the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Red Hat Enterprise Linux 5

Version 2.0.0

December 16th, 2011

http://cisecurity.org

feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Red Hat Enterprise Linux 5* provides prescriptive guidance for establishing a secure configuration posture for Red Hat Enterprise Linux (RHEL) versions 5.0 - 5.5 running on x86 platforms. This guide was tested against RHEL 5.5 as installed by RHEL5_U5_i386_DVD. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract 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 released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

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

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:

Authors
Carole Fennelly
Jonathan Klein

Contributors and Reviewers
Samuel Apperson, *NASA*
Robert Aspinall, *NOAA*
Maria Bello, *Lunarline, Inc.*
Michael Boelen
Frank Breedijk, *Schuberg Philis*
Than Thi Cham
Mike Cross
Mike de Libero, *MDE Development, Inc.*
Ralph Durkee, *Durkee Consulting, Inc.*
William Eckler, *General Dynamics*
Wallace Epperson, *Virginia Information Technologies Agency*
Philippe Eveque, *Hewlett-Packard*
Howard Farmer, *Shell*
AJ Fasano
Victor Forno
Blake Frantz, *Center for Internet Security*
Jason Frisvold
Margaret Garland, *General Electric*
David Gendel
Andrew Gilmore
Vladimir Giszpenc
Alex Gockmann, *Algo Consulting*
Steve Grubb, *Red Hat*
Hilary Holz
Duncan Innes
Roger Kennedy, *VMC*
David Kennel, *U.S. Dept. of Energy*
Lucky Leavell, *U.S. Census Bureau*
Matt Marcotte, *Tenable Network Security, Inc.*
Rodney McKee
Nikhil Mittal
Jason Morgan, *CSC*
Tim Muniz
Alexei Nazario, *U.S. SEC*
Delvin Nelson, *General Dynamics*
Mike Nitulescu
Tom Pietschmann
Ely Pinto, *JRI America/SMBC*
Alexey Rogozhkin
Keith Schincke, *NASA*
Bruno Silva, *Algar Telecom*
Peter Sjoberg
Stephen Smoogen
Laura Stitely, *U.S. Dept. of Defense*
Andrew Stueve, *Neovera, Inc.*
Tran Thanh Chien
Robert Thomas, *U.S. Census Bureau*
Stephen Tihor, *Church Pension Group*
James Trigg, *U.S. Census Bureau*
Trevor Vaughan, *Onyx Point, Inc.*
Sven Vermeulen
Vytautas Vysniauskas, *Consumer Direct*
Kevin Walker, *NASA*
Don Williams
Joe Wulf, *G2-Inc*

CIS also extends special thanks to Joe Wulf, the author of the CIS Red Hat 5 Benchmark v1.0.0, along with the contributors to that benchmark: John Banghart, Michael Boelen, Giacomo G. Brussino, Keith Buck, Ron Colvin, Ralf Durkee, Dean Farrington, Blake Frantz, David Gendel, Andrew Gilmore, Steve Grubb, Richard Holbert, James B. Horwat, David A. Kennel, Joel Kirch, Rodney McKee, Robert Miller, Adam Montville, Keith D. Schincke, Dave Shackleford, Stephen John Smoogen, Nguyen Thi Xuan Thu, George Toft, John Traenky, Trevor Vaughan, and Zack Yang.

Additionally, CIS extends special thanks the Steve Grubb of Red Hat, the USGCB RHEL5 development team, and the authors of the NSA's *Guide to the Secure Configuration of Red Hat Enterprise Linux.*

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Interpret text exactly as presented, with the exception of the backslash character (\) which is used to indicate that the code continues to the next line (i.e. the carriage return is to be ignored). Text that is typed by the user will appear in **`bold-face courier`** while responses from the system will be displayed in `non-bold courier`.
`Monospace font`	Used for inline code, commands, or examples. Interpret text 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

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

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

Level-II Benchmark settings/actions

Level-II Benchmark recommendations 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

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernible in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Identification Table

The Identification Table identifies the areas to which an item applies. The identifiers for this table are as follows:

- Configuration Level. This identifier notes the configuration level associated with this benchmark item.
- OS Default. This identifier specifies if the recommended action or setting corresponds to the default configuration as set by the vendor.
- Reboot Required. This identifier specifies whether a system restart is needed in order for the recommended setting to take effect.
- Scorable Item. This identifier denotes whether the CIS Scoring can be used to determine if a system is compliant with an item.
- CCE Reference. This identifier specifies the Common Configuration Enumeration number for system configuration issues. If there is no CCE reference number associated with the item, it is designated as "N/A".

Assumptions and Recommendations

OS Platform

The recommendations and actions described in this document are based on a RHEL5 OS installation using Software Developers selection. Therefore, some actions may not apply to systems that have been installed with other installation clusters or fewer software packages.

Package Installation

It is assumed that all software packages have been installed using the appropriate `yum` or `rpm` utility.

System State

It is recommended that all actions be applied when the system is in a "quiet" state - one in which application and third party software and services are not active. Hardening services that may be used by running applications can have unpredictable results. If possible perform the actions when the system is running in "single user mode."

Test Actions

It is strongly recommended that all actions be first executed on a test or non-critical system before being performed on a production server. While the actions described in this document have been tested, there is no way to predict with certainty how they will affect a given environment.

Shell Environment

The actions listed in this document are written with the assumption that they will be executed by the *root* user running the `/sbin/sh` shell and without `noclobber` set.

Order of Operations

The actions listed in this document are written with the assumption that they will be executed in the order presented here. Some actions may need to be modified if the order is changed. Actions are written so that they may be copied directly from this document into a *root* shell window with a "cut-and-paste" operation.

Backup Key Files

Before performing the steps of this benchmark it is **strongly recommended** that administrators at least make backup copies their system configuration as critical files will be modified by recommended actions listed in this document. If this step is not performed, then the site may have no reasonable back-out strategy to reverse system modifications made as a result of this document's recommendations. It is preferable to perform a complete system backup to ensure that nothing is missed.

Benchmark Items

1. Install Updates, Patches and Additional Security Software

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. User's data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations. The directives in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

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

1.1.1 Create Separate Partition for `/tmp`

Configuration Level	Level-I
OS Default	No
Reboot Required	Yes
Scorable Item	Yes
CCE reference	CCE-14161-4

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

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

Remediation:

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

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

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

References:
See the guidance on the Logical Volume Manager (LVM) for more information on repartitioning filesystems:

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

1.1.2 Set `nodev` option for `/tmp` Partition

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14412-1

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`.

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

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

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

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

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

1.1.3 Set `nosuid` option for `/tmp` Partition

Configuration Level	Level-I
OS Default	N/A

Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14940-1

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

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

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

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

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

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

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

1.1.4 Set `noexec` option for `/tmp` Partition

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14412-1

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`.

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

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

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

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

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

1.1.5 Create Separate Partition for /var

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE reference	CCE-14777-7

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.

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

Audit:

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

References:
See the guidance on the Logical Volume Manager (LVM) for more information on repartitioning filesystems:

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

1.1.6 Bind Mount the /var/tmp directory to /tmp

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14584-7

Description:
The /var/tmp directory is normally a standalone directory in the /var file system. Binding /var/tmp to /tmp establishes an unbreakable link to /tmp that cannot be removed (even by the root user). It also allows /var/tmp to inherit the same mount options

that /tmp owns, allowing /var/tmp to be protected in the same /tmp is protected. It will also prevent /var from filling up with temporary files as the contents of /var/tmp will actually reside in the file system containing /tmp.

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

Remediation:

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

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

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

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

```
# grep -e "^/tmp" /etc/fstab | grep /var/tmp
/tmp /var/tmp none none 0 0
# mount | grep -e "^/tmp" | grep /var/tmp
/tmp on /var/tmp type none (rw,bind)
```

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

1.1.7 Create Separate Partition for /var/log

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE reference	CCE-14011-1

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

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

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

Audit:

```
# grep /var/log /etc/fstab
```

```
<volume>    /var/log    ext3  <options>
```

References:
See the guidance on the Logical Volume Manager (LVM) for more information on repartitioning filesystems:

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

1.1.8 Create Separate Partition for `/var/log/audit`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE reference	CCE-14171-3

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.

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

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

References:
See the guidance on the Logical Volume Manager (LVM) for more information on repartitioning filesystems:

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

1.1.9 Create Separate Partition for `/home`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE reference	CCE-14559-9

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`.

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

Audit:

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

References:
See the guidance on the Logical Volume Manager (LVM) for more information on repartitioning filesystems:

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

1.1.10 Add `nodev` Option to `/home`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-4249-9

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

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

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

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

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

Audit:

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

Note: There may be other options listed for this filesystem

1.1.11 Add `nodev` Option to Removable Media Partitions

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE reference	CCE-3522-0

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

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

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

Audit:

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

1.1.12 Add `noexec` Option to Removable Media Partitions

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE reference	CCE-4275-4

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

Rationale:

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

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

Audit:

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

1.1.13 Add `nosuid` Option to Removable Media Partitions

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE reference	CCE-4042-8

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

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

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

Audit:

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

1.1.14 Add `nodev` Option to `/dev/shm` Partition

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-15007-8

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

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

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

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

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

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

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

1.1.15 Add `nosuid` Option to `/dev/shm` Partition

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14306-5

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

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

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

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

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

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

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

1.1.16 Add `noexec` Option to `/dev/shm` Partition

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14927-8

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

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

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

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

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

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

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

1.1.17 Set Sticky Bit on All World-Writable Directories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-3399-3

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.

Remediation:

```
# find / -type d -perm -0002 2>/dev/null | chmod a+t
```

Audit:

```
# find / -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

1.1.18 Disable Mounting of `cramfs` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14089-7

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.

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

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

Audit:

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

1.1.19 Disable Mounting of `freevxfs` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14457-6

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

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

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

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

Audit:

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

1.1.20 Disable Mounting of `jffs2` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14853-6

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

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

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

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

Audit:

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

1.1.21 Disable Mounting of `hfs` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-15087-0

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

Rationale:

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

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

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

Audit:

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

1.1.22 Disable Mounting of `hfsplus` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14093-9

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

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

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

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

Audit:

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

1.1.23 Disable Mounting of `squashfs` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14118-4

Description:

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

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

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

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

Audit:

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

1.1.24 Disable Mounting of `udf` Filesystems

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	CCE-14871-8

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

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

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

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

Audit:

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

1.2 Use the Latest OS Release

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE reference	N/A

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

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

Remediation:
Obtain and install the latest update of the RHEL5 software.

Audit:
Run the following command to determine the current OS level:

```
# uname -r
```

or

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

1.3 Configure Software Updates

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

1.3.1 Configure Connection to the RHN RPM Repositories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE reference	N/A

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

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

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

```
# rhn register
```

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

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

```
# yum check-update
```

1.3.2 Verify Red Hat GPG Key is Installed

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14440-2

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

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

Remediation:

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

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

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

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

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

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

1.3.3 Verify that `gpgcheck` is Globally Activated

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-14914-6

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

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

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

```
gpgcheck=1
```

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

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

1.3.4 Disable the `rhnsd` Daemon

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE reference	CCE-3416-5

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

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

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

```
# chkconfig rhnsd off
```

Audit:

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

1.3.5 Disable `yum-updatesd`

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE reference	CCE-4218-4

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

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

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

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

Audit:

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

1.3.6 Obtain Software Package Updates with `yum`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

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

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

Remediation:

```
# yum update
```

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

```
# yum check-update
```

1.3.7 Verify Package Integrity Using RPM

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-14931-0

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

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

Remediation:

```
Address unexpected discrepancies identified in the audit step.
```

Audit:
Perform the following to verify integrity of installed packages.

