the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Red Hat Enterprise Linux 5

Version 1.1.1

May 2009

http://cisecurity.org

feedback@cisecurity.org

Terms of Use Agreement

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

THIS PAGE INTENTIONALLY LEFT BLANK

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 versions 5.0 – 5.1 running on x86 platforms.

This Benchmark was developed and tested on Red Hat Enterprise Linux (RHEL) version 5.0 and 5.1 (the initial release and first update). It is likely to work for subsequent Red Hat Enterprise Linux distributions and other Red Hat, Fedora and CENTOS derivatives. The scoring tool may not execute or may yield inaccurate results on non-RHEL systems. The CIS RHEL5 Benchmark has been tested and verified on Intel/AMD 32. Specifically, it has not been vetted against the Intel 64 bit, Itanium and the various IBM architectures.

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.

This edition of the CIS RHEL5 Benchmark consists of fixes to language and content, as well as remediation recommendations from the Center for Internet Security community. It does not introduce new content, but improves and corrects what has been previously published.

Consensus Guidance

This guide 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.

Intended Audience

This document 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.

Acknowledgements

The following individuals have contributed greatly to the creation of this guide:

Author
Joe Wulf, *ProSync Technology Group*

Contributors and Reviewers
John Banghart
Michael Boelen {*Contributed to v1.1.1*}
Giacomo G. Brussino
Keith Buck
Ron Colvin
Ralf Durkee
Dean Farrington
Blake Frantz {*Contributed to v1.1.1*}
David Gendel
Andrew Gilmore {*& contributed to v1.1.1*}
Steve Grubb {*& contributed to v1.1.1*}
Richard Holbert
James B. Horwath
David A. Kennel
Joel Kirch
Rodney McKee
Robert Miller {*Contributed to v1.1.1*}
Adam Montville {*Contributed to v1.1.1*}
Keith D. Schincke {*Contributed to v1.1.1*}
Dave Shackleford
Stephen John Smoogen {*Contributed to v1.1.1*}
Nguyen Thi Xuan Thu {*Contributed to v1.1.1*}
George Toft
John Traenky {*Contributed to v1.1.1*}
Trevor Vaughan
Zack Yang

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. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 discernable 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.

THIS PAGE INTENTIONALLY LEFT BLANK

1 CIS Red Hat Enterprise Linux 5 Benchmark

Introduction

Red Hat Enterprise Linux version 5 (RHEL5) is the new server-class release from Red Hat, Inc, that stabilizes SELinux, has been Common Criteria evaluated at EAL4+ and brings further stability and robustness to the enterprise level with this OS. Security hardening remains a vital element to the defense-in-depth approach for all computing elements within the enterprise.. The Center for Internet Security proudly brings the latest consensus-achieved security hardening recommendations in this Benchmark and accompanying scoring tool.

The content and intent of this Benchmark is to drive you, the reader to be more informed in regards to actions necessary for hardening and securing Red Hat Enterprise Linux systems. It is not going to provide non-security hardening information and guidance just for the sake of providing it. Some basics of a particular function might be touched upon, but this is usually for the relevance it directly provides to the security hardening actions at hand.

Please enjoy this edition of the Center for Internet Security Benchmark to harden Red Hat Enterprise Linux version 5.

Applying CIS Benchmark Recommendations

Question[1]:
After applying all the recommendations in the Benchmark (and due diligence), is my system "secure"?

The answer to this question depends on what is meant by "*secure*". If you're asking whether following the Benchmark eliminates *all* known security vulnerabilities and renders this system *completely* invulnerable to unauthorized access, then the answer has to be an unequivocal "**no**".

However, **carefully following the steps in a CIS Benchmark results in a system which has a smaller attack surface** than a default install of the given OS.

