure below.

Remediation:

Configure the operating system to do certificate status checking for `PKI authentication`.
Modify all of the `cert_policy` lines in `/etc/pam_pkcs11/pam_pkcs11.conf` to include `ocsp_on`.
Note: Make sure there is a minimum of `3` cert_policy lines.
Example: `vim /etc/pam_pkcs11/pam_pkcs11.conf`
Add, uncomment or update the `cert_policy` lines to inlcude `ocsp_on`:

```
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72433

Rule ID: SV-87057r5_rule

STIG ID: RHEL-07-041003

Severity: CAT II
```

5.3.11 Ensure system-auth is used when changing passwords (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that `/etc/pam.d/passwd` implements `/etc/pam.d/system-auth` when changing passwords.

Rationale:

Pluggable authentication modules `(PAM)` allow for a modular approach to integrating authentication methods. `PAM` operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Audit:

Verify that `/etc/pam.d/passwd` is configured to use `/etc/pam.d/system-auth` when changing passwords:

```
# cat /etc/pam.d/passwd | grep -i substack | grep -i system-auth

password substack system-auth
```

If no results are returned, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure `PAM` to utilize `/etc/pam.d/system-auth` when changing passwords.
Add the following line to `/etc/pam.d/passwd` (or modify the line to have the required value):
Example: `vim /etc/pam.d/passwd`
Add, uncomment or update the following line:

```
password substack system-auth
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-81003

Rule ID: SV-95715r1_rule

STIG ID: RHEL-07-010118

Severity: CAT II
```

5.3.12 Ensure password prohibited reuse is at a minumum `5` (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that passwords are prohibited from reuse for a minimum of `5` generations.

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Audit:

Verify the operating system prohibits password reuse for a minimum of `5` generations. Check for the value of the `remember` argument in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` with the following command:

```
# grep -i remember /etc/pam.d/system-auth /etc/pam.d/password-auth

password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

If the line containing the `pam_pwhistory.so` line does not have the `remember` module argument set, is commented out, or the value of the `remember` module argument is set to less than `5`, refer to the remediation procedure below.

Remediation:

To configure the operating system to prohibit password reuse for a minimum of 5 generations.
Add the following line in /etc/pam.d/system-auth and /etc/pam.d/password-auth (or modify the line to have the required value):
Example: vim /etc/pam.d/system-auth
Add, uncomment or update the following line:

```
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

Note: Manual changes to the listed files may be overwritten by the authconfig program. The authconfig program should not be used to update the configurations listed in this requirement.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71933

Rule ID: SV-86557r3_rule

STIG ID: RHEL-07-010270

Severity: CAT II
```

5.4 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.4.1 Set Shadow Password Suite Parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs`will only be applied if the `usermod`command is used. If user IDs are added a different way, use the `chage`command to effect changes to individual user IDs.

5.4.1.1 Ensure password expiration is 365 days or less (Scored)

Profile Applicability:

- Level 1

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy (no more than 365 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 (no more than 365 days):

```
# grep -E '^[^:]+:[^!*]' /etc/shadow | cut -d: -f1,5

<user>:<PASS_MAX_DAYS>
```

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>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 5th field should be 365 or less for all users with a password.

Note: A value of -1 will disable password expiration. Additionally 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.

5.4.1.2 Ensure minimum days between password changes is 7 or more (Scored)

Profile Applicability:

- Level 1

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 7 days):

```
# grep PASS_MIN_DAYS /etc/login.defs

PASS_MIN_DAYS 7
```

Run the following command and Review list of users and PAS_MIN_DAYS to Verify that all users' PAS_MIN_DAYS conform s to site policy (no less than 7 days):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,4

<user>:<PASS_MIN_DAYS>
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 7 in `/etc/login.defs` :

```
PASS_MIN_DAYS 7
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 4th field should be 7 or more for all users with a password.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71925

Rule ID: SV-86549r2_rule

STIG ID: RHEL-07-010230

Severity: CAT II


Vul ID: V-71927

Rule ID: SV-86551r2_rule

STIG ID: RHEL-07-010240

Severity: CAT II
```

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.

5.4.1.3 Ensure password expiration warning days is 7 or more (Scored)

Profile Applicability:

- Level 1

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

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):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,6

<user>:<PASS_WARN_AGE>
```

Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs` :

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 6th field should be 7 or more for all users with a password.

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.

5.4.1.4 Ensure inactive password lock is 30 days or less (Scored)

Profile Applicability:

- Level 1

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 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):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,7

<user>:<INACTIVE>
```

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>
```

Notes:

You can also check this setting in `/etc/shadow` directly. The 7th field should be 30 or less for all users with a password.

Note: 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.

5.4.1.5 Ensure all users last password change date is in the past (Scored)

Profile Applicability:

- Level 1

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

```
# for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep
'^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(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.

5.4.1.6 Ensure encrypted respresentation of passwords is set. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured to use the shadow file to store only encrypted representations of passwords.

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the system's shadow file is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is `SHA512`.
Check that the system is configured to create `SHA512` hashed passwords with the following command:

```
# grep -i encrypt /etc/login.defs

ENCRYPT_METHOD SHA512
```

If the `/etc/login.defs` configuration file does not exist or allows for password hashes other than `SHA512` to be used, refer to the remediation procedure below.

Remediation:

Configure the operating system to store only `SHA512` encrypted representations of passwords.
Add or update the following line in `/etc/login.defs`:
Example: `vim /etc/login.defs`
Add, uncomment or update the following line:

```
ENCRYPT_METHOD SHA512
```

Notes:

This Benchmark maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71921

Rule ID: SV-86545r2_rule

STIG ID: RHEL-07-010210

Severity: CAT II
```

5.4.1.7 Ensure account administration utilities are configured to store only encrypted representations of passwords. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The Operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the user and group account administration utilities are configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is `SHA512`.
Check that the system is configured to create `SHA512` hashed passwords with the following command:

```
# grep -i sha512 /etc/libuser.conf

crypt_style = sha512
```

If the `crypt_style` variable is not set to `sha512`, is not in the defaults section, is commented out, or does not exist, refer to the remediation procedure below.

Remediation:

Configure the operating system to store only `SHA512` encrypted representations of passwords.
Add or update the following line in `/etc/libuser.conf` in the [defaults] section:
Example: `vim /etc/libuser.conf`
Add, uncomment or update the following line:

```
crypt_style = sha512
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71923

Rule ID: SV-86547r3_rule

STIG ID: RHEL-07-010220

Severity: CAT II
```

5.4.1.8 Ensure password expiration is 60 Day maximum for new users (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

If passwords are not being used for authentication, this is Not Applicable.
Verify the operating system enforces a 60-day maximum password lifetime restriction for new user accounts.
Check for the value of `PASS_MAX_DAYS` in `/etc/login.defs` with the following command:

```
# grep -i pass_max_days /etc/login.defs

PASS_MAX_DAYS 60
```

If the `PASS_MAX_DAYS` parameter value is not `60` or less, or is commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to enforce a 60-day maximum password lifetime restriction.
Add the following line in `/etc/login.defs` (or modify the line to have the required value):

```
PASS_MAX_DAYS 60
```

Notes:

This Benchmark Recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71929

Rule ID: SV-86553r2_rule

STIG ID: RHEL-07-010250

Severity: CAT II
```

5.4.1.9 Ensure password expiration is 60 Day maximum for exisiting passwords (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

Check whether the maximum time period for existing passwords is restricted to 60 days.

```
# awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, refer to the remediation procedure below.

Remediation:

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.
Using the list or accounts collected in the Audit and run this command on the Users:

```
# chage -M 60 [user]
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71931

Rule ID: SV-86555r3_rule

STIG ID: RHEL-07-010260

Severity: CAT II
```

5.4.1.10 Ensure delay between logon prompts on failure (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt.
Check the value of the `fail_delay` parameter in the `/etc/login.defs` file with the following command:

```
# grep -i fail_delay /etc/login.defs

FAIL_DELAY 4
```

If the value of `FAIL_DELAY` is not set to `4` or greater, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.
Modify the `/etc/login.defs` file to set the `FAIL_DELAY` parameter to `4` or greater:
Example: `vim /etc/login.defs`
Add, uncomment or update the following line:

```
FAIL_DELAY 4
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71951

Rule ID: SV-86575r2_rule

STIG ID: RHEL-07-010430

Severity: CAT II
```

5.4.1.11 Ensure inactive password lock is 0 days (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Audit:

If passwords are not being used for authentication, this is Not Applicable.
Verify the operating system disables account identifiers (individuals, groups, roles, and devices) after the password expires with the following command:

```
# grep -i inactive /etc/default/useradd

INACTIVE=0
```

If the value is not set to `0`, is commented out, or is not defined, refer to the remediation procedure below.