```
# rpm -qVa | awk '$2 != "c" { print $0}'
If any output shows up, you may have an integrity issue with that package
```

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

1.4 Advanced Intrusion Detection Environment (AIDE)

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

1.4.1 Install AIDE

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14081-4

Description:
In some installations, AIDE is not installed automatically.

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

Remediation:

```
# yum install aide
<Output messages from Yum install>
aide.<hardware platform>      <package version>       installed
```

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

Audit:
Perform the following to determine if AIDE is installed.

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

1.4.2 Implement Periodic Execution of File Integrity

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
Implement periodic file checking, in compliance with site policy.

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

Remediation:
Execute the following command:

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

Add the following line to the crontab:

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

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

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

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

1.5 Configure SELinux

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

been designed for use with RHEL5 and are included with the system: `targeted`, `strict`, and `mls`. These are described as follows:

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

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

References:

1. NSA SELinux resources:
   a. http://www.nsa.gov/research/selinux
   b. http://www.nsa.gov/research/selinux/list.shtml

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

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

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

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

1.5.1 Enable SELinux in `/etc/grub.conf`

Configuration Level	Level-II
OS Default	No
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-3977-6

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

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

Remediation:

```
# ed /etc/grub.conf << END 2> /dev/null
g/selinux=0/d
g/enforcing=0/d
w
q
END
```

Audit:

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

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

1.5.2 Set the SELinux State

Configuration Level	Level-II
OS Default	No
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-3999-0

Description:

Set SELinux to enable when the system is booted.

Rationale:

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

Remediation:

```
# ed /etc/selinux/config << END
g/SELINUX=/d
g/SELINUXTYPE=/d
$a
SELINUX=enforcing
.
w
q
END
```

Audit:

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

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

# /usr/sbin/sestatus

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

1.5.3 Set the SELinux Policy

Configuration Level	Level-II
OS Default	No
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-3624-4

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.

Remediation:

```
# ed /etc/selinux/config << END
g/SELINUX=/d
g/SELINUXTYPE=/d
$a
SELINUXTYPE=targeted
.
w
q
END
```

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

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

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

# /usr/sbin/sestatus

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

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

1.5.4 Remove SETroubleshoot

Configuration Level	Level-II
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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.

Remediation:
```
# rpm –qa setroubleshoot
```

Audit:
Perform the following to determine if `setroubleshoot` is disabled.
```
# chkconfig --list setroubleshoot
setroubleshoot 0: off 1: off 2: off 3: off 4: off 5: off 6: off
```

1.5.5 Disable MCS Translation Service (`mcstrans`)

Configuration Level	Level-II
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3668-1

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

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

Remediation:
```
# chkconfig mctrans off
```

Audit:
Perform the following to determine if `mctrans` is disabled:
```
# chkconfig --list mctrans
mctrans 0: off 1: off 2: off 3: off 4: off 5: off 6: off
```

1.5.6 Check for Unconfined Daemons

Configuration Level	Level-II
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14991-4

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.

Remediation:
Investigate any unconfined daemons found during the audit action.

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

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

[no output produced]
```

1.6 Secure Boot Settings

1.6.1 Set User/Group Owner on `/etc/grub.conf`

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4144-2 CCE-4197-0

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

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

Remediation:

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

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

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

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

1.6.2 Set Permissions on /etc/grub.conf

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3923-0

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

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

Remediation:

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

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

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

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

1.6.3 Set Boot Loader Password

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3818-2

Description:
Setting the boot loader password will require that the person who is rebooting the must enter a password before being able to set command line boot parameters

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

Remediation:

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

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

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

1.6.4 Require Authentication for Single-User Mode

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4241-6

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

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

Remediation:
Add the following to `/etc/inittab`:

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

Audit:
Perform the following to determine

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

1.6.5 Disable Interactive Boot

Configuration Level	Level-I

OS Default	No
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-4245-7

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

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

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

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

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

1.7 Additional Process Hardening

1.7.1 Restrict Core Dumps

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	

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.

Remediation:

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

```
*     hard core 0
```

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

```
fs.suid.dumpable = 0
```

Audit:
Perform the following to determine if core dumps are restricted.

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

1.7.2 Configure ExecShield

Configuration Level	Level-I
OS Default	Yes
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-4168-1

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

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

Remediation:
Add the following line to the /etc/sysctl.conf file.

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

Audit:
Perform the following to determine if ExecShield is enabled.

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

1.7.3 Enable Randomized Virtual Memory Region Placement

Configuration Level	Level-I
OS Default	Yes
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-4146-7

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

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

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

```
kernel.randomize_va_space = 1
```

Audit:
Perform the following to determine if virtual memory is randomized.

```
# sysctl kernel.randomize_va_space
kernel.randomize_va_space = 1
```

1.7.4 Enable XD/NX Support on 32-bit x86 Systems

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	

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

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

Remediation:

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

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

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

1.7.5 Disable Prelink

Configuration Level	Level-I
OS Default	No

Reboot Required	No
Scorable Item	Yes
CCE Reference	

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

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

Remediation:

```
# ed /etc/sysconfig/prelink << END
/PRELINKING/
s/=.*/s//=no/
w
q
```

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

Audit:
Perform the following to determine or prelinking is disabled.

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

2. OS Services

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

2.1 Remove Legacy Services

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

Note: The audit items in the section check to see if the packages are listed in the `yum` database and installed using `rpm`. It could be argued that someone may have installed them

separately. However, this is also true for any other type of rogue software. It is beyond the scope of this benchmark to address software that is installed using non-standard methods and installation directories.

2.1.1 Remove `telnet-server`

Configuration Level	Level-I
OS Default	disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3390-2 CCE-4330-7

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

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

Remediation:

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

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

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

2.1.2 Remove `telnet` Clients

Configuration Level	Level-I
OS Default	disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3390-2 CCE-4330-7

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

Rationale:
The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an authorized user to steal credentials. The `ssh` package

provides an encrypted session and stronger security and is included in most Red Hat Linux distributions.

Remediation:

```
# yum erase telnet
```

Audit:

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

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

2.1.3 Remove `rsh-server`

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4308-3

Description:

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

Rationale:

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

Remediation:

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

Audit:

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

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

2.1.4 Remove `rsh`

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4141-8 (rsh) CCE- 3974-3 (rcp) CCE- 3537-8 (rlogin)

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`.

Remediation:
```
# yum erase rsh
```

Audit:
Perform the following to determine if `rsh` is installed on the system.
```
# yum list rsh
rsh.<hard platform>     <release>   <anything except installed>
```

2.1.5 Remove NIS Client

Configuration Level	Level-I
OS Default	disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3705-1 (disable) CCE-4348-9 (uninstall)

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.

Remediation:
```
# yum erase ypbind
```

Audit:
Perform the following to determine if `ypbind` is installed on the system.
```
# yum list ypbind
ypbind.<hard platform>  <release>   <anything except installed>
```

2.1.6 Remove NIS Server

Configuration Level	Level-I
OS Default	disabled

Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3705-1 (disable) CCE-4348-9 (uninstall)

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

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

Remediation:
```
# yum erase ypserv
```

Audit:
Perform the following to determine if `ypserv` is installed on the system.
```
# yum list ypserv
ypserv.<hard platform>  <release>   <anything except installed>
```

2.1.7 Remove `tftp`

Configuration Level	Level-I
OS Default	disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4273-9 (disable) CCE-3916-4 (uninstall)

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

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

Remediation:
```
# yum erase tftp
```

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

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

2.1.8 Remove `tftp-server`

Configuration Level	Level-I
OS Default	disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4273-9 (disable) CCE-3916-4 (uninstall)

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

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

Remediation:
```
# yum erase tftp-server
```

Audit:
Perform the following to determine if `tftp-server` is installed on the system.
```
# yum list tftp-server
tftp-server.<hard platform>   <release>   <anything except installed>
```

2.1.9 Remove `talk`

Configuration Level	Level-I
OS Default	Enabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

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

Remediation:
```
# yum erase talk
```

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

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

2.1.10 *Remove `talk-server`*

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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.

Remediation:

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

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

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

2.1.11 Remove `xinetd`

Configuration Level	Level-II
OS Default	Not installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4234-1 CCE-4164-0

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

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

Remediation:

```
# yum erase xinetd
```

Audit:

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

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

2.1.12 Disable `chargen-dgram`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:

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

Rationale:

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

Remediation:

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

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

Audit:

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

2.1.13 Disable `chargen-stream`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:

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

Rationale:

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

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

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

Audit:

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

2.1.14 Disable `daytime-dgram`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
`daytime-dram` is a network service that respondes with the server's current date and time. This service is intended for debugging and testing puposes. It is recommended that this service be disabled.

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

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

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

Audit:

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

2.1.15 Disable `daytime-stream`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

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

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

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

Audit:

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

2.1.16 Disable `echo-dgram`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

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

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

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

Audit:

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

2.1.17 Disable `echo-stream`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

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

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

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

Audit:

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

2.1.18 Disable `tcpmux-server`

Configuration Level	Level-I
OS Default	Disabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

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

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

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

Audit:

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

3. Special Purpose Services

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

3.1 Set Daemon `umask`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:

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

Rationale:

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

Remediation:

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

```
umask 027
```

Audit:

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

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

3.2 Remove X Windows

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

Description:

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

Rationale:

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

Remediation:

```
# ed /etc/inittab
/^id:/
s/:5:/:3:/
# yum groupremove "X Window System"
```

Audit:

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

```
# grep "^id:" /etc/inittab
id:3:initdefault
# yum grouplist "X Window System"
loaded plugins: rhnplugin, security
Seeting up Group Process
Available Groups:
  X Window System
Done
```

3.3 Disable Avahi Server

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

Description:

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

Rationale:

Since servers are not normally used for printing, this service is not needed unless dependencies require it. If this is the case, disable the service to reduce the potential attack surface. If for some reason the service is required on the server, follow the recommendations in sub-sections 3.2.1 - 3.2.5 to secure it.

Remediation:

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

In addition, edit the `/etc/sysconfig/network` file and remove zeroconf.

Audit:

Perform the following to determine if Avahi is disabled.

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

3.3.1 Service Only via Required Protocol

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

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

```
#if only using IPv4, disable IPv6 with this line:
use-ipv6=no

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

use-ipv4=no
```

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

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

3.3.2 Check Responses TTL Field

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

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

Rationale:

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

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

```
check-response-ttl=yes
# grep "^check-response-ttl=yes" /etc/avahi/avahi-daemon.conf
# if [ $? -ne 0 ]
# then
# ed  /etc/avahi/avahi-daemon.conf
g/ check-response-ttl /d
/^\[server]/
a
check-response-ttl=yes
.
w
q
#fi
```

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

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

3.3.3 Prevent Other Programs from Using Avahi's Port

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

Remediation:

```
#!/bin/bash
grep "^disallow-other-stacks=yes" /etc/avahi/avahi-daemon.conf
if [ $? -ne 0 ]
then
# ed  /etc/avahi/avahi-daemon.conf
g/disallow-other-stacks/d
/^\[server]/
a
disallow-other-stacks=yes
```

```
.
w
q
fi
```

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

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

3.3.4 Disable Publishing

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

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

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

Audit:
Perform the following to determine if publishing is disabled.

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

3.3.5 Restrict Published Information (if publishing is required)

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

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

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

Audit:
Perform the following to determine if publishing is restricted:

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

3.4 Disable Print Server - CUPS

Configuration Level	Level-I
OS Default	Enabled
Reboot Required	No
Scorable Item	No

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.

Remediation:

```
# chkconfig cups off
```

Audit:
Perform the following to determine if CUPS is disabled.

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

References:

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

3.5 Remove DHCP Server

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	No

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

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

Remediation:

```
# yum erase dhcp
```

Audit:
Perform the following to determine if DHCP is disabled.

```
# yum list dhcp
```

```
dhcp.<hardware platform>      <release>   <anything but installed>
```

References:

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

3.6 Configure Network Time Protocol (NTP)

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

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

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

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

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

Also, make sure /etc.ntp.conf has an NTP server specified:

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

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

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

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

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

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

References:

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

3.7 Remove LDAP

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No

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

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

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

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

Audit:
Perform the following to determine if LDAP is running.

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

References:

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

3.8 Disable NFS and RPC

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

Remediation:

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

Audit:
Perform the following to determine if NFS is disabled.

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

3.9 Remove DNS Server

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

Remediation:

```
# yum erase bind
```

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

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

3.10 Remove FTP Server

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

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.

Remediation:

```
# yum erase vsftpd
```

Audit:
Perform the following to determine if FTP is disabled.

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

3.11 Remove HTTP Server

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

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

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

Remediation:

```
# yum erase httpd
```

Audit:

Perform the following to determine if apache is disabled.