At the time of this Benchmark's writing, the Center for Internet Security's consensus-building process resulted in a solid core of security recommendations. These targeted specific, otherwise vulnerable, portions of the Red Hat Enterprise Linux operating system for hardening. The vulnerability discovery process continues without abatement. So, more are likely to exist, even now.
Every day, many systems are compromised (and later used to attack other systems) because the administrators of those machines failed to exercise even "minimum due care" when installing and configuring the system: patches are not kept up to date, dangerous services remain installed, much less left running even though vulnerabilities have been published, etc...
Compliance with the Benchmark means the System Administrator has executed a regular backup process (which supports disaster recovery), brought the system up to date with patches (system is current) and accomplished the Benchmark recommendations (done the hardening)--AND--continue to actively monitor/manage it, you've done the best possible from a CIS security hardening perspective.

[1] Original question/answer from online CIS Members forum, dated 2006/08/30

When accomplishing Benchmark compliance, CIS recommends a log be kept. This could be a paper trail of notes regarding actions taken and results along the way. Another option would be a terminal window (or windows) with very large numbers of scroll back history where all the actions are accomplished and errors are visible. Also, the `script` command is a very useful alternative, too.

Precedence of Benchmark-Compliance Audit

A Benchmark 'audit' is a method to check if an item has been secured. The following precedence was used in developing this Benchmark, it will guide implementer's in their application, and will demonstrate how a scoring/assessment tool should score/evaluate a system being reviewed based upon this guidance.

- Determine if an applicable service or application is installed. When ...
  - **True** - Process other relevant audit/checks, even if the service/app is disabled
  - **False** - All other related checks automatically PASS (it is not an error for the service to not exist)
- Service and applications only require hardening if installed
- All other audit/checks proceed in sequential order, from the top of the document to the bottom

For any specific CIS Benchmark recommendation where this precedence must be over-ridden, such will be clearly stated for that check. This might affect the implementation of the hardening actions, and will also guide exactly how a scoring tool is to assess the system. This provides stability and consistency across the network, within individual systems, and for those implementing it.

Partitioning Considerations

Prior to installing the RHEL5 operating system, comprehensively plan out available disk space to provide for a security-minded partitioning scheme that integrates security concerns and vital mission/application needs. Thus, should a partition become corrupt or full, the system will generally remain operational, resilient and resistant to damage or data loss.

Note: Neither the partitioning configuration, nor implementation of quotas, will be scored due to their inherent complexity and diversity, while still complying with the intent of this Benchmark.

The overall strategy is to apply security concepts to OS partitioning in the beginning of system build and installation activities in such a way that mount options can be applied to secure the machine --- such as `noexec` options for `/tmp` and `/home`, etc... Red Hat does not recommend putting things (i.e. partitions, directories and files) in non-standard locations, since SELinux already has a well-defined notion of where things belong (otherwise, run `semanage` to properly adjust file contents, though its at your own risk).

CIS recommends the following security-minded partitioning guidance, as it protects and segments various portions of operating system functionality. Such partitioning provides various benefits, among them being the protection of any one of them becoming full not adversely affecting the others.

- "`/`" (slash), the root partition is required; it is the top of the Unix filesystem tree structure and must be established as its own partition.
- "`/boot`"; required partition; allocated on the first physical drive the BIOS will look to for boot and/or start-up information.
- "`/home`"; it is assumed that systems will have non-root users, if for no other reason than to serve as the place for SysAdmins to log in as themselves, then switch users to root in order to manage it.

- "/tmp"; provides a safe container for temporary storage.
- "/var"; container for application, security and audit logs.
- "/var/log/audit"; It is preferable to have the audit data stored on its own partition so that auditd will correctly calculate when its partition is out of space. For example, any user can otherwise loop the logger program in a script and fill up /var with messages to syslogd.
- "<swap>"; provides additional virtual memory to supplement physical memory. Strong preference to being implemented as a partition (for performance) vice a file, though both do work.
- … Other, additional partitions may be added, and sized, as site/mission requirements dictate. These include /opt, /usr and other local-use data partitions.