Remediation:

Configure the operating system to disable account identifiers (individuals, groups, roles, and devices) after the password expires.
Add the following line to `/etc/default/useradd` (or modify the line to have the required value):
Example: `vim /etc/default/useradd`
Add, uncomment or update the following line:

```
INACTIVE=0
```

Notes:

The Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71941

Rule ID: SV-86565r2_rule

STIG ID: RHEL-07-010310

Severity: CAT II
```

5.4.2 Ensure system accounts are secured (Scored)

Profile Applicability:

- Level 1

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" && $1!="sync" && $1!="shutdown" && $1!="halt" &&
$1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' &&
$7!="'"$(which nologin)"'" && $7!="/bin/false") {print}' /etc/passwd

awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

Remediation:

Run the commands appropriate for your distribution:
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" && $1!="sync" && $1!="shutdown" && $1!="halt" &&
$1!~/^\+/ && $3<'"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' &&
$7!="'"$(which nologin)"'" && $7!="/bin/false") {print $1}' /etc/passwd |
while read user do usermod -s $(which nologin) $user done
```

The following command will automatically lock not root system accounts:

```
awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s*UID MIN/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}' | while read user do usermod -L $user
done
```

Notes:

The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

5.4.3 Ensure default group for the root account is GID 0 (Scored)

Profile Applicability:

- Level 1

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

5.1 Establish Secure Configurations

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

5.4.4 Ensure default user umask is 027 or more restrictive (Scored)

Profile Applicability:

- Level 1

Description:

The default `umask` determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the `umask` command into the standard shell configuration files (`.profile` , `.bashrc` , etc.) in their home directories.

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Audit:

Run the following commands and verify all umask lines returned are 027 or more restrictive.

```
# grep "umask" /etc/bashrc
umask 027
# grep "umask" /etc/profile /etc/profile.d/*.sh
umask 027
```

Remediation:

Edit the `/etc/bashrc`, `/etc/profile` and `/etc/profile.d/*.sh` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
umask 027
```

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

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

5.4.5 Ensure default user shell timeout is 900 seconds or less (Scored)

Profile Applicability:

- Level 2

Description:

The default `TMOUT` determines the shell timeout for users. The TMOUT value is measured in seconds.

Rationale:

Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Audit:

Run the following commands and verify all TMOUT lines returned are 900 or less and at least one exists in each file.

```
# grep "^TMOUT" /etc/bashrc
readonly TMOUT=900 ; export TMOUT

# grep "^TMOUT" /etc/profile /etc/profile.d/*.sh
readonly TMOUT=900 ; export TMOUT
```

Remediation:

Edit the `/etc/bashrc`, `/etc/profile` and `/etc/profile.d/*.sh` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
readonly TMOUT=900 ; export TMOUT
```

Note that setting the value to `readonly` prevents unwanted modification during runtime.

Notes:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

5.4.6 Ensure users must provide password for escalation (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that users must provide a password for privilege escalation.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Audit:

***If passwords are not being used for authentication, this is Not Applicable.
Verify the operating system requires users to supply a password for privilege escalation.
Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -i nopasswd /etc/sudoers /etc/sudoers.d/*
```

If any uncommented line is found with a `NOPASSWD` tag, refer to the remediation procedure below.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.
Check the configuration of the `/etc/sudoers` file with the following command:

```
# vim /etc/sudoers
```

Remove any occurrences of `NOPASSWD` tags in the file.
Check the configuration of the `/etc/sudoers.d/*` files with the following command to get the list:

```
# grep -i nopasswd /etc/sudoers.d/*
```

Edit the list of files using this command:

```
# vim /etc/sudoers.d/path_of_file
```

Remove any occurrences of `NOPASSWD` tags in the file.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71947

Rule ID: SV-86571r3_rule

STIG ID: RHEL-07-010340

Severity: CAT II
```

5.4.7 Ensure users must re-autenticate for privilege escalation (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that users must re-authenticate for privilege escalation.

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Audit:

Verify the operating system requires users to reauthenticate for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

If any uncommented line is found with a `!authenticate` tag, refer to the remediation procedure below.

Remediation:

Configure the operating system to require users to reauthenticate for privilege escalation.
Check the configuration of the `/etc/sudoers` file with the following command:

```
# vim /etc/sudoers
```

Remove any occurrences of `!authenticate` tags in the file.
Check the configuration of the `/etc/sudoers.d/*` files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

Edit the list of files using this command:

```
# vim /etc/sudoers.d/path_of_file
```

Remove any occurrences of `!authenticate` tags in the file(s).

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71949

Rule ID: SV-86573r3_rule

STIG ID: RHEL-07-010350

Severity: CAT II
```

5.4.8 Ensure Default user umask is 077 (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.
Check for the value of the `UMASK` parameter in `/etc/login.defs` file with the following command:
Note: If the value of the `UMASK` parameter is set to `000` in `/etc/login.defs` file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs
UMASK 077
```

If the value for the `UMASK` parameter is not `077`, or the `UMASK` parameter is missing or is commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.
Add or edit the line for the `UMASK` parameter in `/etc/login.defs` file to `077`:
Example: `vim /etc/login.defs`
Add, uncomment or update the following line:

```
UMASK 077
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71995

Rule ID: SV-86619r2_rule

STIG ID: RHEL-07-020240

Severity: CAT II
```

5.4.9 Ensure there are no unnecessary accounts (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must not have unnecessary accounts.

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Audit:

Verify all accounts on the system are assigned to an active system, application, or user account.
Obtain the list of authorized system accounts from the Authorizing Official.
Check the system accounts on the system with the following command:

```
# more /etc/passwd

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.
If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, refer to the remediation procedure below.

Remediation:

Configure the system so all accounts on the system are assigned to an active system, application, or user account.
Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.
To remove the user, the user's home directory and the users mail spool

```
# userdel -r user's username
```

Document all authorized accounts on the system.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72001

Rule ID: SV-86625r2_rule

STIG ID: RHEL-07-020270

Severity: CAT II
```

5.4.10 Ensure default user umask is 077 (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must set the umask value to 077 for all local interactive user accounts.

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the default umask for all local interactive users is `077`.
Identify the locations of all local interactive user home directories by looking at the `/etc/passwd` file.
Check all local interactive user initialization files for interactive users with the following command:
Note: The example is for a system that is configured to create users home directories in the `/home` directory.

```
# grep -i umask /home/*/.*
```

If any local interactive user initialization `(dot)` files are found to have a umask statement that has a value less restrictive than `077`, refer to the remediation procedure below.

Remediation:

Remove the umask statement from all local interactive user's initialization files.
Using the list collected in the audit run the following command on all the files located with a less restrictive umask:

```
user@server# ~]$ echo 'umask 077' [] /home/user/path_to_file
```

If the account is for an application, the requirement for a umask less restrictive than `077` can be documented, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72049

Rule ID: SV-86673r2_rule

STIG ID: RHEL-07-021040

Severity: CAT II
```

5.4.11 Ensure default user shell timeout is 600 seconds or less (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all network connections associated with a communication session are terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

Verify the operating system terminates all network connections associated with a communications session at the end of the session or based on inactivity.
Check the value of the system inactivity timeout with the following command:

```
# grep -i tmout /etc/profile.d/*

etc/profile.d/tmout.sh:TMOUT=600

/etc/profile.d/tmout.sh:readonly TMOUT

/etc/profile.d/tmout.sh:export TMOUT
```

If `TMOUT` is not set to `600` or less in a script located in the `/etc/profile.d/` directory to enforce session termination after inactivity, refer to the remediation procedure below.

Remediation:

Configure the operating system to terminate all network connections associated with a communications session at the end of the session or after a period of inactivity.
Create a script to enforce the inactivity timeout (for example `/etc/profile.d/tmout.sh`) such as:
Example: `vim /etc/profile.d/tmout.sh`
Add the following lines to the script.

```
#!/bin/bash

TMOUT=600
readonly TMOUT
export TMOUT
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72223

Rule ID: SV-86847r4_rule

STIG ID: RHEL-07-040160

Severity: CAT II
```

5.5 Ensure root login is restricted to system console (Not Scored)

Profile Applicability:

- Level 1

Description:

The file `/etc/securetty` contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Audit:

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

Remediation:

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

CIS Controls:

Version 7

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

5.6 Ensure access to the su command is restricted (Scored)

Profile Applicability:

- Level 1

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in the wheel group to execute `su`.

Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following command and verify output includes matching line:

```
# grep pam_wheel.so /etc/pam.d/su
auth required pam_wheel.so use_uid
```

Run the following command and verify users in `wheel` group match site policy:

```
# grep wheel /etc/group
wheel:x:10:root,<user list>
```

Remediation:

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

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

Create a comma separated list of users in the wheel statement in the `/etc/group` file:

```
wheel:x:10:root,<user list>
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

5.7 Ensure multi-factor authentication is enable for users (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multi-factor authentication.

Rationale:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;

and

2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Audit:

Verify the operating system requires organizational users to use multifactor authentication.
Check to see if smartcard authentication is enforced on the system:

```
# authconfig --test | grep "pam_pkcs11 is enabled"
```

If no results are returned, refer to the remediation procedure below.
Check to see if smartcard removal action is set:

```
# authconfig --test | grep "smartcard removal action"
```

If smartcard removal action is blank, refer to the remediation procedure below.
Check to see if smartcard module is set:

```
# authconfig --test | grep "smartcard module"
```

If smartcard module is blank, refer to the remediation procedure below.