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

3.12 Remove Dovecot (IMAP and POP3 services)

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

Description:

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

Rationale:

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

Remediation:

```
# yum erase dovecot
```

Audit:

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

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

References:

1. http://www.dovecot.org

3.13 Remove Samba

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	No

Description:

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

Rationale:

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

Remediation:

```
# yum erase samba
```

Audit:

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

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

3.14 Remove HTTP Proxy Server

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No

Description:

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

Rationale:

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

Remediation:

```
# yum erase squid
```

Audit:

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

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

3.15 Remove SNMP Server

Configuration Level	Level-I
OS Default	Not Installed
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:

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

Rationale:

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

Remediation:

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

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

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

3.16 Configure Mail Transfer Agent for Local-Only Mode

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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

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

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

Remediation:
Edit `/etc/mail/sendmail.cf` and add the following line to the Options section. If the line already exists, change it to look like the line below.

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

# Execute the following command to restart sendmail
# service sendmail restart
```

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

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

4. Network Configuration and Firewalls

This section provides guidance for secure network and firewall configuration.

4.1 Modify Network Parameters (Host Only)

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

4.1.1 Disable IP Forwarding

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3561-8

Description:

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

Rationale:

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

Remediation:

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

Audit:

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

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

4.1.2 Disable Send Packet Redirects

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4151-7, CCE-4155-8

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.

Remediation:

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

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

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

4.2 Modify Network Parameters (Host and Router)

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

4.2.1 Disable Source Routed Packet Acceptance

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4236-6 CCE-4091-5

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

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

private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Remediation:

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

Audit:

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

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

4.2.2 Disable ICMP Redirect Acceptance

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4217-6, CCE-4186-3

Description:

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

Rationale:

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

Remediation:

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

Audit:

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

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

4.2.3 Disable Secure ICMP Redirect Acceptance

Configuration Level	Level-II
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3472-8, CCE-3339-9

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.

Remediation:

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

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

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

4.2.4 Log Suspicious Packets

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4320-8

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

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

Remediation:

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

Audit:
Perform the following to determine if suspicious packets are logged.

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

4.2.5 Enable Ignore Broadcast Requests

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3644-2

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.

Remediation:

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

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

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

4.2.6 Enable Bad Error Message Protection

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4133-5

Description:

Setting `icmp_ignore_bogus_error_responses` to 1 prevents the 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.

Remediation:

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

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

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

4.2.7 Enable RFC-recommended Source Route Validation

Configuration Level	Level-II
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4080-8, CCE-3840-6

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

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

Remediation:

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

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

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

4.2.8 Enable TCP SYN Cookies

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4265-5

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

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

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

Audit:
Perform the following to determine if TCP SYN Cookies is enabled.
```
# /sbin/sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
```

4.3 Wireless Networking

4.3.1 Deactivate Wireless Interfaces

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No

Scorable Item	No
CCE Reference	CCE-4276-2

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

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

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

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

Audit:
Perform the following to determine if wireless interfaces are active.

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

4.4 Disable IPv6

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

4.4.1 Disable IPv6

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE Reference	CCE-3562-6

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

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

Remediation:

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

Audit:
Perform the following to determine if IPv6 is enabled

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

4.4.2 Configure IPv6

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

4.4.2.1 Disable IPv6 Router Advertisements

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4269-7

Description:
This setting disables the systems ability to accept router advertisements

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

Remediation:

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

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

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

4.4.2.2 Disable IPv6 Redirect Acceptance

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4313-3

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

Rationale:

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

Remediation:
Execute the following commands to prevent the system from accepting ICMP redirects.

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

Audit:
Perform the following to determine if IPv6 redirects are disabled.

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

4.5 Install TCP Wrappers

Configuration Level	Level-I
OS Default	Not installed
Reboot Required	No
Scorable Item	No
CCE Reference	

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

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

Remediation:

```
# yum install tcp_wrappers
```

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.

Audit:
Perform the following to determine if TCP Wrappers is enabled.

```
# yum list tcp-wrappers
tcp_wrappers.<hardware platform>    <release>   <installed>
```

4.5.1 Create /etc/hosts.allow

Configuration Level	Level-I
OS Default	Installed
Reboot Required	No
Scorable Item	No
CCE Reference	

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

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

Remediation:
Create `/etc/hosts.allow`:

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

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

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

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

4.5.2 Verify Permissions on /etc/hosts.allow

Configuration Level	Level-I
OS Default	Installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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

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

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

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

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

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

4.5.3 Create /etc/hosts.deny

Configuration Level	Level-I
OS Default	Installed
Reboot Required	No
Scorable Item	No
CCE Reference	

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

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

Remediation:
Create `/etc/hosts.deny`:

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

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

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

4.5.4 Verify Permissions on /etc/hosts.deny

Configuration Level	Level-I
OS Default	Installed
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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

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

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

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

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

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

4.6 Enable IPtables

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4189-7

Description:
IPtables is an application that allows a system administrator to configure the IPv4 tables, chains and rules provided by the Linux kernel firewall.

Rationale:
IPtables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv4 addresses and ports.

Remediation:

```
# service iptables restart
# chkconfig iptables on
```

Audit:
Perform the following to determine if IPtables is enabled.

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

4.7 Enable IP6tables

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4167-3

Description:
IP6tables is an application that allows a system administrator to configure the IPv6 tables, chains and rules provided by the Linux kernel firewall.

Rationale:
IP6tables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv6 addresses and ports.

Note:
IP6Tables should only be enabled if IPv6 has been enabled on your system.

Remediation:

```
# service ip6tables restart
# chkconfig ip6tables on
```

Audit:
Perform the following to determine if IP6Tables is enabled:

```
# chkconfig --list ip6tables
ip6tables    0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

4.8 Uncommon Network Protocols

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

4.8.1 Disable DCCP

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE Reference	CCE-14268-7

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.

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

Audit:
Perform the following to determine if DCCP is disabled.
```
# grep "install dccp /bin/true" /etc/modprobe.conf
install dccp /bin/true
```

4.8.2 Disable SCTP

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE Reference	CCE-14132-5

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.

Remediation:
```
# echo "install sctp /bin/true" >> /etc/modprobe.conf
```

Audit:
Perform the following to determine if SCTP is disabled.
```
# grep "install sctp /bin/true" /etc/modprobe.conf
install sctp /bin/true
```

4.8.3 Disable RDS

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE Reference	CCE-14027-7

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.

Remediation:
```
# echo "install rds /bin/true" >> /etc/modprobe.conf
```

Audit:
Perform the following to determine if RDS is disabled.
```
# grep "install rds /bin/true" /etc/modprobe.conf
install rds /bin/true
```

4.8.4 Disable TIPC

Configuration Level	Level-I
OS Default	N/A
Reboot Required	Yes
Scorable Item	No
CCE Reference	CCE-14911-2

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.

Remediation:
```
# echo "install tipc /bin/true" >> /etc/modprobe.conf
```

Audit:
Perform the following to determine if TIPC is disabled.
```
# grep "install tipc /bin/true" /etc/modprobe.conf
install tipc /bin/true
```

5. Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included with RHEL5.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing

summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the `ntpd(8)` manual page for more information on configuring NTP.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log. Although it is recommended that `rsyslog` be used for logging, guidance for configuring `syslog` is provided in for sites where `rsyslog` does not meet the requirements.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

5.1 Configure Syslog

Description:
The `syslogd` logging daemon is the default for RHEL and is used by many applications to log activity in accordance with settings in the `/etc/syslog.conf` file. There are some limitations to syslog, such as lack of authentication for client or servers, lack of encryption, or reliable network transportation.

Rationale:

Despite the limitations of `syslog`, it is better to configure it properly than to have no or limited logging. If possible, it is recommended that `rsyslog` be used instead.

5.1.1 *Configure* `/etc/syslog.conf`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
The `/etc/syslog.conf` file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:
A great deal of important security-related information is sent via `syslog` (e.g., successful and failed `su` attempts, failed login attempts, `root` login attempts, etc.).

Remediation:
Edit the following lines in the `/etc/syslog.conf` file as appropriate for your environment:

```
auth,user.*                                             /var/log/messages
kern.*                                                  /var/log/kern.log
daemon.*                                                /var/log/daemon.log
syslog.*                                                /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.*
      /var/log/unused.log

# Execute the following command to restart syslogd
# pkill -HUP syslogd
```

Audit:
Review the contents of the `/etc/syslog.conf` file to ensure appropriate logging is set. In addition, perform the following command and ensure that the log files are logging information:

```
# ls -l /var/log
```

References:
See the `syslog(2)` man page for more information.

5.1.2 *Create and Set Permissions on `syslog` Log Files*

Configuration Level	Level-I
OS Default	N/A

Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
A log file must already exist for `syslog` to be able to write to it.

Rationale:
It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `syslog` data is archived and protected.

Remediation:
For sites that have **not** implemented a secure admin group:
For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands:

```
# touch <LOGFILE>
# chown root:root <LOGFILE>
# chmod og-rwx <LOGFILE>
```

For sites that **have** implemented a secure admin group:
For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands (where *<securegrp>* is the name of the security group):

```
# touch <LOGFILE>
# chown root:<securegrp> <LOGFILE>
# chmod g-wx,o-rwx <LOGFILE>
```

Audit:
For each `LOGFILE` listed in the `/etc/syslog.conf` file, perform the following commands and verify that the `owner:group` is `root:root` and the permissions are `0600` (for sites that do not use a security group) and `root:<securegrp>` with permissions of `0640` (for sites that use a secure group):

```
# ls -l <LOGFILE>
```

References:
See the `syslog.conf(5)` man page for more information.

5.1.3 Configure `syslog` to Send Logs to a Remote Log Host

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:

The `syslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Rationale:
Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Remediation:
Edit the `/etc/syslog.conf` file and add the following line (where logfile.example.com is the name of your central log host).

```
*.*                                             @loghost.example.com
# Execute the following command to restart syslogd
# pkill -HUP syslogd
```

Audit:
Review the `/etc/syslog.conf` file and verify that logs are sent to a central host (where `logfile.example.com` is the name of your central log host).

```
# grep "^*.*[^I][^I]*@" /etc/syslog.conf
*.*                                             @loghost.example.com
```

References:
See the `syslog.conf(5)` man page for more information.

5.1.4 Accept Remote `syslog` Messages Only on Designated Log Hosts

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
By default, `syslog` on RHEL5 does not listen for log messages coming in from remote systems. The `-r` flag can be used to enable this ability and the `-s` option can be used to strip the domain name from incoming messages to reduce redundant information in log files.

Rationale:
The guidance in the section ensures that remote log hosts are configured to only accept syslog data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `syslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

NOTE:
Since syslog uses UDP to send messages to a remote host, there is no guarantee that the remote host will actually receive all the data. Log messages may be lost, especially on busy sites.

Remediation:
For each host designated as a log host, edit the `/etc/sysconfig/syslog` file and add the following line:

```
SYSLOGD_OPTIONS="-m 0 -r -s <LOGHOST> "

# Execute the following command to restart syslogd
# pkill -HUP syslogd
```

For hosts that are **not** designated log hosts, edit the `/etc/sysconfig/syslog` file and add the following line:

```
SYSLOGD_OPTIONS="-m 0"

# Execute the following command to restart syslogd
# pkill -HUP syslogd
```

Audit:

```
# grep SYSLOGD_OPTIONS /etc/sysconfig/syslog
-m 0 -r -s example.com (if designated as a log host)
-m 0 (if not designated as a log host)
```

References:
See the `syslog(8)` man page for more information.

5.2 Configure rsyslog

The rsyslog software is recommended as a replacement for the default syslogd daemon and provides improvements over syslogd, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

5.2.1 Install the `rsyslog` package

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:

The rsyslog package is a third party package that provides many enhancements to syslog, such as multi-threading, TCP communication, message filtering and data base support. As of RHEL 5.2, rsyslog is available as part of the core distribution.

Rationale:
The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Remediation:

```
# yum install rsyslog
```

Audit:
Perform the following command to verify that rsyslog is installed.

```
# yum list rsyslog
rsyslog.<hardware platform>   <release>   <installed>
```

References:
See http://www.rsyslog.com/docs for information on rsyslog.

5.2.2 Activate the rsyslog Service

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
The chkconfig command can be used to ensure that the syslog service is turned off and that the rsyslog service is turned on.