/home should be its own distinct partition as a repository for local storage of administrative and/or enterprise user files. CIS RHEL5 Benchmark sections 2.3 and 8.6 (at least) address sane security-based prohibitions against remote root logins. The underlying issue is that any place a user can write to must be on a separate partition from /bin, /sbin, and /usr. Otherwise a miscreant can potentially hardlink against any installed setuid and/or setgid application/utility. If (when) an exploit is found, even though the SysAdmin can upgrade the affected package(s), the aforementioned hardlink would provide a compromise vector, since a private copy would still remain, and with all access mode flags intact. Also, with /home as its own partition, mount options can/should be employed to limit permissions and support implementation of quotas.

Note: To further limit the inconveniences caused by filling up /home, consider implementing user and group quotas on, at least, the /home filesystem (i.e. on those servers that are repositories for users and their home directories). Quotas will limit how much a single user (or single group) can store on a given filesystem. Application of quotas is also not a scorable item.

Generally, partitions can all be within primary and/or extended partitions, without leveraging Logical Volume Management (LVM), though CIS strongly encourages LVMs to provide increased robustness is disk and partition management.

Recommend manually changing the /var/tmp directory to be a symbolic link to /tmp. This will prevent hardlinks to databases and executables possibly held in /var somewhere. This is accomplished with:

```
rm  -rf  /var/tmp
ln  -s   /tmp  /var/tmp
```

Balanced by the guidance provided above, the CIS Benchmark recommends system disk partitioning similar to what is found in the following table. This display presumes a modest 72GB drive (your configuration might be more robust). Also, this presumes the default of 32MB physical extents.

Example Partition Table

```
{df -h}                                 Original
Filesystem                      Size    Allot.  Used  Avail  Use%  Mounted on
/dev/mapper/VolGroup00-LogVol00  15G   (15360)  1.8G    13G   13%  /
/dev/sda1                       114M     (118)   12M    97M   11%  /boot
tmpfs                           302M                0   302M    0%  /dev/shm
/dev/mapper/VolGroup00-LogVol01 3.9G    (4096)  137M   3.6G    4%  /home
/dev/mapper/VolGroup00-LogVol02  12G   (12800)  159M    11G    2%  /tmp
/dev/mapper/VolGroup00-LogVol03 7.8G    (8192)  176M   7.2G    3%  /var
/dev/mapper/VolGroup00-LogVol04  16G   (16384)  173M    15G    2%  /var/log/audit
                                 4G    (4095)                     <swap>
```

Note: The "***Original Allot.***" column shows partitioning sizes entered during system installation. Further, this configuration, leave an approximate 32GB unallocated, within LVM.

More information is available from the online websites:
http://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/Deployment_Guide-en-US/ch-disk-quotas.html
http://h20331.www2.hp.com/enterprise/downloads/RHEL5-CC-EAL4-HP-Configuration-Guide.pdf
http://www.ibm.com/developerworks/library/os-ltc-security/index.html?ca=drs-

Software Package Removal

There has been considerable debate over the disposition of unused software packages. Some people feel that as long as the software is not being used, leaving it installed poses no appreciable risk. Others feel that unused software presents another attack vector and increases the maintenance effort for the administrators. This Benchmark currently makes no recommendation for the removal of *specific* unused software. This Benchmark does encourage a healthy review of installed packages, with an emphasis towards removing those that are clearly not required to support mission applications.

Note: When vulnerable software is present on a system, that vulnerability may be exploitable by a local attacker, and the reader is advised to consider the effort in either its removal or maintenance and the security risks thereof. For example, a service might be unused, disabled (via `chkconfig`)---yet it might also have SUID/SGID executables or scripts that could be used by a miscreant for attacks. This Benchmark recommends carefully evaluating what packages are installed and removing as many of those known to not have a bearing on the functionality of the mission system. Where possible, evaluate this minimization technique on a laboratory system. The rpm commands provide access to the internal documentation of installed packages.