Remediation:

Configure the operating system to require individuals to be authenticated with a multifactor authenticator.
Enable smartcard logons with the following commands:

```
# authconfig --enablesmartcard --smartcardaction=0 --update
# authconfig --enablerequiresmartcard -update
```

Modify the `/etc/pam_pkcs11/pkcs11_eventmgr.conf` file to uncomment the following line:
Example: `vim /etc/pam_pkcs11/pkcs11_eventmgr.conf`
Uncomment the following line:

```
/usr/X11R6/bin/xscreensaver-command -lock
```

Note: Modify the `/etc/pam_pkcs11/pam_pkcs11.conf` file to use the cackey module if required.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71965

Rule ID: SV-86589r2_rule

STIG ID: RHEL-07-010500

Severity: CAT II
```

5.8 Ensure non-privileged users are prevented from executing privileged functions (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Rationale:

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Audit:

If an HBSS or HIPS is active on the system, this is Not Applicable.
Verify the operating system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
Get a list of authorized users (other than System Administrator and guest accounts) for the system.
Check the list against the system by using the following command:

```
# semanage login -l | more
Login Name SELinux User MLS/MCS Range Service
__default__ user_u s0-s0:c0.c1023 *
root unconfined_u s0-s0:c0.c1023 *
system_u system_u s0-s0:c0.c1023 *
joe staff_u s0-s0:c0.c1023 *
```

All administrators must be mapped to the `sysadm_u` or `staff_u` users role.
All authorized non-administrative users must be mapped to the `user_u` role.
If they are not mapped in this way, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
Utilizing the list of users gathered in the Audit section run the applicable command for that user below.
Use the following command to map a new user to the `sysdam_u` role:

```
#semanage login -a -s sysadm_u <username>
```

Use the following command to map an existing user to the `sysdam_u` role:

```
#semanage login -m -s sysadm_u <username>
```

Use the following command to map a new user to the `staff_u` role:

```
#semanage login -a -s staff_u <username>
```

Use the following command to map an existing user to the `staff_u` role:

```
#semanage login -m -s staff_u <username>
```

Use the following command to map a new user to the `user_u` role:

```
# semanage login -a -s user_u <username>
```

Use the following command to map an existing user to the `user_u` role:

```
# semanage login -m -s user_u <username>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71971

Rule ID: SV-86595r2_rule

STIG ID: RHEL-07-020020

Severity: CAT II
```

5.9 Ensure number of concurrent sessions is limited (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

Verify the operating system limits the number of concurrent sessions to `10` for all accounts and/or account types by issuing the following command:

```
# grep "maxlogins" /etc/security/limits.conf
* hard maxlogins 10
```

This can be set as a global domain `(with the * wildcard)` but may be set differently for multiple domains.
If the `maxlogins` item is missing, commented out, or the value is not set to `10` or less for all domains that have the `maxlogins` item assigned, refer to the remediation procedure below.

Remediation:

Configure the operating system to limit the number of concurrent sessions to `10` for all accounts and/or account types.
Example: `vim /etc/security/limits.conf`
Add the following line to the top of the `/etc/security/limits.conf`:

```
* hard maxlogins 10
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72217

Rule ID: SV-86841r2_rule

STIG ID: RHEL-07-040000

Severity: CAT III
```

5.10 Ensure enable smartcard authentication is set to true (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.

Rationale:

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Audit:

Verify the operating system uniquely identifies and authenticates users using multifactor authentication via a graphical user logon.
Note: If the system does not have GNOME installed, this requirement is Not Applicable.
Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user

system-db:local
```

Note: The example is using the database local for the system, so the path is `/etc/dconf/db/local.d`. This path must be modified if a database other than local is being used.

```
# grep enable-smartcard-authentication /etc/dconf/db/local.d/*

enable-smartcard-authentication=true
```

If `enable-smartcard-authentication` is set to `false` or the keyword is missing, refer to the remediation procedure below.

Remediation:

Configure the operating system to uniquely identify and authenticate users using multifactor authentication via a graphical user logon.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example is using the database local for the system, so if the system is using another database in `/etc/dconf/profile/user`, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/00-defaults
```

Edit `[org/gnome/login-screen]` and add or update the following line:

```
enable-smartcard-authentication=true
```

Update the system databases:

```
# dconf update
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-77819

Rule ID: SV-92515r2_rule

STIG ID: RHEL-07-010061

Severity: CAT II
```

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Audit system file permissions (Not Scored)

Profile Applicability:

- Level 2

Description:

The RPM and Debian package managers have a number of useful options. One of these, the `--verify` (or `-V` for RPM) option, can be used to verify that system packages are correctly installed. The `--verify` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

```
Code   Meaning

S      File size differs.

M      File mode differs (includes permissions and file type).

5      The MD5 checksum differs.

D      The major and minor version numbers differ on a device file.

L      A mismatch occurs in a link.

U      The file ownership differs.

G      The file group owner differs.

T      The file time (mtime) differs.
```

The `rpm -qf` or `dpkg -S` command can be used to determine which package a particular file belongs to. For example the following commands determines which package the `/bin/bash` file belongs to:

```
# rpm -qf /bin/bash

bash-4.1.2-29.el6.x86_64

# dpkg -S /bin/bash

bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V bash-4.1.2-29.el6.x86_64

.M.......    /bin/bash

# dpkg --verify bash

??5?????? c /etc/bash.bashrc
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`

.M...... c /etc/passwd

S.5....T c /etc/printcap
```

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Audit:

Run one of the following commands to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename>
# dpkg --verify > <filename>
```

Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

References:

1. http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html

Notes:

Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.

Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-71849

Rule ID: SV-86473r3_rule

STIG ID: RHEL-07-010010

Severity: CAT I


Vul ID: V-71855

Rule ID: SV-86479r3_rule

STIG ID: RHEL-07-010020

Severity: CAT I
```

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 (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

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

Audit:

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

```
# stat /etc/passwd

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

Remediation:

Run the following command to set permissions on `/etc/passwd` :

```
# chown root:root /etc/passwd

# chmod 644 /etc/passwd
```

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/shadow are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

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

Audit:

Run the following command and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow`, and `Access` is `640` or more restrictive:

```
# stat /etc/shadow

Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following chown command and the chmod to set permissions on `/etc/shadow` :

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

# chmod o-rwx,g-wx /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.

6.1.4 Ensure permissions on /etc/group are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

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

```
# stat /etc/group

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

Remediation:

Run the following command to set permissions on `/etc/group` :

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

# chmod 644 /etc/group
```

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/gshadow are configured (Scored)

Profile Applicability:

- Level 1

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: (    0/    root)
```

Remediation:

Run the following chown command and the chmod to set permissions on `/etc/gshadow` :

```
# chown root:root /etc/gshadow

# chmod o-rwx,g-rw /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.

6.1.6 Ensure permissions on /etc/passwd- are configured (Scored)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd-` file contains backup user account information.

Rationale:

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

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `600` or more restrictive:

```
# stat /etc/passwd-

Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd-` :

```
# chown root:root /etc/passwd-

# chmod u-x,go-rwx /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.

6.1.7 Ensure permissions on /etc/shadow- are configured (Scored)

Profile Applicability:

- Level 1

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: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following chown command and the chmod to set permissions on `/etc/shadow-` :

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

# chmod u-x,go-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/group- are configured (Scored)

Profile Applicability:

- Level 1

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-------)  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.

6.1.9 Ensure permissions on /etc/gshadow- are configured (Scored)

Profile Applicability:

- Level 1

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 verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow`, and `Access` is `640` or more restrictive:

```
# stat /etc/gshadow-

Access: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following chown command and the chmod to set permissions on `/etc/gshadow-` :

```
# chown root:root /etc/gshadow-

# chmod o-rwx,g-rw /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 (Scored)

Profile Applicability:

- Level 1

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72037

Rule ID: SV-86661r2_rule

STIG ID: RHEL-07-020730

Severity: CAT II
```

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

6.1.11 Ensure no unowned files or directories exist (Scored)

Profile Applicability:

- Level 1

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72007

Rule ID: SV-86631r3_rule

STIG ID: RHEL-07-020320

Severity: CAT II
```

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 (Scored)

Profile Applicability:

- Level 1

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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72009

Rule ID: SV-86633r3_rule

STIG ID: RHEL-07-020330

Severity: CAT II
```

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 (Not Scored)

Profile Applicability:

- Level 1

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

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 (Not Scored)

Profile Applicability:

- Level 1

Description:

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

Audit:

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 password fields are not empty (Scored)

Profile Applicability:

- Level 1

Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

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

Audit:

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

```
# 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.

6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Scored)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

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

```
# grep '^\+:' /etc/passwd
```

Remediation:

Remove any legacy '+' entries from `/etc/passwd` if they exist.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Scored)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

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

```
# grep '^\+:' /etc/shadow
```

Remediation:

Remove any legacy '+' entries from `/etc/shadow` if they exist.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)

Profile Applicability:

- Level 1

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

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

```
# grep '^\+:' /etc/group
```

Remediation:

Remove any legacy '+' entries from `/etc/group` if they exist.

CIS Controls:

Version 7

16.2 Configure Centralized Point of Authentication

Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.

6.2.5 Ensure root is the only UID 0 account (Scored)

Profile Applicability:

- Level 1

Description:

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72005

Rule ID: SV-86629r2_rule

STIG ID: RHEL-07-020310

Severity: CAT I
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

6.2.6 Ensure root PATH Integrity (Scored)

Profile Applicability:

- Level 1

Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in `root` 's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
if [ "$(echo "$PATH" | grep ::)" != "" ]; then
  echo "Empty Directory in PATH (::)"
fi

if [ "$(echo "$PATH" | grep :$)"  != "" ]; then
  echo "Trailing : in PATH"
fi

p=$(echo "$PATH" | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g')
set -- $p
while [ "$1" != "" ]; do
  if [ "$1" = "." ]; then
    shift
  continue
  fi
  if [ -d "$1" ]; then
    dirperm=$(ls -ldH "$1" | cut -f1 -d" ")
    if [ "$(echo "$dirperm" | cut -c6)" != "-" ]; then
      echo "Group Write permission set on directory $1"
    fi
    if [ "$(echo "$dirperm" | cut -c9)" != "-" ]; then
    echo "Other Write permission set on directory $1"
    fi
    dirown=$(ls -ldH "$1" | awk '{print $3}')
    if [ "$dirown" != "root" ] ; then
      echo "$1 is not owned by root"
    fi
  else
    echo "$1 is not a directory"
  fi
  shift
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

6.2.7 Ensure all users' home directories exist (Scored)

Profile Applicability:

- Level 1

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read -r user
dir; do
        if [ ! -d "$dir" ]; then
                echo "The home directory ($dir) of user $user does not exist."
        fi
done
```