Rationale:
It is important to ensure that syslog is turned off so that it does not interfere with the rsyslog service.

Remediation:

```
# chkconfig syslog off
# chkconfig rsyslog on
```

Audit:

```
# chkconfig --list syslog
syslog      0:off 1:off 2:off 3:off 4:off 5:off 6:off
# chkconfig --list rsyslog
rsyslog     0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

5.2.3 Configure /etc/rsyslog.conf

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
The /etc/rsyslog.conf file specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:
A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Remediation:
Edit the following lines in the /etc/rsyslog.conf file as appropriate for your environment:

```
auth,user.*                                          /var/log/messages
kern.*                                               /var/log/kern.log
daemon.*                                             /var/log/daemon.log
syslog.*                                             /var/log/syslog
lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6.*
/var/log/unused.log

# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

Audit:
Review the contents of the /etc/rsyslog.conf file to ensure appropriate logging is set. In addition, perform the following command and ensure that the log files are logging information:

```
# ls -l /var/log/
```

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

5.2.4 Create and Set Permissions on rsyslog Log Files

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:

A log file must already exist for `rsyslog` to be able to write to it.

Rationale:
It is important to ensure that log files exist and have the correct permissions to ensure that sensitive `rsyslog` data is archived and protected.

Remediation:
For sites that have **not** implemented a secure admin group:

Create the `/var/log/` directory and for each *<logfile>* listed in the `/etc/rsyslog.conf` file, perform the following commands:

```
# touch <logfile>
# chown root:root <logfile>
# chmod og-rwx <logfile>
```

For sites that **have** implemented a secure admin group:

Create the `/var/log/` directory and for each *<logfile>* listed in the `/etc/rsyslog.conf` file, perform the following commands (where *<securegrp>* is the name of the security group):

```
# touch <logfile>
# chown root:<securegrp> <logfile>
# chmod g-wx,o-rwx <logfile>
```

Audit:
For each *<logfile>* listed in the `/etc/rsyslog.conf` file, perform the following command and verify that the *<owner>*:*<group>* is `root:root` and the permissions are `0600` (for sites that have not implemented a secure group) and `root:securegrp` with permissions of `0640` (for sites that have implemented a secure group):

```
# ls -l <logfile>
```

References:
See the `rsyslog.conf(5)` man page for more information.

5.2.5 Configure `rsyslog` to Send Logs to a Remote Log Host

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

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

Remediation:
Edit the /etc/rsyslog.conf file and add the following line (where *logfile.example.com* is the name of your central log host).

```
*.*                                             @@loghost.example.com

# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

Note:
The double "at" sign (@@) directs rsyslog to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

Audit:
Review the /etc/rsyslog.conf file and verify that logs are sent to a central host (where *logfile.example.com* is the name of your central log host).

```
# grep "^*.*[^I][^I]*@" /etc/rsyslog.conf
*.*                                             @@loghost.example.com
```

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

5.2.6 Accept Remote rsyslog Messages Only on Designated Log Hosts

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	

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.

Remediation:
For hosts that are designated as log hosts, edit the `/etc/rsyslog.conf` file and add or modify the following lines:

```
$ModLoad imtcp.so
$InputTCPServerRun 514

# Execute the following command to restart rsyslogd
# pkill -HUP rsyslogd
```

Audit:

```
# grep '$ModLoad' /etc/rsyslog.conf
$ModLoad imtcp.so
# grep '$InputTCPServerRun' /etc/rsyslog.conf
$InputTCPServerRun 514
```

References:
See the `rsyslog(8)` man page for more information.

5.3 Configure System Accounting (`auditd`)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, auditd will audit SELinux AVC denials, system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

Note:
For 64 bit systems that have arch as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems. For 32 bit systems, only one rule is needed.

5.3.1 Enable `auditd` Service

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4292-9

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.

Remediation:
```
# chkconfig auditd on
```

Audit:
Perform the following to determine if `auditd` is enabled.
```
# chkconfig --list auditd
auditd:     0: off  1: off  2: on  3: on  4: on   5: on   6: off
```

5.3.2 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, `auditd` will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

5.3.2.1 Configure Audit Log Storage Size

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

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.

Remediation:
```
# ed /etc/audit/auditd.conf << END
/max_log_file/
s/=.*/s//= MB/
w
q
END
```

Note: `MB` is the number of MegaBytes the file can be.

Audit:
Perform the following to determine the maximum size of the audit log files.

```
# grep max_log_file /etc/audit/auditd.conf
max_log_file = MB
```

5.3.2.2 Disable System on Audit Log Full

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

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.

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

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

Audit:
Perform the following to determine if `auditd` is configured to notify the administrator and halt the system when audit logs are full.

```
# grep space_left_action /etc/audit/auditd.conf
space_left_action = email
# grep action_mail_acct /etc/audit/auditd.conf
action_mail_acct = email
# grep admin_space_left_action /etc/audit/auditd.conf
admin_space_left_action = email
```

5.3.2.3 Keep All Auditing Information

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:

Normally, `auditd` will hold 4 logs of maximum log file size before deleting older log files.

Rationale:
In hight security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Remediation:
Add the following line to the `/etc/audit/auditd.conf` file.

```
max_log_file_action = keep_logs
```

Audit:
Perform the following to determine if audit logs are retained.

```
# grep max_log_file_action /etc/audit/auditd.conf
max_log_file_action = keep_logs
```

5.3.3 Enable Auditing for Processes That Start Prior to `auditd`

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-15026-8

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.

Remediation:

```
# ed /etc/grub.conf << END
g/audit=1/s///g
g/kernel/s/$/ audit=1/
w
q
END
```

Audit:
Perform the following to determine if `/etc/grub.conf` is configured to log processes that start prior to `auditd`.

```
# grep "audit=1" /etc/grub.conf
Make sure each line that starts with kernel has the audit=1 parameter set.
```

5.3.4 Record Events That Modify Date and Time Information

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14051-7

Description:
Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the `adjtimex` (tune kernel clock), `settimeofday` (Set time, using timeval and timezone structures) `stime` (using seconds since 1/1/1970) or `clock_settime` (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the `/var/log/audit.log` file upon exit, tagging the records with the identifier "time-change"

Rationale:
Unexpected changes in system data and/or time could be a sign of malicious activity on the system.

Remediation:

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

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

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

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

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

Audit:
Perform the following to determine if events where the system date and/or time has been modified are captured.

On a 64 bit system, perform the following command and ensure the output is as shown.

```
# grep time_change /etc/audit/audit.rules
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

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

On a 32 bit system, perform the following command and ensure the output is as shown.

```
# grep time_change /etc/audit/audit.rules
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-
change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

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

5.3.5 Record Events That Modify User/Group Information

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14829-6

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.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
```

```
-w /etc/security/opasswd -p wa -k identity

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

Audit:
Perform the following to determine if events that modify user/group information are recorded.

```
# grep identity /etc/audit/audit.rules
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

5.3.6 Record Events That Modify the System's Network Environment

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14816-3

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."

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

```
-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale

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

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale

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

Audit:
On a 64 bit system, perform the following command and ensure the output is as shown to determine if events that modify the system's environment are recorded.

```
# grep system-locale /etc/audit/audit.rules
-a exit,always -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if events that modify the system's environment are recorded.

```
# grep system-locale /etc/audit/audit.rules
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
```

5.3.7 Record Events That Modify the System's Mandatory Access Controls

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14821-3

Description:
Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the `/etc/selinux` directory.

Rationale:
Changes to files in this directory could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
Add the following lines to /etc/audit/audit.rules

-w /etc/selinux/ -p wa -k MAC-policy

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

Audit:
Perform the following to determine if events that modify the system's mandatory access ontrols are recorded

```
# grep MAC_policy /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
```

5.3.8 Collect Login and Logout Events

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14904-7

Description:
Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file `/var/log/faillog` tracks failed events from login. The file `/var/log/lastlog` maintain records of the last time a user successfully logged in. The file `/var/log/tallylog` maintains a tally of failed logins associated with programs that use pam for authentication and have the pam_tally2.so module configured. The file `/var/log/btmp` keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`. All audit records will be tagged with the identifier "logins."

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p -wa -k logins
-w /var/log/btmp -p wa -k session

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

Audit:
Perform the following to determine if login and logout events are recorded.

```
# grep logins  /etc/audit/audit.rules
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/log/tallylog -p -wa -k logins
-w /var/log/btmp -p wa -k session
```

5.3.9 Collect Session Initiation Information

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14679-5

Description:
Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file `/var/run/utmp` file tracks all currently logged in users. The `/var/log/wtmp` file tracks logins, logouts, shutdown and reboot events. All audit records will be tagged with the identifier "session."

Rationale:
Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session

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

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

Audit:
Perform the following to determine if session initiation information is collected.

```
# grep session  /etc/audit/audit.rules
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
```

5.3.10 Collect Discretionary Access Control Permission Modification Events

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14058-2

Description:
Monitor changes to file permissions, attributes, ownership and group. The parameters inn this section track changes for system calls that affect file permissions and attributes. The `chmod`, `fchmod` and `fchmodat` system calls affect the permissions associated with a file. The `chown`, `fchown`, `fchownat` and `lchown` system calls affect owner and group attributes on a file. The `setxattr`, `lsetxattr`, `fsetxattr` (set extended file attributes) and `removexattr`, `lremovexattr`, `fremovexattr` (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system userids (auid >= 500) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier "perm_mod."

Rationale:
Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

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

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
```

```
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

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

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

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

Audit:

For 64 bit systems, perform the following command and ensure the output is as shown to determine if permission modifications are being recorded.

```
# grep perm_mod  /etc/audit/audit.rules
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if permission modifications are being recorded.

```
# grep perm_mod  /etc/audit/audit.rules
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=500 \
-F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S \
```

```
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod
```

5.3.11 Collect Unsuccessful Unauthorized Access Attempts to Files

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14917-9

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.

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

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

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

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

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

Audit:
On 64 bit systems, perform the following command and ensure the output is as shown to determine if there are unsuccessful attempts to access files.

```
# grep access  /etc/audit/audit.rules
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

On 32 bit systems, perform the following command and ensure the output is as shown to determine if there are unsuccessful attempts to access files.

```
# grep access  /etc/audit/audit.rules
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate \
-F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access
```

5.3.12 Collect Use of Privileged Commands

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14296-8

Description:
Monitor privileged programs (thos 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.

Remediation:
To remediate this issue, the system administrator will have to execute a `find` command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows:

`-F path=" $1 "` - will populate each file name found through the find command and processed by awk.
`-F perm=x` - will write an audit record if the file is executed.
`-F auid>=500` - will write a record if the user executing the command is not a privileged user.
`-F auid!= 4294967295` - will ignore Daemon events

All audit records will be tagged with the identifier "privileged."

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

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

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

5.3.13 Collect Successful File System Mounts

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4024-6

Description:
Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user

Rationale:
It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Note:
This tracks successful and unsuccessful `mount` commands. File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS)

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

```
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts

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

For 32 bit systems, add the following lines to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts

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

Audit:
For 64 bit systems perform the following command and ensure the output is as shown to determine if filesystem mounts are recorded.

```
# grep mounts  /etc/audit/audit.rules
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

For 32 bit systems perform the following command and ensure the output is as shown to determine if filesystem mounts are recorded.

```
# grep mounts  /etc/audit/audit.rules
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k
mounts
```

5.3.14 Collect File Deletion Events by User

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14820-5

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.

Remediation:
At a minimum, configure the audit system to collect file deletion events for all users and root.
For 64 bit systems, add the following to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
-F auid!=4294967295 -k delete

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

For 32 bit systems, add the following to the `/etc/audit/audit.rules` file.

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
-F auid!=4294967295 -k delete

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

Audit:
For 64 bit systems, perform the following command and ensure the output is as shown to determine if file deletion events by user are recorded.

```
# grep deleted  /etc/audit/audit.rules
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
-F auid!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
-F auid!=4294967295 -k delete
```

For 32 bit systems, perform the following command and ensure the output is as shown to determine if file deletion events by user are recorded.

```
# grep deleted  /etc/audit/audit.rules
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 \
```

```
-F auid!=4294967295 -k delete
```

5.3.15 Collect Changes to System Administration Scope (sudoers)

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14824-7

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.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /etc/sudoers -p wa -k scope

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

Audit:
Perform the following to determine if changes to `/etc/sudoers` are recorded.

```
# grep scope  /etc/audit/audit.rules
-w /etc/sudoers -p wa -k scope
```

5.3.16 Collect System Administrator Actions (sudolog)

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14824-7

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.