Backup Key Files

Before performing the steps of this Benchmark on a production system it is **strongly recommended** that administrators make backup copies of critical configuration files that may get modified by various Benchmark items. If this step is not performed, then the site may have no reasonable back-out strategy for reversing system modifications made as a result of this document. The critical file protection script. provided in Appendix B of this document will automatically back up all files that may be modified by accomplishing the Benchmark actions below.

Note: An executable copy of the backup script is also provided in the archive containing the PDF version of this document and the CIS scoring tool. Assuming the administrator is in the directory where the archive has been unpacked, the command to execute the backup script would be:
`./do-backup.sh`

One of the byproducts of the `do-backup.sh` script is a dynamic system-specific restoration script: "`/root/cis/do-restore.sh`", which is generated based on the results of the `do-backup.sh` script.

To roll back the changes made as you applied this Benchmark, run `do-restore.sh` with a subsequent reboot, and all changes will be backed out. Since Linux installations are not all identical, the `do-restore.sh` script is created based on the files that actually existed at the time `do-backup.sh` was run, to include preservation of their original permissions.

Once the Benchmark items have been planned for a particular system, it is wise to fully test on a lab duplicate the backup and restoration process and the resultant system operation.

Many of the scriptlets in this Benchmark provide 'diff' comparisons against files preserved before the scriptlet was run (that is the assumption, anyway). Files, and in some cases directories, are duplicated by the `do-backup.sh` script where it appends a "`-preCIS`" bit of text to the end of the name.

Note: When making changes manually to any of the files that were preserved by `do-backup.sh`, those changes will be lost when `do-restore.sh` is executed. It would be prudent to delete (or save an offline copy of) the `do-restore.sh` script (and specific to the system it came from) once all changes have been validated to prevent inadvertently undoing the changes. The recommended CIS Benchmark backup script is generic, the restoration script is dynamically generated and unique.

Executing Actions

The actions listed in this document are written with the assumption that they will be executed in the order presented, and especially should be evaluated on a test/lab system representing a like-production system first. Some actions may need to be modified if the order is changed, as all possibilities and combinations cannot be anticipated nor exhaustively tested. Remediation has been written so that the scriptlets may be copied directly from this document into a root shell window with a "cut-and-paste" operation.

It is possible for some of the "`chkconfig`" actions, which activate or deactivate services, produce the message: "`error reading information on service <svc>: No such file or directory`". These messages are quite normal and are not a cause for alarm – they simply indicate the program or service being referenced was not installed on the machine being hardened. As Red Hat Enterprise Linux installs allow a great deal of flexibility in what software is chosen to be installed (as well as behind-the-scenes resolution of dependencies), these messages occur at times while accomplishing some Benchmark compliance tasks; and are normal.

Note: **A strong word of caution is necessary here**. Many of the Benchmark scriptlets **assume** *specific* content within configuration files, *specific* file locations, etc... They are good *enough* for demonstrating to a SysAdmin what should be addressed, and perhaps good enough to execute against clean/virgin systems. However, some scriptlets are downright **DANGEROUS** to run on a production system with changed configuration files, that have evolved as the system is used and administered, without otherwise testing them first!
A relevant, non-trivial, example is the scriptlet within Section 2.3 "Configure SSH". At one point it removes all "`Host *`" lines. This potentially changes the semantics of the configuration file on an operational production system, if the removed entry was preceded by a different, and yet valid, "`Host`" header (or more). This is but one example, even within this section, but by no means the only one.

So, the prudent precaution is to perform CIS Benchmark actions on a duplicate of a production system, not the production system itself! Carefully examine all before and after files for the changes made, and incorporate 'fixes' beyond what the Benchmark can anticipate, to ensure the system is still functioning correctly. Test resulting changed files, configurations and functionality for proper, assured and consistent behavior. Subsequently, migrate stable security hardening, tempered by lessons learned, to production system(s).