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Notes:

The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72011

Rule ID: SV-86635r2_rule

STIG ID: RHEL-07-020600

Severity: CAT II


Vul ID: V-72015

Rule ID: SV-86639r2_rule

STIG ID: RHEL-07-020620

Severity: CAT II


Vul ID: V-72019

Rule ID: SV-86643r5_rule

STIG ID: RHEL-07-020640

Severity: CAT II


Vul ID: V-72059

Rule ID: SV-86683r2_rule

STIG ID: RHEL-07-021310

Severity: CAT III
```

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    dirperm=$(ls -ld $dir | cut -f1 -d" ")
    if [ $(echo $dirperm | cut -c6) != "-" ]; then
      echo "Group Write permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c8) != "-" ]; then
      echo "Other Read permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c9) != "-" ]; then
      echo "Other Write permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c10) != "-" ]; then
      echo "Other Execute permission set on the home directory ($dir) of user
$user"
    fi
  fi
done
```

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72017

Rule ID: SV-86641r3_rule

STIG ID: RHEL-07-020630

Severity: CAT II
```

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 users own their home directories (Scored)

Profile Applicability:

- Level 1

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
   owner=$(stat -L -c "%U" "$dir")
   if [ "$owner" != "$user" ]; then
     echo "The home directory ($dir) of user $user is owned by $owner."
   fi
 fi
done
```

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

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.

6.2.10 Ensure users' dot files are not group or world writable (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.[A-Za-z0-9]*; do
      if [ ! -h "$file" -a -f "$file" ]; then
        fileperm=$(ls -ld $file | cut -f1 -d" ")

        if [ $(echo $fileperm | cut -c6)  != "-" ]; then
          echo "Group Write permission set on file $file"
        fi
        if [ $(echo $fileperm | cut -c9)  != "-" ]; then
          echo "Other Write permission set on file $file"
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72037

Rule ID: SV-86661r2_rule

STIG ID: RHEL-07-020730

Severity: CAT II
```

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.

6.2.11 Ensure no users have .forward files (Scored)

Profile Applicability:

- Level 1

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
      echo ".forward file $dir/.forward exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

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

6.2.12 Ensure no users have .netrc files (Scored)

Profile Applicability:

- Level 1

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
      echo ".netrc file $dir/.netrc exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.2.13 Ensure users' .netrc Files are not group or world accessible (Scored)

Profile Applicability:

- Level 1

Description:

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

`.netrc`files may contain unencrypted passwords that may be used to attack other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.netrc; do
      if [ ! -h "$file" -a -f "$file" ]; then
        fileperm=$(ls -ld $file | cut -f1 -d" ")
        if [ $(echo $fileperm | cut -c5)  != "-" ]; then
          echo "Group Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c6)  != "-" ]; then
          echo "Group Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c7)  != "-" ]; then
          echo "Group Execute set on $file"
        fi
        if [ $(echo $fileperm | cut -c8)  != "-" ]; then
          echo "Other Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c9)  != "-" ]; then
          echo "Other Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c10)  != "-" ]; then
          echo "Other Execute set on $file"
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` file permissions and determine the action to be taken in accordance with site policy.

Notes:

While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.

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.

6.2.14 Ensure no users have .rhosts files (Scored)

Profile Applicability:

- Level 1

Description:

While no `.rhosts` files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.rhosts; do
      if [ ! -h "$file" -a -f "$file" ]; then
        echo ".rhosts file in $dir"
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.rhosts` files and determine the action to be taken in accordance with site policy.

Notes:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Scored)

Profile Applicability:

- Level 1

Description:

Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group` .

Rationale:

Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:

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.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72003

Rule ID: SV-86627r2_rule

STIG ID: RHEL-07-020300

Severity: CAT III
```

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

6.2.16 Ensure no duplicate UIDs exist (Scored)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

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

6.2.17 Ensure no duplicate GIDs exist (Scored)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

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.

Notes:

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

6.2.18 Ensure no duplicate user names exist (Scored)

Profile Applicability:

- Level 1

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read 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

6.2.19 Ensure no duplicate group names exist (Scored)

Profile Applicability:

- Level 1

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group` . Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/group | sort | uniq -d | while read 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

6.2.20 Ensure all local interactive user home directories are group-owned (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.

Rationale:

If the Group Identifier `(GID)` of a local interactive user's home directory is not the same as the primary `GID` of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user's primary `GID`.
Check the home directory assignment for all local interactive users on the system with the following command:

```
# ls -ld $(egrep ':[0-9]{4}' /etc/passwd | cut -d: -f6)

-rwxr-x--- 1 smithj users 18 Mar 5 17:06 /home/smithj
```

Check the user's primary group with the following command:

```
# grep users /etc/group

users:x:250:smithj,jonesj,jacksons
```

If the local interactive users home directory referenced in `/etc/passwd` is not group-owned by that user's primary `GID`, refer to the remediation procedure below.

Remediation:

Change the group owner of a local interactive user's home directory to the group found in `/etc/passwd`. To change the group owner of a local interactive user's home directory, use the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`, and has a primary group of users.

```
# chgrp users /home/smithj
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72021

Rule ID: SV-86645r5_rule

STIG ID: RHEL-07-020650

Severity: CAT II
```

6.2.21 Ensure that all files and directories contained in local interactive user home directories are owned by the user (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all files and directories contained in local interactive user home directories are owned by the user of the home directory.

Rationale:

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Audit:

Verify all files and directories in a local interactive user's home directory are owned by the user.
Check the owner of all files and directories in a local interactive user's home directory with the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`.

```
# ls -lLR /home/smithj

-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r--r-- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files are found with an owner different than the home directory user, refer to the remediation procedure below.

Remediation:

Change the owner of a local interactive user's files and directories to that owner. To change the owner of a local interactive user's files and directories, use the following command: Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`.

```
# chown smithj /home/smithj/<file or directory>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72023

Rule ID: SV-86647r2_rule

STIG ID: RHEL-07-020660

Severity: CAT II
```

6.2.22 Ensure local interactive user is a member of the group owner. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

Rationale:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Audit:

Verify all files and directories in a local interactive user home directory are group-owned by a group the user is a member of.
Check the group owner of all files and directories in a local interactive user's home directory with the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`.

```
# ls -lLR /<home directory>/<users home directory>/

-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r--r-- 1 smithj sa 231 Mar 5 17:06 file3
```

If any files are found with an owner different than the group home directory user, check to see if the user is a member of that group with the following command:

```
# grep smithj /etc/group

sa:x:100:juan,shelley,bob,smithj
smithj:x:521:smithj
```

If the user is not a member of a group that group owns file(s) in a local interactive user's home directory, refer to the remediation procedure below.

Remediation:

Change the group of a local interactive user's files and directories to a group that the interactive user is a member of. To change the group owner of a local interactive user's files and directories, use the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj` and is a member of the users group.

```
# chgrp users /home/smithj/<file>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72025

Rule ID: SV-86649r2_rule

STIG ID: RHEL-07-020670

Severity: CAT II
```

6.2.23 Ensure local interactive users' dot files for are owned by the user or root. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local initialization `(dot)` files for interactive users are owned by the home directory user or root.

Rationale:

Local initialization `(dot)` files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify all local initialization files for interactive users are owned by the `home directory user` or `root`.
Check the owner on all local initialization files with the following command:
Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj`.

```
# ls -al /home/smithj/.* | more

-rwxr-xr-x 1 smithj users 896 Mar 10 2011 .bash_profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .profile
```

If any file that sets a local interactive user's environment variables to override the system is not owned by the `home directory owner` or `root`, refer to the remediation procedure below.

Remediation:

Set the owner of the local initialization files for interactive users to either the `home directory owner` or `root` with the following command:
Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj`.

```
# chown smithj /home/smithj/.*
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72029

Rule ID: SV-86653r2_rule

STIG ID: RHEL-07-020690

Severity: CAT II
```

6.2.24 Ensure local interactive users' dot files are group-owned by the users group or root. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local initialization `(dot)` files for local interactive users are group-owned by the `users primary group` or `root`.

Rationale:

Local initialization `(dot)` files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify the local initialization files of all local interactive users are group-owned by that user's primary Group Identifier (GID).
Check the home directory assignment for all non-privileged users on the system with the following command:
Note: The example will be for the smithj user, who has a home directory of /home/smithj and a primary group of users.

```
# cut -d: -f 1,4,6 /etc/passwd | egrep ":[1-4][0-9]{3}"

smithj:1000:/home/smithj

# grep 1000 /etc/group

users:x:1000:smithj,jonesj,jacksons
```

Note: This may miss interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.
Check the group owner of all local interactive user's initialization files with the following command:

```
# ls -al /home/smithj/.*

-rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something
```

If all local interactive user's initialization files are not group-owned by that user's primary GID, refer to the remediation procedure below.

Remediation:

Change the group owner of a local interactive user's files to the group found in `/etc/passwd` for the user. To change the group owner of a local interactive user's home directory, use the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`, and has a primary group of users.

```
# chgrp users /home/smithj/<file>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72031

Rule ID: SV-86655r3_rule

STIG ID: RHEL-07-020700

Severity: CAT II
```

6.2.25 Ensure users' `dot` files have `0740` or less set. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local initialization `(dot)` files have mode `0740` or less permissive.

Rationale:

Local initialization `(dot)` files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify that all local initialization files have a mode of `0740` or less permissive.
Check the mode on all local initialization files with the following command:
Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj`.