Remediation:
Add the following lines to the /etc/audit/audit.rules file.

```
-w /var/log/sudo.log -p wa -k actions

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

Note: The system must be configured with su disabled (See Item 7.6 Restrict Access to the su Command) to force all command execution through sudo. This will not be effective on the console, as administrators can log in as root.

Audit:
Perform the following to determine if administrator activity is recorded.

```
# grep actions  /etc/audit/audit.rules
-w /var/log/sudo.log -p wa -k actions
```

5.3.17 Collect Kernel Module Loading and Unloading

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14688-6

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.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -S init_module -S delete_module -k modules
```

Audit:
Perform the following to determine if kernel module loading and unloading is recorded.

```
# grep modules  /etc/audit/audit.rules
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -S init_module -S delete_module -k modules
```

5.3.18 Make the Audit Configuration Immutable

Configuration Level	Level-II
OS Default	N/A
Reboot Required	Yes
Scorable Item	Yes
CCE Reference	CCE-14692-8

Description:
Set system audit so that audit rules cannot be modified with `auditctl`. Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

Rationale:
In immutable mode, unauthorized users cannot execute changes to the audit system to potential hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Remediation:
Add the following lines to the `/etc/audit/audit.rules` file.

```
-e 2
```

Note: This must be the last entry in the `/etc/audit/audit.rules` file

Audit:
Perform the following to determine if the audit configuration is immutable.

```
# grep "^-e 2" /etc/audit/audit.rules
-e 2
```

5.4 Configure `logrotate`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4182-2

Description:
The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageable large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`. These files are rotated on a weekly basis via a cron job and the last 4 weeks are kept.

Rationale:
By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Remediation:

```
# ed /etc/logrotate.d/syslog << END
1d
0a
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler
/var/log/boot.log /var/log/cron {
.
w
q
END
```

Audit:
Perform the following to determine if the appropriate system logs are rotated.

```
# grep '{' /var/logrotate.d/syslog
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler
/var/log/boot.log /var/log/cron {
```

6. System Access, Authentication and Authorization

6.1 Configure cron and anacron

6.1.1 Enable anacron Daemon

Configuration Level	Level-II
OS Default	Enabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The anacron daemon is used on systems that are not up 24x7. The anacron daemon will execute jobs that would have normally been run had the system not been down.

Rationale:
Cron jobs may include critical security or administrative functions that need to run on a regular basis. Use this daemon on machines that are not up 24x7, or if there are jobs that need to be executed after the system has been brought back up after a maintenance window.

Remediation:

```
# chkconfig anacron on
```

Note: NSA Guidance recommends disabling anacron for systems that are intended to be up 24X7, with the rationale that unnecessary software should be disabled to reduce risk. However, even systems that are designed to be up at all times can experience downtime that could prevent important system maintenance jobs from running. Review the requirements for your site to determine your appropriate risk level.

Audit:
Perform the following to determine if anacron is enabled.

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

6.1.2 Enable cron Daemon

Configuration Level	Level-I
OS Default	Enabled
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4324-0

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.

Remediation:
```
# chkconfig cron on
```

Audit:
Perform the following to determine if `cron` is enabled.
```
# chkconfig --list cron
cron: 0:off  1:off  2:on  3:on  4:on  5:on  6:off
```

6.1.3 Set User/Group Owner and Permission on `/etc/anacrontab`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The `/etc/anacrontab` file is used by `anacron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and is the only user that can read and write the file.

Rationale:
This file contains information on what system jobs are run by `anacron`. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Remediation:
```
# chown root:root /etc/anacrontab
# chmod og-rwx /etc/anacrontab
```

Audit:
Perform the following to determine if the `/etc/anacrontab` file has the correct permissions.
```
# stat -c "%a %u %g" /etc/anacrontab | egrep ".00 0 0"
```

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

6.1.4 Set User/Group Owner and Permission on /etc/crontab

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3626-9, CCE-3851-3, CCE-4388-5

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

Rationale:
This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Remediation:

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

Audit:
Perform the following to determine if the /etc/crontab file has the correct permissions.

```
# stat -c "%a %u %g" /etc/crontab | egrep ".00 0 0"
```

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

6.1.5 Set User/Group Owner and Permission on /etc/cron.hourly

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4054-3 CCE-3983-4 CCE-4106-1

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.

Remediation:

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

Audit:
Perform the following to determine if the `/etc/cron.hourly` file has the correct permissions.

```
# stat -c "%a %u %g" /etc/cron.hourly | egrep ".00 0 0"
```

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

6.1.6 Set User/Group Owner and Permission on `/etc/cron.daily`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3481-9 CCE-4022-0 CCE-4450-3

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.

Remediation:

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

Audit:

Perform the following to determine if the /etc/cron.daily directory has the correct permissions.

```
# stat -c "%a %u %g" /etc/cron.daily | egrep ".00 0 0"
```

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

6.1.7 Set User/Group Owner and Permission on /etc/cron.weekly

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4331-5 CCE-3833-1 CCE-4203-6

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.

Remediation:

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

Audit:
Perform the following to determine if the /etc/cron.weekly directory has the correct permissions.

```
# stat -c "%a %u %g" /etc/cron.weekly | egrep ".00 0 0"
```

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

6.1.8 Set User/Group Owner and Permission on /etc/cron.monthly

Configuration Level	Level-I

OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4322-4 CCE-4441-2 CCE-4251-5

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.

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

Audit:
Perform the following to determine if the `/etc/cron.monthly` directory has the correct permissions.

```
# stat -c "%a %u %g" /etc/cron.monthly | egrep ".00 0 0"
```

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

6.1.9 Set User/Group Owner and Permission on `/etc/cron.d`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4212-7 CCE-4380-2 CCE-4250-7

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.

Remediation:

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

Audit:
Perform the following to determine if the `/etc/cron.d` directory has the correct permissions.

```
# stat -c "%a %u %g" /etc/cron.d | egrep ".00 0 0"
```

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

6.1.10 Restrict `at` Daemon

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14466-7

Description:
The `at` daemon works with the cron daemon to allow non-privileged users to submit one time only jobs at their convenience. There are two files that control `at`: `/etc/at.allow` and `/etc/at.deny`. If `/etc/at.allow` exists, then users listed in the file are the only ones that can create `at` jobs. If `/etc/at.allow` does not exist and `/etc/at.deny` does exist, then any user on the system, with the exception of those listed in `/etc/at.deny`, are allowed to execute at jobs. An empty `/etc/at.deny` file allows any user to create `at` jobs. If neither `/etc/at.allow` nor `/etc/at.deny` exist, then only superuser can create `at` jobs. The commands below remove the `/etc/at.deny` file and create an empty `/etc/at.allow` file that can only be read and modified by user and group root.

Rationale:
Granting write access to this directory for non-privileged users could provide them the means to gain 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. In addition, it is a better practice to create a white list of users who can

execute `at` jobs versus a blacklist of users who can't execute at jobs as a system administrator will always know who can create jobs and does not have to worry about remembering to add a user to the blacklist when a new user id is created.

Remediation:

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

Audit:
Perform the following to determine if `at` jobs are restricted.

```
# stat /etc/at.deny > /dev/null
# stat -c "%a %u %g" /etc/at.allow | egrep ".00 0 0"
```

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

6.1.11 Restrict `at/cron` to Authorized Users

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation:

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

```
# chown root:root /etc/at.allow
```

Audit:
Perform the following to determine if the remediation in the section has been performed:

```
# ls -l /etc/cron.deny
[no output returned]
# ls -l /etc/at.eny
[no output returned]
# ls -l /etc/cron.allow
-rw------- 1 root root <date> /etc/cron.allow
# ls -l /etc/at.allow
-rw------- 1 root root <date> /etc/at.allow
```

6.2 Configure SSH

Description:
SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`.

Rationale:
It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

6.2.1 Set SSH Protocol to 2

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4245-7

Description:
SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:
SSH v1 suffers from insecurities that do not affect SSH v2.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^Protocol" /etc/ssh/sshd_config
Protocol 2
```

References:
For more information on the status of the SSH1 protocol, see the SSH web site http://www.ssh.com/company/newsroom/article/210/

6.2.2 Set LogLevel to VERBOSE

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The `VERBOSE` parameter specifices that record login and logout activity will be logged.

Rationale:
SSH provides several logging levels with varying amounts of verbosity. The "`DEBUG`" is specifically *not* recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information. The "`INFO`" level is the basic level that only records login activity of SSH users. The VERBOSE level records both login and logout activity. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^LogLevel" /etc/ssh/sshd_config
LogLevel VERBOSE
```

6.2.3 Set Permissions on /etc/sshd_config

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3958-6 CCE-3495-9

Description:

The /etc/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.

Rationale:
The /etc/sshd_config file needs to be protected from unauthorized changes by non-priliveged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:
Run the following command to determine the user and group ownership on the /etc/sshd_config file.

```
# /bin/ls -l /etc/sshd_config
-rw-r--r-- 1 root root 762 Sep 23  002 /etc/sshd_config
```

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

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

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

```
# chmod 644 /etc/sshd_config
```

6.2.4 Disable SSH X11 Forwarding

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^X11Forwarding" /etc/ssh/sshd_config
X11Forwarding no
```

6.2.5 Set SSH MaxAuthTries to 4 or Less

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `syslog` file detailing the login failure.

Rationale:
Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, it is set the number based on site policy.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^MaxAuthTries" /etc/ssh/sshd_config
MaxAuthTries 4
```

6.2.6 Set SSH IgnoreRhosts to Yes

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes

CCE Reference	CCE-4250-7

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`.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^IgnoreRhosts" /etc/ssh/sshd_config
IgnoreRhosts yes
```

6.2.7 Set SSH HostbasedAuthentication to No

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4251-5

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 .

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^HostbasedAuthentication" /etc/ssh/sshd_config
HostbasedAuthentication no
```

6.2.8 Disable SSH Root Login

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4252-3

Description:
The `PermitRootLogin` parameter specifies if the root user can log in using `ssh(1)`. The default is no.

Rationale:
Disallowing root logins over SSH requires server admins to authenticate using their own individual account, then escalating to root via `sudo` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^PermitRootLogin" /etc/ssh/sshd_config
PermitRootLogin no
```

6.2.9 Set SSH PermitEmptyPasswords to No

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4256-4

Description:
The `PermitEmptyPasswords` parameter specifies if the server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^PermitEmptyPasswords" /etc/ssh/sshd_config
PermitEmptyPasswords no
```

6.2.10 Do Not Allow Users to Set Environment Options

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4265-5

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)

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep PermitUserEnvironment /etc/ssh/sshd_config
PermitUserEnvironment no
```

6.2.11 Use Only Approved Ciphers in Counter Mode

Configuration Level	Level-I
OS Default	No

Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4269-7

Description:
This variable limits the types of ciphers that SSH can use during communication.

Rationale:
Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBD) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Cipher aes128-ctr,aes192-ctr,aes256-ctr
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "Cipher" /etc/ssh/sshd_config
Cipher aes128-ctr,aes192-ctr,aes256-ctr
```

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

6.2.12 Set Idle Timeout Interval for User Login

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4247-3

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.

Remediation:
Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^ClientAliveInterval" /etc/ssh/sshd_config
ClientAliveInterval 300
# grep "^ClientAliveCountMax" /etc/ssh/sshd_config
ClientAliveCountMax 0
```

6.2.13 Limit Access via SSH

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
There are several options available to limit which users and group can access the system via SSH. It is recommended that at least of the following options be leveraged:
AllowUsers
The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

AllowGroups

The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of comma separated user names. Numeric groupIDs are not recognized with this variable.

DenyUsers
The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

DenyGroups
The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

Rationale:
Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Remediation:
Edit the /etc/ssh/sshd_config file to set the parameter as follows:

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

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^AllowUsers" /etc/ssh/sshd_config
AllowUsers <userlist>

# grep "^AllowGroups" /etc/ssh/sshd_config
AllowGroups <grouplist>

# grep "^DenyUsers" /etc/ssh/sshd_config
DenyUsers <userlist>
# grep "^DenyGroups" /etc/ssh/sshd_config
DenyGroups <grouplist>
```

6.2.14 Set SSH Banner

Configuration Level	Level-I
OS Default	No
Reboot Required	No

Scorable Item	Yes
CCE Reference	CCE-4260-6

Description:
The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:
Banners are used to warn connecting users of the particular site's policy regarding connection. Consult with your legal department for the appropriate warning banner for your site.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner <bannerfile>
```

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "^Banner" /etc/ssh/sshd_config
Banner <bannerfile>
```

6.3 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

6.3.1 Set Password Creation Requirement Parameters Using `pam_cracklib`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The `pam_cracklib` module checks of the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the `pam_cracklib.so` options.