Finally, no single change or application of a single section from this Benchmark will fully harden a system. In fact, the bulk of these recommendations are necessary as a whole, though, of course, tailored to the specific environment and role/function of the system itself.

A Root Shell Environment Is Required

The actions spelled out in this CIS RHEL5 Benchmark are written with the expectation they will be executed by an Administrative person (SysAdmin) logged into the system as the `root` user (UID 0), running the `bash` shell and with `noclobber` unset (equivalent to "`set +o noclobber`"). Also, two directories are assumed to be in `root`'s path while accomplishing the CIS Red Hat Enterprise Linux 5 Benchmark hardening/compliance.

Use "`echo $PATH`" to determine what the current path is set to. An example of correct output is:
`/bin:/sbin:/usr/bin:/usr/sbin`

There is the concept of an established 'place', a directory, whereby the CIS Benchmark is executed from, and potentially any hardening actions are operated from. Not every section of the CIS Benchmark will need to change directory; where it is done, it is for end-user typing convenience. This is established, for consistency, as:

```
cishome='/root/cis'; export cishome
```

Where two or more lines to are shown in the remediation area to execute, System Administrators are encouraged to carefully collect and run them from a separate shell script rather than individually pasting them directly in an SSH session or terminal to the shell. There can be inadvertent and unresolved line wrapping, line termination, and quoting issues with the latter. To make a shell script, do the following in creating a file with a favorite editor, such as:

```
vi /root/myscript.sh
```

Put this text as the very first line in the `/root/myscript.sh` file:
```
#!/bin/bash
```

Paste the commands to run from the Benchmark into the file (ensure the entire scriptlet for the applicable sections are copied intact). A method to accomplish this would be to have the Benchmark PDF file open in one window, with an xterm window open beside it. Then simply cut and paste sections of script from the Benchmark directly onto the test/development/lab system.
For those lines of script ending in a backslash ("\"), make sure that is the last character on the line within the script. The line feed <enter key> must immediately follow it, with no trailing spaces or tabs.

Note: When pasting from Windows or a Macintosh, be careful to ensure the final file has a Unix style of line break; i.e. a single LF (Line Feed, ASCII 0x10). Files edited on Windows will commonly have a CR (Carriage Return, 0x13) followed by LF (Line Feed, 0x15). This causes odd errors, including shell scripts that do not run; the typical "Command not found" error occurs because it appears to Unix that the script asked for a shell of "`#!/bin/bash^M`", not "`#!/bin/bash`".

To prevent this from happening, execute the following:
```
tr -d "\015" < /root/myscript.sh > /root/myscriptNEW.sh
mv /root/myscriptNEW.sh /root/myscript.sh
```
{Another alternative would be to use "`unix2dos`"; check the `man` page}

Once the script has been saved, make it executable with:
```
chmod 0700 /root/myscript.sh
```

As necessary, ensure root ownership with:
```
chown root:root /root/myscript.sh
```

Finally, though beneficial when using the bash shell (it isn't required) unalias the `mv` and `cp` commands, as some Unix commands during Benchmark hardening will overwrite files; and might be prompted numerous times about overwriting these files:
```
unalias mv cp
```

Software Package Installation

Throughout the CIS RHEL5 Benchmark, a SysAdmin will find discussion and recommendations to enable individual software package `init` scripts using the `chkconfig` command. This assumes the SysAdmin has already installed the said `rpm` package(s), and then, only if they are vital to satisfy the mission of the particular system. CIS recommends against frivolous installation of any packages or software not critically **required** for the mission the system serves. CIS specifically recommends no package be installed on mission critical systems for convenience.