```
# ls -al /home/smithj/.* | more

-rwxr----- 1 smithj users 896 Mar 10 2011 .profile
-rwxr----- 1 smithj users 497 Jan 6 2007 .login
-rwxr----- 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than `0740`, refer to the remediation procedure below.

Remediation:

Set the mode of the local initialization files to `0740` with the following command:
Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj`.

```
# chmod 0740 /home/smithj/.<INIT_FILE>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72033

Rule ID: SV-86657r2_rule

STIG ID: RHEL-07-020710

Severity: CAT II
```

6.2.26 Ensure local interactive users' `dot` files executable paths resolve to the users home directory. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local interactive user initialization `(dot)` files executable search paths contain only paths that resolve to the users home directory.

Rationale:

The executable search path `(typically the PATH environment variable)` contains a list of directories for the shell to search to find executables. If this path includes the current working directory `(other than the user's home directory)`, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Audit:

Verify that all local interactive user initialization files' `(dot)` executable search path statements do not contain statements that will reference a working directory other than the users' home directory.
Check the executable search path statement for all local interactive user initialization files in the users' home directory with the following commands:
Note: The example will be for the `smithj` user, which has a home directory of `/home/smithj`.

```
# grep -i path /home/smithj/.*

/home/smithj/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/bin
/home/smithj/.bash_profile:export PATH
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, refer to the remediation procedure below.

Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.
Note: The example will be for the `smithj` user, which has a home directory of `/home/smithj`.
Utilizing the files listed in the Audit run this command to edit them and change the PATH variable statement.
Example: `vim /home/smithj/.bash_profile`
Update the PATH accordingly:

```
:PATH=$PATH:$HOME/.local/bin:$HOME/bin
```

If a local interactive user requires path variables to reference a directory owned by the application, it must be documented with the ISSO.

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72035

Rule ID: SV-86659r4_rule

STIG ID: RHEL-07-020720

Severity: CAT II
```

6.2.27 Ensure nosuid is set on users' home directories. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that file systems containing user home directories are mounted to prevent files with the `setuid` and `setgid` bit set from being executed.

Rationale:

The `nosuid` mount option causes the system to not execute `setuid` and `setgid` files with owner privileges. This option must be used for mounting any file system not containing approved `setuid` and `setguid` files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that contain user home directories are mounted with the `nosuid` option. Find the file system(s) that contain the user home directories with the following command: Note: If a separate file system has not been created for the user home directories `(user home directories are mounted under "/")`, this is not a finding as the `nosuid` option cannot be used on the `/` system.

```
# cut -d: -f 1,3,6 /etc/passwd | egrep ":[1-4][0-9]{3}"

smithj:1001:/home/smithj
thomasr:1002:/home/thomasr
```

Check the file systems that are mounted at boot time with the following command:

```
# more /etc/fstab

UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4
rw,relatime,discard,data=ordered,nosuid 0 2
```

If a file system found in `/etc/fstab` refers to the user home directory file system and it does not have the `nosuid` option set, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `nosuid` option on file systems that contain user home directories.
Example: `vim /etc/fstab`
Update any of the file systems listed without the `nosuid` option"

```
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4
rw,relatime,discard,data=ordered,nosuid 0 2
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019

Vul ID: V-72041

Rule ID: SV-86665r4_rule

STIG ID: RHEL-07-021000

Severity: CAT II
```

6.2.28 Ensure upon user creation a home directory is assigned. (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify all local interactive users on the system are assigned a home directory upon creation.
Check to see if the system is configured to create home directories for local interactive users with the following command:

```
# grep -i create_home /etc/login.defs

CREATE_HOME yes
```

If the value for `CREATE_HOME` parameter is not set to `yes`, the line is missing, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to assign home directories to all new local interactive users by setting the `CREATE_HOME` parameter in `/etc/login.defs` to `yes` as follows.
Example: `vim /etc/login.defs`
Add, uncomment or update the following line:

```
CREATE_HOME yes
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72013

Rule ID: SV-86637r2_rule

STIG ID: RHEL-07-020610

Severity: CAT II
```

6.2.29 Ensure users' files and directories within the home directory permissions are 750 or more restrictive (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of `0750` or less permissive.

Rationale:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of `0750`.
Check the mode of all non-initialization files in a local interactive user home directory with the following command:
Files that begin with a `.` are excluded from this requirement.
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj`.

```
# ls -lLR /home/smithj

-rwxr-x--- 1 smithj smithj 18 Mar 5 17:06 file1
-rwxr----- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r-x--- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files are found with a mode more permissive than `0750`, refer to the remediation procedure below.

Remediation:

Set the mode on files and directories in the local interactive user home directory with the following command:
Note: The example will be for the user `smithj`, who has a home directory of `/home/smithj` and is a member of the users group.

```
# chmod 0750 /home/smithj/<file>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-72027

Rule ID: SV-86651r2_rule

STIG ID: RHEL-07-020680

Severity: CAT II
```

6.3 Ensure removal of software components after update (Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must remove all software components after updated versions have been installed.

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Verify the operating system removes all software components after updated versions have been installed.
Check if `yum` is configured to remove unneeded packages with the following command:

```
# grep -i clean_requirements_on_remove /etc/yum.conf

clean_requirements_on_remove=1
```

If `clean_requirements_on_remove` is not set to `1`, `True`, or `yes`, or is not set in `/etc/yum.conf`, refer to the remediation procedure below.

Remediation:

Configure the operating system to remove all software components after updated versions have been installed.
Set the `clean_requirements_on_remove` option to `1` in the `/etc/yum.conf` file:
Example: `vim /etc/yum.conf`
Add, uncomment or update the following line:

```
clean_requirements_on_remove=1
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019



Vul ID: V-71987

Rule ID: SV-86611r2_rule

STIG ID: RHEL-07-020200

Severity: CAT III
```

6.4 Ensure system device files are labeled. (Not Scored)

Profile Applicability:

- Level 3 - STIG

Description:

The operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

Rationale:

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Audit:

Verify that all system device files are correctly labeled to prevent unauthorized modification.
List all device files on the system that are incorrectly labeled with the following commands:
Note: Device files are normally found under `/dev`, but applications may place device files in other directories and may necessitate a search of the entire system.

```
# find /dev -context *:device_t:* \( -type c -o -type b \) -printf "%p %Z\n"

# find /dev -context *:unlabeled_t:* \( -type c -o -type b \) -printf "%p
%Z\n"
```

Note: There are device files, such as `/dev/vmci`, that are used when the operating system is a host virtual machine. They will not be owned by a user on the system and require the `device_t` label to operate. These device files are not a finding.
If there is output from either of these commands, other than already noted, refer to the remediation procedure below.

Remediation:

Run the following command to determine which package owns the device file:

```
# rpm -qf <filename>
```

The package can be reinstalled from a `yum` repository using the command:

```
# sudo yum reinstall <packagename>
```

Alternatively, the package can be reinstalled from trusted media using the command:

```
# sudo rpm -Uvh <packagename>
```

Notes:

This Benchmark recommendation maps to:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide:

Version 2, Release: 3 Benchmark Date: 26 Apr 2019


Vul ID: V-72039

Rule ID: SV-86663r2_rule

STIG ID: RHEL-07-020900

Severity: CAT II
```

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Initial Setup**		
1.1	**Filesystem Configuration**		
1.1.1	**Disable unused filesystems**		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Scored)	☐	☐
1.1.1.2	Ensure mounting of hfs filesystems is disabled (Scored)	☐	☐
1.1.1.3	Ensure mounting of hfsplus filesystems is disabled (Scored)	☐	☐
1.1.1.4	Ensure mounting of squashfs filesystems is disabled (Scored)	☐	☐
1.1.1.5	Ensure mounting of udf filesystems is disabled (Scored)	☐	☐
1.1.2	Ensure /tmp is configured (Scored)	☐	☐
1.1.3	Ensure seperate file system for /tmp (Scored)	☐	☐
1.1.4	Ensure nodev option set on /tmp partition (Scored)	☐	☐
1.1.5	Ensure nosuid option set on /tmp partition (Scored)	☐	☐
1.1.6	Ensure noexec option set on /tmp partition (Scored)	☐	☐
1.1.7	Ensure separate partition exists for /var (Scored)	☐	☐
1.1.8	Ensure separate partition exists for /var/tmp (Scored)	☐	☐
1.1.9	Ensure nodev option set on /var/tmp partition (Scored)	☐	☐
1.1.10	Ensure nosuid option set on /var/tmp partition (Scored)	☐	☐
1.1.11	Ensure noexec option set on /var/tmp partition (Scored)	☐	☐
1.1.12	Ensure separate partition exists for /var/log (Scored)	☐	☐
1.1.13	Ensure separate partition exists for /var/log/audit (Scored)	☐	☐
1.1.14	Ensure separate partition exists for /home (Scored)	☐	☐
1.1.15	Ensure nodev option set on /home partition (Scored)	☐	☐
1.1.16	Ensure nodev option set on /dev/shm partition (Scored)	☐	☐
1.1.17	Ensure nosuid option set on /dev/shm partition (Scored)	☐	☐
1.1.18	Ensure noexec option set on /dev/shm partition (Scored)	☐	☐
1.1.19	Ensure sticky bit is set on all world-writable directories (Scored)	☐	☐
1.1.20	Disable Automounting (Scored)	☐	☐
1.1.21	Ensure all world-writable directories are group-owned. (Not Scored)	☐	☐
1.2	**Configure Software Updates**		
1.2.1	Ensure package manager repositories are configured (Not Scored)	☐	☐
1.2.2	Ensure GPG keys are configured (Not Scored)	☐	☐
1.2.3	Ensure gpgcheck is globally activated (Scored)	☐	☐