- `try_first-pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 3 tries before sending back a failure.
- `minlen=14` - password must be 14 characters or more
- `dcredit=-1` - provide at least 1 digit
- `ucredit=-1` - provide at least one uppercase character
- `ocredit=-1` - provide at least one special character
- `lcredit=-1` - provide at least one lowercase character

The setting shown above is one possible policy. Alter these values to conform to your own organization's password policies.

Rationale:
Strong passwords protect systems from being hacked through brute force methods.

Remediation:

```
# ed /etc/pam.d/system-auth: << END
/password.*requisite.*pam_cracklib.so/
d
a
password    required    pam_cracklib.so try_first_pass retry=3
minlen=14,dcredit=-1,ucredit=-1,ocredit=-1 lcredit=-1
.
w
q
END
```

Audit:
Perform the following to determine the current settings in the `pam_cracklib.so` file.

```
# grep pam_cracklib.so /etc/pam.d/system-auth
password    required    pam_cracklib.so try_first_pass retry=3
minlen=14,dcredit=-1,ucredit=-1,ocredit=-1 lcredit=-1
```

6.3.2 Set Strong Password Creation Policy Using `pam_passwdqc`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The `pam_passwdqc.so` module checks for a password strength in PAM configured password changing programs. In addition to checking passwords, it can also support passphrases. All features are optional and can be changed without rebuilding. The configuration line below describes the kinds of passwords that are allowed:

min=N0, N1, N2, N3,N4 where

N0 - passwords consisting of one character class only (e.g. digits, lower case, upper case, other characters) (disabled in this configuration)

N1 - passwords consisting of two character classes (disabled in this configuration)

N2 - passphrases. Note passphrases must contain a sufficient number of words (default is 3. It can be changed by setting passphrase=N, where N is the number of words) (minimum of 16 characters)

N3 - passwords consisting of three character classes (minimum of 12 characters)

N4 - passwords consisting of four characters classes (minimum of 8 characters)

There are a number of other options available for `pam_passwdqc` that can be set. Configure the module to support your organization's password policy.

Rationale:
The `passwdqc.so` module provides for stronger passwords to deter brute force password attacks on systems.

Remediation:

```
# ed /etc/pam.d/system-auth << END
/pam_cracklib.so/
d
a
password    requisite    pam_passwdqc.so min=disabled,disabled,16,12,8
.
w
q
END
```

Audit:
Perform the following to determine the current settings in the `pam_passwdqc.so` module.

```
# grep pam_passwdqc.so /etc/pam.d/system-auth
password    requisite    pam_passwdqc.so min=disabled,disabled,16,12,8
```

Note:
These password security measures apply to,; local passwords only. The organization may have password strength policies implemented by external systems such as LDAP or Active Directory.

References:
See the Linux man page for `pam_passwdqc` (8) for more configuration information.

6.3.3 Set Lockout for Failed Password Attempts

Configuration Level	Level-I

OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
Lock out userIDs after *n* unsuccessful consecutive login attempts. The first set of changes are made to the main PAM configuration file `/etc/pam.d/system-auth`. The second set of changes are applied to the program specific PAM configuration file (in this case, the `ssh` daemon). The second set of changes must be applied to each program that will lock out userID's.

Set the lockout number to the policy in effect at your site.

Rationale:
Locking out userIDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Remediation:
```
# sed -i "5i\auth\trequired\pam_tally2.so deny=5 onerr=fail"
/etc/pam.d/system-auth
```

Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` is the `pam_tally2.so` module, the user can be unlocked by issuing the command `/usr/sbin/pam_tally2 -u <username> --reset=0`. This command sets the failed tally count to 0, effectively unlocking the userid.

Audit:
Perform the following to determine the current settings for userID lockout.
```
# grep "pam_tally2" /etc/pam.d/system-auth
auth  required    pam_tally2.so deny=5 onerr=fail
```

6.3.4 Use `pam_deny.so` to Deny Services

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	

Description:
Adding `pam_deny.so` as a requisite to a PAM aware service allows you to quickly disable the service. The requisite tag on the `auth` line tells PAM that authentication must fail if the name module returns a failure. Since `pam_deny.so` always returns failure, authentication will always fail for this service. This mechanism can be applied to any other PAM aware service on the system.

Rationale:
While there are other ways to disable a service, adding `pam_deny.so` allows you to disable the service for new users without affecting current users of the service.

Remediation:
Edit PAM aware services as shown below. For example the `sshd` service would be modified as shown below.

```
# ed /etc/pam.d/sshd << END
0a
auth  requisite   pam_deny.so
.
w
q
END
```

Note: Perform this action for every service that provides authentication and supports PAM.

Audit:
Perform the following to determine if `pam_deny.so` is a requisite in the service. Perform this command for each PAM-aware authentication service.

```
# grep "^auth" /etc/pam.d/sshd
auth  requisite   pam_deny.so
```

6.3.5 Upgrade Password Hashing Algorithm to SHA-512

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The SHA-512 encryption has been available since Red Hat release 5.2,. The commands below change password encryption from `md5` to `sha512` (a much stronger encryption algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:
The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Remediation:
Perform the following to configure the system as recommended:

```
# authconfig --passalgo=sha512
```

Note: If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all userID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used.

Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# cat /etc/passwd | awk -F: ` ( $3 >=500 && $1 != "nfsnobody ) { print $1 } |
xargs -n 1 chage -d 0
```

Audit:
Perform the following to determine if the password-hashing algorithm is set to SHA-512:

```
# authconfig --test | grep hashing | grep sha512
```

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

6.3.6 Limit Password Reuse

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation:

```
# ed /etc/pam.d/system_auth << END
/password.*pam_unix.so/
s/$/remember=5/
w
q
END
```

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

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

```
# grep "remember" /etc/pam.d/system_auth
password sufficient pam_unix.o <existing options> remember=5
```

6.3.7 Remove the `pam_ccreds` Package

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No

Scorable Item	Yes
CCE Reference	

Description:
The `pam_ccreds` module provides the ability for Linux users to locally authenticate using an enterprise identity when the network is unavailable.

Rationale:
While cached credentials provide flexibility in allowing enterprise users to authenticate when not attached to the network, it provides attackers with the ability of compromising those credentials if they've compromised the system.

Remediation:
```
# yum erase pam_ccreds
```

Audit:
Perform the following to determine if users are not permitted to use cached credentials:
```
# yum list pam_ccreds
pam_ccreds.<platform> <other items> <anything but installed>
```

6.4 Restrict root Login to System Console

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3485-0

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.

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

Audit:
```
# cat /etc/securetty
```

6.5 Restrict Access to the `su` Command

Configuration Level	Level-I
OS Default	No

Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation:
Edit the `/etc/pam.d/su` file as follows. Once this is done, create a comma separated list of users in the wheel statement in the `/etc/group` file.

```
# ed /etc/pam.d/su << END
/required.*pam_wheel.so/
s/^#//
w
q
END
```

Audit:

```
# grep pam_wheel.so /etc/pam.d/su
auth  required    pam_wheel.so use_uid
# grep wheel /etc/group
wheel:x:10:root, <user list>
```

7. User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment. Guidance for monitoring these settings and others that may change over time is provided in Section 10 System Maintenance.

7.1 Disable System Accounts

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4060-0

Description:
There are a number of accounts provided with the Red Hat that are used to manage applications and are not intended to provide an interactive shell.

Rationale:
It is important to make sure that accounts that are not being used by regular users are locked to prevent them from being used to provide an interactive shell. By default, Red Hat sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to `/sbin/nologin`**.** This prevents the account from potentially being used to run any commands.

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

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

7.2 Set Shadow Password Suite Parameters (`/etc/login.defs`)

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to

/etc/login.defs will only be applied if the usermod command is used. If userIDs are added a different way, use the chage command to effect changes to individual userIDs.

7.2.1 Set Password Expiration Days

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 90 days.

Rationale:
The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an an attacker's window of opportunity.

Remediation

```
# ed /etc/login.defs << END
/PASS_MAX_DAYS/
/[    ].*/s//  90/
w
q
END
#chage --maxdays 90 <user>
```

Audit:

```
# grep PASS_MAX_DAYS /etc/login.defs
PASS_MAX_DAYS 90
# chage --list <user>
Maximum number of days between password change: 90
```

7.2.2 Set Password Change Minimum Number of Days

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation

```
# ed /etc/login.defs << END
/PASS_MIN_DAYS/
/[    ].*/s//  7/
w
q
END
# chage --mindays 7 <user>
```

Audit:

```
# grep PASS_MIN_DAYS /etc/login.defs
PASS_MAX_DAYS 7
# chage --list <user>
Miniumum number of days between password change:      7
```

7.2.3 Set Password Expiring Warning Days

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	

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.

Remediation

```
# ed /etc/login.defs << END
/PASS_WARN_AGE/
/[    ].*/s//  7/
w
q
```

```
END
# chage --warndays 7 <user>
```

Audit:

```
# grep PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
# chage --list <user>
Number of days of warning before password expires:    7
```

7.3 Set Default Group for root Account

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4060-0

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.

Remediation:

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

Audit:

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

7.4 Set Default umask for Users

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4060-0

Description:
The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile, .cshrc, etc.) in their home directories.

Rationale:
Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.
Note:
The directives in this section apply to `bash` and `shell`. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Remediation:
Edit the `/etc/bashrc` and `/etc/profile` files (and the appropriate files for any other shell supported on your system) and add the following the UMASK parameter as shown:

```
UMASK=077
```

Audit:

```
# grep "^UMASK=077" /etc/bashrc
UMASK=077
# grep "^umask 077" /etc/profile
umask 077
```

7.5 Lock Inactive User Accounts

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4060-0

Description:
Guidelines published by the U.S. Department of Defense specify that user accounts must be locked out after 35 days of inactivity. This number may vary based on the particular site's policy.

Rationale:
Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Remediation:

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

Audit:

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

8. Warning Banners

Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.
Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

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

8.1 Set Warning Banner for Standard Login Services

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4060-0

Description:
The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices, and also prior to logins via telnet. The contents of the `/etc/motd` file is generally displayed after all successful logins, no matter where the user is logging in from, but is thought to be less useful because it only provides notification to the user after the machine has been accessed.

Rationale:
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Remediation:

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

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

Audit:
Run the following commands and ensure that the files exist and have the correct permissions.

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

# ls /etc/issue
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue
# ls /etc/issue.net
-rw-r--r-- 1 root root 2055 Jan 30 16:30 /etc/issue
```

The commands above simply validate the presence of the `/etc/motd`, `/etc/issue` and `/etc/issue.net` files. Review the contents of these files with the "`cat`" command and ensure that it is appropriate for your organization.

8.1.1 Remove OS Information from Login Warning Banners

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

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

\m - machine architecture (uname -m)
\r - operating system release (uname -r)
\s - operating system name
\v – operating system version (uname –v)

Rationale:
Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of

a system. Authorized users can easily get this information by running the "`uname –a`" command once they have logged in.

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

Audit:
Perform the following commands to check if OS information is set to be displayed in the system login banners:

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

8.2 Set GNOME Warning Banner

Configuration Level	Level-I
OS Default	No
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-4188-9

Description:
The GNOME Display Manager is used for login session management. See the manual page `gdm(1)` for more information. The remediation action for this item sets a warning message for GDM users before they log in.