1.2.4	Ensure software packages have been digitally signed by a Certificate Authority (CA) (Scored)	☐	☐
1.2.5	Ensure the version of the operating system is an active vendor supported release. (Not Scored)	☐	☐
1.3	**Filesystem Integrity Checking**		
1.3.1	Ensure AIDE is installed (Scored)	☐	☐
1.3.2	Ensure filesystem integrity is regularly checked (Scored)	☐	☐
1.3.3	Ensure AIDE is configured to verify ACLs (Scored)	☐	☐
1.3.4	Ensure AIDE is configured to verify XATTRS (Scored)	☐	☐
1.3.5	Ensure AIDE is configured to use FIPS 140-2 (Scored)	☐	☐
1.4	**Secure Boot Settings**		
1.4.1	Ensure permissions on bootloader config are configured (Scored)	☐	☐
1.4.2	Ensure authentication required for single user mode (Scored)	☐	☐
1.4.3	Ensure boot loader does not allow removable media (Scored)	☐	☐
1.4.4	Ensure UEFI requires authentication for single-user and maintenance modes. (Scored)	☐	☐
1.5	**Additional Process Hardening**		
1.5.1	Ensure core dumps are restricted (Scored)	☐	☐
1.5.2	Ensure address space layout randomization (ASLR) is enabled (Scored)	☐	☐
1.5.3	Ensure prelink is disabled (Scored)	☐	☐
1.5.4	Ensure the Ctrl-Alt-Delete key sequence is disabled. (Scored)	☐	☐
1.5.5	Ensure kernel core dumps are disabled. (Scored)	☐	☐
1.5.6	Ensure NIST FIPS-validated cryptography is configured (Scored)	☐	☐
1.5.7	Ensure DNS is servers are configured (Scored)	☐	☐
1.6	**Mandatory Access Control**		
1.6.1	**Configure SELinux**		
1.6.1.1	Ensure SELinux is installed (Scored)	☐	☐
1.6.1.2	Ensure SELinux is not disabled in bootloader configuration (Scored)	☐	☐
1.6.1.3	Ensure the SELinux state is enforcing (Scored)	☐	☐
1.6.1.4	Ensure SELinux policy is configured (Scored)	☐	☐
1.6.1.5	Ensure SETroubleshoot is not installed (Scored)	☐	☐
1.6.1.6	Ensure the MCS Translation Service (mcstrans) is not installed (Scored)	☐	☐
1.6.1.7	Ensure no unconfined daemons exist (Scored)	☐	☐
1.7	**Warning Banners**		
1.7.1	**Command Line Warning Banners**		

1.7.1.1	Ensure message of the day is configured properly (Scored)	☐	☐
1.7.1.2	Ensure local login warning banner is configured properly (Scored)	☐	☐
1.7.1.3	Ensure remote login warning banner is configured properly (Scored)	☐	☐
1.7.1.4	Ensure permissions on /etc/motd are configured (Scored)	☐	☐
1.7.1.5	Ensure permissions on /etc/issue are configured (Scored)	☐	☐
1.7.1.6	Ensure permissions on /etc/issue.net are configured (Scored)	☐	☐
1.7.1.7	Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Scored)	☐	☐
1.8	Ensure updates, patches, and additional security software are installed (Scored)	☐	☐
1.9	Ensure anti-virus is installed and running (Not Scored)	☐	☐
1.10	Ensure required packages for multifactor atuentication are installed (Scored)	☐	☐
1.11	Ensure host-based intrusion detection tool is used (Not Scored)	☐	☐
2	**Services**		
2.1	**inetd Services**		
2.1.1	Ensure the rsh package has been removed (Scored)	☐	☐
2.1.2	Ensure the ypserv package has been removed (Scored)	☐	☐
2.1.3	Ensure the TFTP server has not been installed (Scored)	☐	☐
2.1.4	Ensure TFTP daemon is configured to operate in secure mode. (Scored)	☐	☐
2.2	**Special Purpose Services**		
2.2.1	**Time Synchronization**		
2.2.1.1	Ensure time synchronization is in use (Not Scored)	☐	☐
2.2.1.2	Ensure ntp is configured (Scored)	☐	☐
2.2.1.3	Ensure chrony is configured (Scored)	☐	☐
2.2.1.4	Ensure NTP "maxpoll" is set. (Scored)	☐	☐
2.2.2	**GNOME Configuration**		
2.2.2.1	Ensure the screen package is installed. (Scored)	☐	☐
2.2.2.2	Ensure GNOME Screen Lock is Enabled. (Scored)	☐	☐
2.2.2.3	Ensure GNOME Screensaver period of inactivity is configured. (Scored)	☐	☐
2.2.2.4	Ensure GNOME Idle activation is set. (Scored)	☐	☐
2.2.2.5	Ensure GNOME Lock Delay is configured (Scored)	☐	☐
2.2.2.6	Ensure automatic logon via GUI is not allowed (Scored)	☐	☐
2.2.2.7	Ensure unrestricted logon is not allowed (Scored)	☐	☐
2.2.2.8	Ensure overriding the screensaver lock-delay setting is prevented (Scored)	☐	☐
2.2.2.9	Ensure session idle-delay settings is enforced (Scored)	☐	☐

2.2.2.10	Ensure screensaver lock-enabled is set. (Scored)	☐	☐
2.2.2.11	Ensure the screensaver idle-activation-enabled setting (Scored)	☐	☐
2.2.3	Ensure X Window System is not installed (Scored)	☐	☐
2.2.4	Ensure Avahi Server is not enabled (Scored)	☐	☐
2.2.5	Ensure CUPS is not enabled (Scored)	☐	☐
2.2.6	Ensure DHCP Server is not enabled (Scored)	☐	☐
2.2.7	Ensure LDAP server is not enabled (Scored)	☐	☐
2.2.8	Ensure NFS and RPC are not enabled (Scored)	☐	☐
2.2.9	Ensure DNS Server is not enabled (Scored)	☐	☐
2.2.10	Ensure FTP Server is not enabled (Scored)	☐	☐
2.2.11	Ensure HTTP server is not enabled (Scored)	☐	☐
2.2.12	Ensure IMAP and POP3 server is not enabled (Scored)	☐	☐
2.2.13	Ensure Samba is not enabled (Scored)	☐	☐
2.2.14	Ensure HTTP Proxy Server is not enabled (Scored)	☐	☐
2.2.15	Ensure SNMP Server is not enabled (Scored)	☐	☐
2.2.16	Ensure mail transfer agent is configured for local-only mode (Scored)	☐	☐
2.2.17	Ensure rsync service is not enabled (Scored)	☐	☐
2.2.18	Ensure NIS Server is not enabled (Scored)	☐	☐
2.2.19	Ensure rsh server is not enabled (Scored)	☐	☐
2.2.20	Ensure telnet server is not enabled (Scored)	☐	☐
2.2.21	Ensure tftp server is not enabled (Scored)	☐	☐
2.2.22	Ensure rsync service is not enabled (Scored)	☐	☐
2.2.23	Ensure talk server is not enabled (Scored)	☐	☐
2.2.24	Ensure default SNMP community strings don't exist (Scored)	☐	☐
2.2.25	Ensure unrestricted mail relaying is prevented. (Scored)	☐	☐
2.2.26	Ensure ldap_tls_cacert is set for LDAP. (Scored)	☐	☐
2.2.27	Ensure ldap_id_use_start_tls is set for LDAP. (Scored)	☐	☐
2.2.28	Ensure ldap_tls_reqcert is set for LDAP (Scored)	☐	☐
2.2.29	Ensure nosuid option is set for NFS (Scored)	☐	☐
2.2.30	Ensure NFS is configured to use RPCSEC_GSS. (Scored)	☐	☐
2.2.31	Ensure noexec option is configured for NFS. (Scored)	☐	☐
2.3	**Service Clients**		
2.3.1	Ensure NIS Client is not installed (Scored)	☐	☐
2.3.2	Ensure rsh client is not installed (Scored)	☐	☐
2.3.3	Ensure talk client is not installed (Scored)	☐	☐
2.3.4	Ensure telnet client is not installed (Scored)	☐	☐
2.3.5	Ensure LDAP client is not installed (Scored)	☐	☐
3	**Network Configuration**		
3.1	**Network Parameters (Host Only)**		
3.1.1	Ensure IP forwarding is disabled (Scored)	☐	☐

3.1.2	Ensure packet redirect sending is disabled (Scored)	☐	☐
3.1.3	Ensure network interfaces are not in promiscuous mode (Not Scored)	☐	☐
3.2	**Network Parameters (Host and Router)**		
3.2.1	Ensure source routed packets are not accepted (Scored)	☐	☐
3.2.2	Ensure ICMP redirects are not accepted (Scored)	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted (Scored)	☐	☐
3.2.4	Ensure suspicious packets are logged (Scored)	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored (Scored)	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored (Scored)	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled (Scored)	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled (Scored)	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted (Scored)	☐	☐
3.2.10	Ensure rate limiting measures are set. (Scored)	☐	☐
3.3	**TCP Wrappers**		
3.3.1	Ensure TCP Wrappers is installed (Scored)	☐	☐
3.3.2	Ensure /etc/hosts.allow is configured (Not Scored)	☐	☐
3.3.3	Ensure /etc/hosts.deny is configured (Not Scored)	☐	☐
3.3.4	Ensure permissions on /etc/hosts.allow are configured (Scored)	☐	☐
3.3.5	Ensure permissions on /etc/hosts.deny are configured (Scored)	☐	☐
3.4	**Uncommon Network Protocols**		
3.4.1	Ensure DCCP is disabled (Scored)	☐	☐
3.4.2	Ensure SCTP is disabled (Scored)	☐	☐
3.4.3	Ensure RDS is disabled (Scored)	☐	☐
3.4.4	Ensure TIPC is disabled (Scored)	☐	☐
3.5	**Firewall Configuration**		
3.5.1	**Configure iptables**		
3.5.1.1	**Ensure Firewall software is installed**		
3.5.1.1.1	Ensure iptables is installed (Scored)	☐	☐
3.5.1.2	**Configure IPv4 iptables**		
3.5.1.2.1	Ensure default deny firewall policy (Scored)	☐	☐
3.5.1.2.2	Ensure loopback traffic is configured (Scored)	☐	☐
3.5.1.2.3	Ensure outbound and established connections are configured (Not Scored)	☐	☐
3.5.1.2.4	Ensure firewall rules exist for all open ports (Scored)	☐	☐
3.5.1.3	**Configure IPv6 ip6tables**		
3.5.1.3.1	Ensure IPv6 default deny firewall policy (Scored)	☐	☐
3.5.1.3.2	Ensure IPv6 loopback traffic is configured (Scored)	☐	☐
3.5.1.3.3	Ensure IPv6 outbound and established connections are configured (Not Scored)	☐	☐

3.5.1.3.4	Ensure IPv6 firewall rules exist for all open ports (Not Scored)	☐	☐
3.6	Disable IPv6 (Not Scored)	☐	☐
3.7	Ensure IP tunnels are not configured. (Scored)	☐	☐
4	**Logging and Auditing**		
4.1	**Configure System Accounting (auditd)**		
4.1.1	**Configure Data Retention**		
4.1.1.1	Ensure audit log storage size is configured (Scored)	☐	☐
4.1.1.2	Ensure system is disabled when audit logs are full (Scored)	☐	☐
4.1.1.3	Ensure audit logs are not automatically deleted (Scored)	☐	☐
4.1.1.4	Ensure audit logs are stored on a different system. (Not Scored)	☐	☐
4.1.1.5	Ensure audit logs on seperate system are encrypted. (Scored)	☐	☐
4.1.2	**Configure audit of commands**		
4.1.2.1	Ensure all uses of the passwd command are audited. (Scored)	☐	☐
4.1.2.2	Ensure auditing of the unix_chkpwd command (Scored)	☐	☐
4.1.2.3	Ensure audit of the gpasswd command (Scored)	☐	☐
4.1.2.4	Ensure audit all uses of chage (Scored)	☐	☐
4.1.2.5	Ensure audit all uses of the newgrp command. (Scored)	☐	☐
4.1.2.6	Ensure audit all uses of the chsh command. (Scored)	☐	☐
4.1.2.7	Ensure audit the umount command (Scored)	☐	☐
4.1.2.8	Ensure audit of postdrop command (Scored)	☐	☐
4.1.2.9	Ensure audit of postqueue command. (Scored)	☐	☐
4.1.2.10	Enusre audit ssh-keysign command. (Scored)	☐	☐
4.1.2.11	Ensure audit of crontab command (Scored)	☐	☐
4.1.2.12	Ensure audit pam_timestamp_check command (Scored)	☐	☐
4.1.2.13	Ensure audit of kmod command (Scored)	☐	☐
4.1.2.14	Ensure audit of the rmdir syscall (Scored)	☐	☐
4.1.2.15	Ensure audit of unlink syscall (Scored)	☐	☐
4.1.2.16	Ensure audit unlinkat syscall (Scored)	☐	☐
4.1.2.17	Ensure audit of the create_module syscall. (Scored)	☐	☐
4.1.2.18	Ensure audit of the finit_module syscall (Scored)	☐	☐
4.1.2.19	Ensure audit of semanage command (Scored)	☐	☐
4.1.2.20	Ensure audit of the setsebool command. (Scored)	☐	☐
4.1.2.21	Ensure audit of the chcon command (Scored)	☐	☐
4.1.2.22	Ensure audit of setfiles command (Scored)	☐	☐
4.1.2.23	Ensure audit of the userhelper command (Scored)	☐	☐
4.1.2.24	Ensure audit of the su command (Scored)	☐	☐
4.1.2.25	Ensure audit of the mount command and syscall (Scored)	☐	☐
4.1.3	Ensure auditd service is enabled (Scored)	☐	☐

4.1.4	Ensure auditing for processes that start prior to auditd is enabled (Scored)	☐	☐
4.1.5	Ensure events that modify date and time information are collected (Scored)	☐	☐
4.1.6	Ensure events that modify user/group information are collected (Scored)	☐	☐
4.1.7	Ensure events that modify the system's network environment are collected (Scored)	☐	☐
4.1.8	Ensure events that modify the system's Mandatory Access Controls are collected (Scored)	☐	☐
4.1.9	Ensure login and logout events are collected (Scored)	☐	☐
4.1.10	Ensure session initiation information is collected (Scored)	☐	☐
4.1.11	Ensure discretionary access control permission modification events are collected (Scored)	☐	☐
4.1.12	Ensure unsuccessful unauthorized file access attempts are collected (Scored)	☐	☐
4.1.13	Ensure use of privileged commands is collected (Scored)	☐	☐
4.1.14	Ensure successful file system mounts are collected (Scored)	☐	☐
4.1.15	Ensure file deletion events by users are collected (Scored)	☐	☐
4.1.16	Ensure changes to system administration scope (sudoers) is collected (Scored)	☐	☐
4.1.17	Ensure system administrator actions (sudolog) are collected (Scored)	☐	☐
4.1.18	Ensure the audit configuration is immutable (Scored)	☐	☐
4.1.19	Ensure kernel module loading and unloading is collected (Scored)	☐	☐
4.1.20	Ensure the auditing processing failures are handled. (Scored)	☐	☐
4.1.21	Ensure auditing of all privileged functions (Scored)	☐	☐
4.1.22	Ensure auditd service is active (Scored)	☐	☐
4.2	**Configure Logging**		
4.2.1	**Ensure the correct logging software is installed**		
4.2.1.1	Ensure rsyslog or syslog-ng is installed (Scored)	☐	☐
4.2.2	**Configure rsyslog**		
4.2.2.1	Ensure rsyslog Service is enabled (Scored)	☐	☐
4.2.2.2	Ensure logging is configured (Not Scored)	☐	☐
4.2.2.3	Ensure rsyslog default file permissions configured (Scored)	☐	☐
4.2.2.4	Ensure rsyslog is configured to send logs to a remote log host (Scored)	☐	☐
4.2.2.5	Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)	☐	☐
4.2.2.6	Ensure rsyslog imudp and imrelp aren't loaded. (Not Scored)	☐	☐

4.2.3	**Configure syslog-ng**		
4.2.3.1	Ensure syslog-ng service is enabled (Scored)	☐	☐
4.2.3.2	Ensure logging is configured (Not Scored)	☐	☐
4.2.3.3	Ensure syslog-ng default file permissions configured (Scored)	☐	☐
4.2.3.4	Ensure syslog-ng is configured to send logs to a remote log host (Not Scored)	☐	☐
4.2.3.5	Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)	☐	☐
4.2.4	Ensure permissions on all logfiles are configured (Scored)	☐	☐
4.3	Ensure logrotate is configured (Not Scored)	☐	☐
4.4	Ensure audit system is set to single when the disk is full. (Not Scored)	☐	☐
4.5	Ensure system notification is sent out when voume is 75% full (Not Scored)	☐	☐
4.6	Ensure audit system action is defined for sending errors (Not Scored)	☐	☐
4.7	Enable use of the au-remote plugin (Not Scored)	☐	☐
4.8	Enure off-load of audit logs. (Not Scored)	☐	☐
4.9	Ensure action is taken when audisp-remote buffer is full (Not Scored)	☐	☐
4.10	Ensure off-loaded audit logs are labeled. (Not Scored)	☐	☐
5	**Access, Authentication and Authorization**		
5.1	**Configure cron**		
5.1.1	Ensure cron daemon is enabled (Scored)	☐	☐
5.1.2	Ensure permissions on /etc/crontab are configured (Scored)	☐	☐
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Scored)	☐	☐
5.1.4	Ensure permissions on /etc/cron.daily are configured (Scored)	☐	☐
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Scored)	☐	☐
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Scored)	☐	☐
5.1.7	Ensure permissions on /etc/cron.d are configured (Scored)	☐	☐
5.1.8	Ensure at/cron is restricted to authorized users (Scored)	☐	☐
5.2	**SSH Server Configuration**		
5.2.1	Ensure SSH is installed (Scored)	☐	☐
5.2.2	Ensure SSH is running (Scored)	☐	☐
5.2.3	Ensure permissions on /etc/ssh/sshd_config are configured (Scored)	☐	☐