Rationale:
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Remediation:
Edit the file `/usr/share/gdm/themes/RHEL/RHEL.xml` and add the following statements after the two (2) pixmap blocks.

```
<item type="rect" id="custom-banner">
<pos anchor="nw" x="20%" y="10" width="80%" height="100%"/>
<box>
<item type="label">
<normal font="Sans Bold 9" color="#ffffff"/>
<text>
Insert the text of your warning banner here.
</text>
</item>
</box>
</item>
```

Audit:

```
# grep "<Text of Warning banner>" /usr/share/gdm/themes/RHEL/RHEL.xml
<Text of Warning banner>
```

9. System Maintenance

No matter how securely a system has been installed and hardened, administrator and user activity over time can introduce security exposures. The section describes tasks to be performed on a regular, ongoing basis - perhaps in an automated fashion via the `cron` utility.

Note: unlike other sections, the items in this section specify an Audit action followed by a Remediation action since it is necessary to determine what the current setting is before determining remediation measures, which will vary depending on the site's policy.

9.1 Verify System File Permissions

Configuration Level	Level-II
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	N/A

Description:

The RPM package manager has a number of useful options. One of these, the `–V` (or `–verify`) option, can be used to verify that system packages are correctly installed. The -V option can be used to verify a particular package or to verify all system packages (`–Va`). If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

Code	Meaning
S	File size differs.
M	File mode differs (includes permissions and file type).
5	The MD5 checksum differs.
D	The major and minor version numbers differ on a device file.
L	A mismatch occurs in a link.
U	The file ownership differs.
G	The file group owner differs.
T	The file time (mtime) differs.

The `rpm -qf` command can be used to determine which package a particular file belongs to. For example the following command determines which package the `/etc/passwd` file belongs to:

```
# rpm -qf /etc/passwd
setup-2.5.58-7.el5
```

To verify the settings for the package that controls the `/etc/passwd` file, run the following:

```
# rpm -V setup-2.5.58-7.el5
.M......  c /etc/passwd
S.5....T c /etc/printcap
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`
.M...... c /etc/passwd
S.5....T c /etc/printcap
```

Rationale:
It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

Note:
Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and is therefore not a scorable benchmark item, but is provided for those interested in additional security measures.

Audit:
Run the following command to review all installed packages. Note 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>
```

Remediation:
Correct any discrepancies found and rerun the command until output is clean or risk is mitigated or accepted.

References:
http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html

9.1.1 Verify Permissions on `/etc/passwd`

Configuration Level	Level-I
OS Default	Yes

Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3566-7

Description:
The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

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

Audit:
Run the following command to determine the permissions on the `/etc/passwd` file.

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

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

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

9.1.2 Verify Permissions on `/etc/shadow`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4130-1

Description:
The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:
If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:
Run the following command to determine the permissions on the `/etc/shadow` file.

```
# /bin/ls -l /etc/shadow
-r-------- 1 root root 633 Sep 23  2002 /etc/shadow
```

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

```
# /bin/chmod 400 /etc/shadow
```

9.1.3 Verify Permissions on `/etc/gshadow`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3932-1

Description:
The `/etc/gshadow` file contains information about group accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:
If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as expiration) could also be useful to subvert the group accounts.

Audit:
Run the following command to determine the permissions on the `/etc/gshadow` file.

```
# /bin/ls -l /etc/gshadow
-r-------- 1 root root 633 Sep 23  2002 /etc/gshadow
```

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

```
# /bin/chmod 400 /etc/gshadow
```

9.1.4 Verify Permissions on `/etc/group`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3967-7

Description:
The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:
The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:
Run the following command to determine the permissions on the `/etc/group` file.

```
# /bin/ls -l /etc/group
-rw-r--r-- 1 root root 762 Sep 23  002 /etc/group
```

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

```
# /bin/chmod 644 /etc/group
```

9.1.5 Verify User/Group Ownership on `/etc/passwd`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3958-6 CCE-3495-9

Description:
The `/etc/passwd` file contains a list of all the valid userIDs defined in the system, but not the passwords. The command below sets the owner and group of the file to root.

Rationale:
The `/etc/passwd` file needs to be protected from unauthorized changes by non-priliveged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:
Run the following command to determine the user and group ownership on the `/etc/passwd` file.

```
# /bin/ls -l /etc/passwd
-rw-r--r-- 1 root root 762 Sep 23  002 /etc/passwd
```

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

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

9.1.6 Verify User/Group Ownership on `/etc/shadow`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3918-0 CCE-3988-3

Description:
The `/etc/shadow` file contains the one-way cipher text passwords for each user defined in the `/etc/passwd` file. The command below sets the user and group ownership of the file to root.

Rationale:
If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:
Run the following command to determine the permissions on the `/etc/shadow` file.

```
# /bin/ls -l /etc/shadow
-r-------- 1 root root 762 Sep 23  2002 /etc/shadow
```

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

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

9.1.7 Verify User/Group Ownership on `/etc/gshadow`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4210-1 CCE-4064-2

Description:
The `/etc/gshadow` file contains information about group accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:
If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as expiration) could also be useful to subvert the group accounts.

Audit:
Run the following command to determine the permissions on the `/etc/gshadow` file.

```
# /bin/ls -l /etc/gshadow
-r-------- 1 root root 633 Sep 23  2002 /etc/gshadow
```

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

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

9.1.8 Verify User/Group Ownership on `/etc/group`

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3276-3 CCE-3883-6

Description:
The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:
The `/etc/group` file needs to be protected from unauthorized changes by non-priliveged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:
Run the following command to determine the permissions on the `/etc/group` file.

```
# /bin/ls -l /etc/group
-rw-r--r-- 1 root root 762 Sep 23  002 /etc/group
```

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

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

9.1.9 Find World Writable Files

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-3795-2 CCE-14794-2

Description:
Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

Rationale:
Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

Audit:

```
#!/bin/bash
for $i in `/bin/egrep '(ext4|ext3|ext2)' /etc/fstab | /bin/awk '{print $2}'`
do
/usr/bin/find $i -xdev -type f -perm -0002 -print
done
```

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.

9.1.10 Find Un-owned Files and Directories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4223-4

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:
A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

```
#!/bin/bash
for $i in `/bin/egrep '(ext3|ext2)' /etc/fstab | /bin/awk '{print $2}'`
do
/usr/bin/find $i -xdev \( -type f -o -type d) -nouser -print
done
```

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.

9.1.11 Find Un-grouped Files and Directories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3573-3

Description:
Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:
A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

```
#!/bin/bash
for $i in `/bin/egrep '(ext3|ext2)' /etc/fstab | /bin/awk '{print $2}'`
do
/usr/bin/find $i -xdev \( -type f -o -type d) -nogroup -print
done
```

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.

9.1.12 Find SUID System Executables

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-14340-4

Description:
The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:
There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

```
#!/bin/bash
for $i in `/bin/egrep '(ext3|ext2)' /etc/fstab | /bin/awk '{print $2}'`
do
/usr/bin/find $i -xdev -type f  -perm -4000 -print
done  -print
```

Remediation:
Ensure that no rogue set-UID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the the integrity of these binaries as described below:

```
# rpm -V `rpm -qf /usr/bin/sudo`
.......T  /usr/bin/sudo
SM5....T  /usr/bin/sudoedit
```

9.1.13 Find SGID System Executables

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	No
CCE Reference	CCE-14340-4

Description:
The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the

group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:
There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced. The following is an example of checking the "`sudo`" executable:

```
# rpm -V `rpm -qf /usr/bin/sudo`
.......T  /usr/bin/sudo
SM5....T  /usr/bin/sudoedit
```

Audit:

```
#!/bin/bash
for $i in `/bin/egrep '(ext3|ext2)' /etc/fstab | /bin/awk '{print $2}'`
do
/usr/bin/find $i -xdev -type f  -perm -2000 -print
done
```

Remediation:
Ensure that no rogue set-GID programs have been introduced into the system

```
# /bin/rpm -V `/bin/rpm -qf sudo`
```

9.2 Review User and Group Settings

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

9.2.1 Ensure Password Fields are Not Empty

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4238-2

Description:
An account with an empty password field means that anybody may log in as that user without providing a password.

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

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

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

Remediation:
If any accounts in the /etc/passwd file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# /usr/bin/passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

9.2.2 Verify No Legacy "+" Entries Exist in /etc/passwd File

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4114-5

Description:
The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

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

```
# /bin/grep '^+:' /etc/passwd
```

Remediation:
Delete these entries if they exist.

9.2.3 Verify No Legacy "+" Entries Exist in /etc/shadow File

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14071-5

Description:
The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

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

```
# /bin/grep '^+:' /etc/shadow
```

Remediation:
Delete these entries if they exist.

9.2.4 Verify No Legacy "+" Entries Exist in `/etc/group` File

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-14675-3

Description:
The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on RHEL5 systems, but may exist in files that have been imported from other platforms.

Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

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

```
# /bin/grep '^+:' /etc/group
```

Remediation:
Delete these entries if they exist.

9.2.5 Verify No UID 0 Accounts Exist Other Than root

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4009-7

Description:
Any account with UID 0 has superuser privileges on the system.

Rationale:
This access must be limited to only the default *root* account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 7.5 Restrict root Login to System Console.

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

```
# /bin/cat /etc/passwd | /bin/awk -F: '($2 == 0) { print $1 }'
root
```

Remediation:
Delete any other entries that are displayed.

9.2.6 Ensure root PATH Integrity

Configuration Level	Level-I
OS Default	Yes
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-3301-9

Description:
The `root` user can execute any command on the system and could be fooled into executing programs unemotionally if the `PATH` is not set correctly.

Rationale:
Including the current working directory (`.`) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:

```
#!/bin/bash
if [ "`echo $PATH | /bin/grep :: `" != "" ]; then
      echo "Empty Directory in PATH (::)"
fi

if [ "`echo $PATH | bin/grep :$`"  != "" ]; then
      echo "Trailing : in PATH"
fi

p=`echo $PATH | /bin/sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
set -- $p
while [ "$1" != "" ]; do
      if [ "$1" = "." ]; then
            echo "PATH contains ."
            shift
            continue
      fi
      if [ -d $1 ]; then
            dirperm=`/bin/ls -ldH $1 | /bin/cut -f1 -d" "`
            if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
                  echo "Group Write permission set on directory $1"
            fi
            if [ `echo $dirperm | /bin/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.

9.2.7 Check Permissions on User Home Directories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	CCE-4090-7

Description:
While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:
Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd  | /bin/egrep -v '(root|halt|sync|shutdown)
|\
      /bin/awk -F: '($8 == "PS" && $7 != "/sbin/nologin") { print $6 }'`; do
            dirperm=`/bin/ls -ld $dir | /bin/cut -f1 -d" "`
            if [ `echo $dirperm | /bin/cut -c6 ` != "-" ]; then
                  echo "Group Write permission set on directory $dir"
            fi
            if [ `echo $dirperm | /bin/cut -c8 ` != "-" ]; then
                  echo "Other Read permission set on directory $dir"

            fi

            if [ `echo $dirperm | /bin/cut -c9 ` != "-" ]; then
                  echo "Other Write permission set on directory $dir"
            fi
            if [ `echo $dirperm | /bin/cut -c10 ` != "-" ]; then
                  echo "Other Execute permission set on directory $dir"
            fi
done
```

Remediation:
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

9.2.8 Check User Dot File Permissions

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:
Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|sync|halt|shutdown)'
| /bin/awk -F: '($8 == "PS" && $7 != "/sbin/nologin") { print $6 }'`; do
      for file in $dir/.[A-Za-z0-9]*; do

            if [ ! -h "$file" -a -f "$file" ]; then
                  fileperm=`/bin/ls -ld $file | /bin/cut -f1 -d" "`

                  if [ `echo $fileperm | /bin/cut -c6 ` != "-" ]; then
                        echo "Group Write permission set on file $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c9 ` != "-" ]; then
                        echo "Other Write permission set on file $file"
                  fi
            fi

      done

done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

9.2.9 Check Permissions on User `.netrc` Files

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	

Description:
While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:
`.netrc` files may contain unencrypted passwords that may be used to attack other systems.

Audit:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|sync|halt|shutdown)'
|\
      /bin/awk -F: '($8 == "PS" && $7 != "/sbin/nologin") { print $6 }'`; do
      for file in $dir/.netrc; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  fileperm=`/bin/ls -ld $file | /bin/cut -f1 -d" "`
                  if [ `echo $fileperm | /bin/cut -c5 ` != "-" ]
                  then
                        echo "Group Read set on $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c6 ` != "-" ]
                  then
                        echo "Group Write set on $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c7 ` != "-" ]
                  then
                        echo "Group Execute set on $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c8 ` != "-" ]
                  then
                        echo "Other Read  set on $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c9 ` != "-" ]
                  then
                        echo "Other Write set on $file"
                  fi
                  if [ `echo $fileperm | /bin/cut -c10 ` != "-" ]
                  then
                        echo "Other Execute set on $file"
                  fi
            fi
      done
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` file permissions and determine the action to be taken in accordance with site policy.

9.2.10 Check for Presence of User `.rhosts` Files

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
While no `.rhosts` files are shipped with RHEL5, users can easily create them.

Rationale:
This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

```
#!/bin/bash
for dir in `/bin/cat /etc/passwd | /bin/egrep -v '(root|halt|sync|shutdown)'
|\
      /bin/awk -F: '($8 == "PS" && $7 != "/sbin/nologin") { print $6 }'`; do
      for file in $dir/.rhosts; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".rhosts file in $dir"
            fi    done
done
```

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

9.2.11 Check Groups in `/etc/passwd`

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group`.

Rationale:
Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:
Create a script as shown below and run it:

```
#!/bin/bash
defUsers="root bin daemon adm lp sync shutdown halt mail news uucp operator
games gopher ftp nobody nscd vcsa rpc mailnull smmsp pcap ntp dbus avahi sshd
rpcuser nfsnobody haldaemon avahi-autoipd distcache apache oprofile webalizer
dovecot squid named xfs gdm sabayon"
/bin/cat /etc/passwd | while:
do
        x=`line`
        if [ "$x" = "" ]
        then
                break
        fi
        userid=`echo "$x" | cut -f1 -d':'`
      found=0
      for n in $defUsers
      do
            if [ $userid = "$n" ]
            then
                  found=1
                  break
            fi
      done
      if [ $found -eq 1 ]
      then
            continue
      fi
            groupid=`echo "$x" | /bin/cut -f4 -d':'`
            /bin/cat /etc/group | while :
            do
                  x=`line`
                  if [ "$x" = "" ]
                  then
                        echo "Groupid $groupid does not exist in /etc/group,
but is used by $userid"
                        break
                  fi
                  y=`echo $x | cut -f3 -d":"`
                  if [ $y -eq $groupid ]
                  then
                        break
                  fi
        done
done
```

Remediation:
Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

9.2.12 Check That Users Are Assigned Home Directories

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
The `/etc/passwd` file defines a home directory that the user is placed in upon login. If there is no defined home directory, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Rationale:
All users must be assigned a home directory in the `/etc/passwd` file.

Audit:
This script checks to make sure a home directory is defined for each user in the `/etc/passwd` file.

```
#!/bin/bash

echo "The Output for the Audit of Control 10.13 - Check That Users Are
Defined Home Directories is"
defUsers="root bin daemon adm lp sync shutdown halt mail news uucp operator
games gopher ftp nobody nscd vcsa rpc mailnull smmsp pcap ntp dbus avahi sshd
rpcuser nfsnobody haldaemon avahi-autoipd distcache apache oprofile webalizer
dovecot squid named xfs gdm sabayon"
 cat /etc/passwd |\
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir
      do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ $found -eq 0 ]
            then
                  if [ -z "$dir" ]
                  then
                        echo "User $user has no home directory."
                  fi
            fi
      done
```

Remediation:

Based on the results of the Audit script, perform the appropriate action for your environment (e.g. delete unneeded users or assign them a home directory).

9.2.13 Check That Defined Home Directories Exist

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
Users can be defined to have a home directory in `/etc/passwd`, even if the directory does not actually exist.

Rationale:
If the user's home directory does not exist, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.14 - Check That Defined Home
Directories Exist is"
defUsers="root bin daemon adm lp sync shutdown halt mail news uucp operator
games gopher ftp nobody nscd vcsa rpc mailnull smmsp pcap ntp dbus avahi sshd
rpcuser nfsnobody haldaemon avahi-autoipd distcache apache oprofile webalizer
dovecot squid named xfs gdm sabayon"
 cat /etc/passwd |\
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir; do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ $found -eq 0 ]
            then
                  if [ -z "${dir}" ]; then
                        echo "User $user has no home directory."
                  elif [ ! -d $dir ]; then
                        echo "User $user home directory not found"
                  fi
            fi
      done
```

Remediation:
If any users' home directories do not exist, create them and make sure the respective user owns the directory.

9.2.14 Check User Home Directory Ownership

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:
Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.15 - Check User Home Directory
Ownership is"
defUsers="root bin daemon adm lp sync shutdown halt mail news uucp operator
games gopher ftp nobody nscd vcsa rpc mailnull smmsp pcap ntp dbus avahi sshd
rpcuser nfsnobody haldaemon avahi-autoipd distcache apache oprofile webalizer
dovecot squid named xfs gdm sabayon"

/usr/bin/cat /etc/passwd |  \
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir; do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ $found -eq "0" ]
            then
                  if [ -d ${dir} ]
                  then
                      owner=`ls -ld $dir | sed -e 's/ */ /g' | cut -f3 -d" "`
                      if [ "$owner" != "$user" ]
                      then
```

```
                              echo "Home directory for $user owned by $owner"
                        fi
                  fi
            fi
      done
```

Remediation:
Change the ownership any home directories that are not owned by the defined user to the correct user.

9.2.15 Check for Duplicate UIDs

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:
Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.16 - Check for Duplicate UIDs
is"
/bin/cat /etc/passwd | /bin/cut -f3 -d":" | /bin/sort -n | /usr/bin/uniq -c
|\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            users=`/bin/gawk -F: '($3 == n) { print $1 }' n=$2 \
                  /etc/passwd | /usr/bin/xargs`
            echo "Duplicate UID ($2): ${users}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique UIDs and review all files owned by the shared UID to determine which UID they are supposed to belong to.

9.2.16 Check for Duplicate GIDs

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:
User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.17 - Check for Duplicate GIDs
is"

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

Remediation:
Based on the results of the script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

9.2.17 Check That Reserved UIDs Are Assigned to System Accounts

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes

CCE Reference	N/A

Description:
Traditionally, UNIX systems establish "reserved" UIDs (0-499 range) that are intended for system accounts.

Rationale:
If a user is assigned a UID that is in the reserved range, even if it is not presently in use, security exposures can arise if a subsequently installed application uses the same UID.

Audit:
This script checks to make sure that "reserved" UIDs (0-499 range) are not assigned to non-system (default) accounts.

```
#!/bin/bash

echo "The Output for the Audit of Control 10.18 - Check That Reserved UIDS
Are Assigned to System Accounts is"
defUsers="root bin daemon adm lp sync shutdown halt mail news uucp operator
games gopher ftp nobody nscd vcsa rpc mailnull smmsp pcap ntp dbus avahi sshd
rpcuser nfsnobody haldaemon avahi-autoipd distcache apache oprofile webalizer
dovecot squid named xfs gdm sabayon"
/bin/cat /etc/passwd |\
      /bin/awk -F: '($3 < 500) { print $1" "$3 }' |\
      while read user uid; do
            found=0
            for tUser in ${defUsers}
            do
                  if [ ${user} = ${tUser} ]; then
                        found=1
                  fi
            done
            if [ $found -eq 0 ]; then
                  echo "User $user has a reserved UID ($uid)."
            fi
      done
```

Remediation:
Based on the results of the script, change any UIDs that are in the reserved range to one that is in the user range. Review all files owned by the reserved UID to determine which UID they are supposed to belong to.

9.2.18 Check for Duplicate User Names

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:

Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.

Rationale:
If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.18 - Check for Duplicate User
Names is"
cat /etc/passwd | cut -f1 -d":" | /bin/sort -n | /usr/bin/uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            uids=`/bin/gawk -F: '($1 == n) { print $3 }' n=$2 \
                  /etc/passwd | xargs`
            echo "Duplicate User Name ($2): ${uids}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

9.2.19 Check for Duplicate Group Names

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.

Rationale:
If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group. Effectively, the GID is shared, which is a security problem.

Audit:

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

```
#!/bin/bash

echo "The Output for the Audit of Control 10.19 - Check for Duplicate Group
Names is"
cat /etc/group | cut -f1 -d":" | /bin/sort -n | /usr/bin/uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            gids=`/bin/gawk -F: '($1 == n) { print $3 }' n=$2 \
                  /etc/group | xargs`
            echo "Duplicate Group Name ($2): ${gids}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

9.2.20 Check for Presence of User .netrc Files

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
The .netrc file contains data for logging into a remote host for file transfers via FTP.

Rationale:
The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.

Audit:

```
#!/bin/bash

echo "The Output from the Audit of Control 10.20 - Check for Presence of User
.netrc Files is"
for dir in `logins -ox |\
      /bin/awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.netrc; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".netrc file $file exists"
            fi
      done
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

9.2.21 Check for Presence of User `.forward` Files

Configuration Level	Level-I
OS Default	N/A
Reboot Required	No
Scorable Item	Yes
CCE Reference	N/A

Description:
The `.forward` file specifies an email address to forward the user's mail to.

Rationale:
Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

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

```
#!/bin/bash

echo "The Output from the Audit of Control 10.21 - Check for Presence of User
.forward Files is"
for dir in `logins -ox |\
      /bin/awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.forward; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".forward file $file exists"
            fi
      done
done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

Appendix A: References

1. *DHCP*. Internet Systems Consortium, 2001-2011. Web. 16 June 2011. <http://www.isc.org/software/dhcp>.
2. Ellis, Stuart & Ben Cotton. *RPM Guide*. Fedora, ed. 0, 2010. Web. 16 June 2011. <http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/index.html>.
3. Lewis, A.J. *LVM Howto*. Sinistra Software, Inc., 2002-2003. Red Hat, Inc., 2004-2005. Terrascale Technologies, Inc., 2005-2006. Rackable Systems, Inc., 2006. Web. 16 June 2011. <http://tldp.org/HOWTO/LVM-HOWTO/>.
4. Mayer, Frank, Karl MacMillan, & David Caplan. "SELinux by Example: Using Security Enhanced Linux." *Red Hat Enterprise Linux 5: Deployment Guide*. Prentice Hall, August 6, 2006. Chapters 43-45. Print.
5. McAllister, Murray, Scott Ravden, Daniel Walsh, Dominick Grift, Eric Paris, & James Morris. *Security-Enhanced Linux*. Fedora, ed. 1.5, 2010. Web. 16 June 2011. <http://docs.fedoraproject.org/en-US/Fedora/13/html/Security-Enhanced_Linux/>.
6. National Security Agency. *Security-Enhanced Linux*. Central Security Service, 15 Jan. 2009. Web. 16 June 2011. <http://www.nsa.gov/research/selinux/>.
7. National Security Agency. *SELinux Mailing List*. Central Security Service, 15 Jan. 2009. Web. 16 June 2011. <http://www.nsa.gov/research/selinux/list.shtml>.
8. Radven, Scott. *Managing Confined Services*. Fedora, ed. 1.4, 2010. Web. 16 June 2011. <http://docs.fedoraproject.org/en-US/Fedora/13/html/Managing_Confined_Services/>.
9. Red Hat. *Certifications & Accreditations*. Web. 16 June 2011. <http://www.redhat.com/solutions/government/certifications/>.
10. Red Hat. *Red Hat Documentation*. *Red Hat Enterprise Linux*. Web. 16 June 2011. <http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/index.html>.
11. *SELinux Project Wiki*. Security Enhanced Linux Project Page. 2010. Web. 16 June 2011. <http://www.selinuxproject.org/page/Main_Page>.
12. United States Department of Justice. *Computer Crime & Intellectual Property Section*. N.d. Web. 16 June 2011. <http://www.justice.gov/criminal/cybercrime/>.
13. Wade, Kartsen, Paul W Frields, & Scott Ravden. *SELinux FAQ*. Fedora, 13, 2010. Web. 16 June 2011. <http://docs.fedoraproject.org/en-US/Fedora/13/html/SELinux_FAQ/>.

Appendix B: Change History

Date	Version	Changes for this version
December 16th, 2012	2.0.0	Redraft of RHEL5 Benchmark