5.2.4	Ensure permissions on SSH private host key files are configured (Scored)	☐	☐
5.2.5	Ensure permissions on SSH public host key files are configured (Scored)	☐	☐
5.2.6	Ensure SSH Protocol is set to 2 (Scored)	☐	☐
5.2.7	Ensure SSH LogLevel is appropriate (Scored)	☐	☐
5.2.8	Ensure SSH X11 forwarding is disabled (Scored)	☐	☐
5.2.9	Ensure SSH MaxAuthTries is set to 4 or less (Scored)	☐	☐
5.2.10	Ensure SSH IgnoreRhosts is enabled (Scored)	☐	☐
5.2.11	Ensure SSH HostbasedAuthentication is disabled (Scored)	☐	☐
5.2.12	Ensure SSH root login is disabled (Scored)	☐	☐
5.2.13	Ensure SSH PermitEmptyPasswords is disabled (Scored)	☐	☐
5.2.14	Ensure SSH PermitUserEnvironment is disabled (Scored)	☐	☐
5.2.15	Ensure only strong Ciphers are used (Scored)	☐	☐
5.2.16	Ensure only strong MAC algorithms are used (Scored)	☐	☐
5.2.17	Ensure only strong Key Exchange algorithms are used (Scored)	☐	☐
5.2.18	Ensure SSH Idle Timeout Interval is configured (Scored)	☐	☐
5.2.19	Ensure SSH LoginGraceTime is set to one minute or less (Scored)	☐	☐
5.2.20	Ensure SSH access is limited (Scored)	☐	☐
5.2.21	Ensure SSH warning banner is configured (Scored)	☐	☐
5.2.22	Ensure only FIPS 140-2 ciphers are used for SSH (Scored)	☐	☐
5.2.23	Ensure RSA rhosts authentication is not allowed (Scored)	☐	☐
5.2.24	Ensure Printlastlog is enabled (Scored)	☐	☐
5.2.25	Ensure SSH setting for "IgnoreUserKnownHosts" is enabled. (Scored)	☐	☐
5.2.26	Ensure only FIPS 140-2 MACs are used for SSH (Scored)	☐	☐
5.2.27	Ensure SSH does not permit GSSAPI (Scored)	☐	☐
5.2.28	Ensure SSH does not permit Kerberos authentication (Scored)	☐	☐
5.2.29	Ensrue SSH performs checks of home directory configuration files. (Scored)	☐	☐
5.2.30	Ensure SSH uses privilege seperation (Scored)	☐	☐
5.2.31	Ensure SSH compressions setting is delayed. (Scored)	☐	☐
5.2.32	Ensure no ".shosts" files exist on the system (Scored)	☐	☐
5.2.33	Ensure no "shosts.equiv" files exist on the system (Scored)	☐	☐
5.2.34	Ensure remote X connections are encrypted. (Scored)	☐	☐
5.3	**Configure PAM**		
5.3.1	Ensure password creation requirements are configured (Scored)	☐	☐
5.3.2	Ensure lockout for failed password attempts is configured (Scored)	☐	☐

5.3.3	Ensure password reuse is limited (Scored)	☐	☐
5.3.4	Ensure password hashing algorithm is SHA-512 (Scored)	☐	☐
5.3.5	Ensure minimum and maximum requirements are set for password changes (Scored)	☐	☐
5.3.6	Ensure no accounts are configured with blank or null passwords (Scored)	☐	☐
5.3.7	Ensure lockout for unsuccessful root logon attempts (Scored)	☐	☐
5.3.8	Ensure date and time of last successful logon. (Scored)	☐	☐
5.3.9	Ensure multifactor authentication for access to privileged accounts (Scored)	☐	☐
5.3.10	Ensure certificate status checking for PKI authentication. (Scored)	☐	☐
5.3.11	Ensure system-auth is used when changing passwords (Scored)	☐	☐
5.3.12	Ensure password prohibited reuse is at a minumum `5` (Scored)	☐	☐
5.4	**User Accounts and Environment**		
5.4.1	**Set Shadow Password Suite Parameters**		
5.4.1.1	Ensure password expiration is 365 days or less (Scored)	☐	☐
5.4.1.2	Ensure minimum days between password changes is 7 or more (Scored)	☐	☐
5.4.1.3	Ensure password expiration warning days is 7 or more (Scored)	☐	☐
5.4.1.4	Ensure inactive password lock is 30 days or less (Scored)	☐	☐
5.4.1.5	Ensure all users last password change date is in the past (Scored)	☐	☐
5.4.1.6	Ensure encrypted respresentation of passwords is set. (Scored)	☐	☐
5.4.1.7	Ensure account administration utilities are configured to store only encrypted representations of passwords. (Scored)	☐	☐
5.4.1.8	Ensure password expiration is 60 Day maximum for new users (Scored)	☐	☐
5.4.1.9	Ensure password expiration is 60 Day maximum for exisiting passwords (Scored)	☐	☐
5.4.1.10	Ensure delay between logon prompts on failure (Scored)	☐	☐
5.4.1.11	Ensure inactive password lock is 0 days (Scored)	☐	☐
5.4.2	Ensure system accounts are secured (Scored)	☐	☐
5.4.3	Ensure default group for the root account is GID 0 (Scored)	☐	☐
5.4.4	Ensure default user umask is 027 or more restrictive (Scored)	☐	☐
5.4.5	Ensure default user shell timeout is 900 seconds or less (Scored)	☐	☐

5.4.6	Ensure users must provide password for escalation (Scored)	☐	☐
5.4.7	Ensure users must re-autenticate for privilege escalation (Scored)	☐	☐
5.4.8	Ensure Default user umask is 077 (Scored)	☐	☐
5.4.9	Ensure there are no unnecessary accounts (Not Scored)	☐	☐
5.4.10	Ensure default user umask is 077 (Scored)	☐	☐
5.4.11	Ensure default user shell timeout is 600 seconds or less (Scored)	☐	☐
5.5	Ensure root login is restricted to system console (Not Scored)	☐	☐
5.6	Ensure access to the su command is restricted (Scored)	☐	☐
5.7	Ensure multi-factor authentication is enable for users (Scored)	☐	☐
5.8	Ensure non-privileged users are prevented from executing privileged functions (Not Scored)	☐	☐
5.9	Ensure number of concurrent sessions is limited (Scored)	☐	☐
5.10	Ensure enable smartcard authentication is set to true (Scored)	☐	☐
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Audit system file permissions (Not Scored)	☐	☐
6.1.2	Ensure permissions on /etc/passwd are configured (Scored)	☐	☐
6.1.3	Ensure permissions on /etc/shadow are configured (Scored)	☐	☐
6.1.4	Ensure permissions on /etc/group are configured (Scored)	☐	☐
6.1.5	Ensure permissions on /etc/gshadow are configured (Scored)	☐	☐
6.1.6	Ensure permissions on /etc/passwd- are configured (Scored)	☐	☐
6.1.7	Ensure permissions on /etc/shadow- are configured (Scored)	☐	☐
6.1.8	Ensure permissions on /etc/group- are configured (Scored)	☐	☐
6.1.9	Ensure permissions on /etc/gshadow- are configured (Scored)	☐	☐
6.1.10	Ensure no world writable files exist (Scored)	☐	☐
6.1.11	Ensure no unowned files or directories exist (Scored)	☐	☐
6.1.12	Ensure no ungrouped files or directories exist (Scored)	☐	☐
6.1.13	Audit SUID executables (Not Scored)	☐	☐
6.1.14	Audit SGID executables (Not Scored)	☐	☐
6.2	**User and Group Settings**		
6.2.1	Ensure password fields are not empty (Scored)	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd (Scored)	☐	☐

6.2.3	Ensure no legacy "+" entries exist in /etc/shadow (Scored)	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group (Scored)	☐	☐
6.2.5	Ensure root is the only UID 0 account (Scored)	☐	☐
6.2.6	Ensure root PATH Integrity (Scored)	☐	☐
6.2.7	Ensure all users' home directories exist (Scored)	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive (Scored)	☐	☐
6.2.9	Ensure users own their home directories (Scored)	☐	☐
6.2.10	Ensure users' dot files are not group or world writable (Scored)	☐	☐
6.2.11	Ensure no users have .forward files (Scored)	☐	☐
6.2.12	Ensure no users have .netrc files (Scored)	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible (Scored)	☐	☐
6.2.14	Ensure no users have .rhosts files (Scored)	☐	☐
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group (Scored)	☐	☐
6.2.16	Ensure no duplicate UIDs exist (Scored)	☐	☐
6.2.17	Ensure no duplicate GIDs exist (Scored)	☐	☐
6.2.18	Ensure no duplicate user names exist (Scored)	☐	☐
6.2.19	Ensure no duplicate group names exist (Scored)	☐	☐
6.2.20	Ensure all local interactive user home directories are group-owned (Scored)	☐	☐
6.2.21	Ensure that all files and directories contained in local interactive user home directories are owned by the user (Scored)	☐	☐
6.2.22	Ensure local interactive user is a member of the group owner. (Scored)	☐	☐
6.2.23	Ensure local interactive users' dot files for are owned by the user or root. (Not Scored)	☐	☐
6.2.24	Ensure local interactive users' dot files are group-owned by the users group or root. (Not Scored)	☐	☐
6.2.25	Ensure users' `dot` files have `0740` or less set. (Not Scored)	☐	☐
6.2.26	Ensure local interactive users' `dot` files executable paths resolve to the users home directory. (Not Scored)	☐	☐
6.2.27	Ensure nosuid is set on users' home directories. (Scored)	☐	☐
6.2.28	Ensure upon user creation a home directory is assigned. (Scored)	☐	☐
6.2.29	Ensure users' files and directories within the home directory permissions are 750 or more restrictive (Scored)	☐	☐
6.3	Ensure removal of software components after update (Scored)	☐	☐
6.4	Ensure system device files are labeled. (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Mar 19, 2020	1.0.0	PUBLISHED