During Benchmark hardening compliance, should the `chkconfig` command fail, verify the installed software is actually required (local policy and system mission requirements will generally dictate this) and installed. To test whether a *package* is required, execute:
```
rpm -e --test <packagename>
```

To query information in a *packagename*, execute:
```
rpm -qi <packagename>
```

There is no direct mapping from a RHEL <servicename> to *packagename*, although for any installed service <foo>, information about that *package* can be obtained by executing:

```
rpm -qif /etc/rd.d/init.d/<foo>
```

The `chkconfig` command enables or disables service initialization at the next reboot, whereas the `service` command affects a service during the current instance.

Note: Though `chkconfig` and `service` are complimentary in function, they employ unique options and arguments in managing services. For additional information, examine their `man` pages.

Additionally, the Red Hat Deployment Guide provides instruction on package management resources; it's found at: "http://www.redhat.com/docs/manuals/enterprise"

Vulnerabilities

Every installed service within the RHEL5 OS has the potential of being an illicit entry point into a system if (*when*?!) a vulnerability is found. This is why CIS Benchmarks specifically recommend that all unneeded services be disabled/removed even though there might currently be no clear way to exploit them, and there has never been a problem with the service in the past (*an ounce of prevention*). When permitting an unnecessary service to continue functioning, additional risks exist of a vulnerability being discovered and/or exploited in that service in the future.

The fact that *you* don't know how to exploit a service or particular functionality is an invalid argument as to whether it is, or will be, in fact, *vulnerable*.

Taking this mindset a step further… Careful thought and consideration should be given to application of the CIS Benchmarks across the various systems employed in any given enterprise. Consider the role of the system, number of administrators and/or users accessing it and automated processes operating on it. Fewer services should be installed, much less executing, on systems directly accessible to the Internet. As opposed to systems physically isolated to a test lab environment which is logically and physically isolated.

Where possible, install and maintain systems with a logical consistency, employ an appropriate level of configuration management, leverage stable backup technology, etc. The point here is that this Benchmark is focused on solid RHEL hardening, while it is the end users responsibility to balance the appropriate level of hardening across the enterprise by role and function.

SELinux

Red Hat Enterprise Linux 5 makes SELinux available during installation. CIS highly recommends to enable this during system installation by specifically selecting "`ENFORCING MODE`" as the default. This setting is key to overall system hardening, as it employs the existing protection profiles incorporated within this release and activates them for dynamic protection during system operation. Again, testing this in a lab environment is recommended in combination with mission applications to validate expected functionality.

With this initial release of the RHEL5 Benchmark, that is as far as SELinux is going to be covered. CIS has plans to develop and release an appendix update to this RHEL5 Benchmark which addresses SELinux in comprehensive detail. The concern is that for this Benchmark many of the scriptlets create new versions of configuration files and then move them into place where the original had been. Many of these files have specific SELinux contexts which get destroyed by running the hardening scriptlet.

- One area to be included in this future section is addressing the restoration of the SELinux 'context' for files this Benchmark modifies. The following scriptlet illustrates the point, though it is not empirically incorporated throughout the Benchmark.

```
if [ -x /sbin/restorecon ]; then
      restorecon -v ${file}
fi
```

About Bastille

Previous editions of this CIS Benchmark recommended, made use of and/or complimented a system hardened with Bastille by Jay Beale. Bastille is a method (not reviewed, nor endorsed by Red Hat) of automating and hardening some actions to the operating system. This edition of the CIS RHEL5 Benchmark focuses exclusively on standardized consensus-based application of security hardening to the operating system without reference to Bastille.

Reboot Required

Rebooting the system is required after completing all of the actions specified within the Benchmark in order to complete the re-configuration of the system. In many cases, the changes made in the steps below will not take effect until this reboot is performed. If substantial operating system updates are performed after the initial OS load, the SysAdmin may have to reboot more than once. Check the SELinux paragraph above and the reboot section (at 11.8) for additional information on relabeling and reconfiguration needed to support SELinux security contexts when SELinux is installed and employed.

Housekeeping, Prepatory To Accomplishing The Remainder Of The Benchmark:

As a matter of consistency (and safety), use of this Benchmark presumes a subdirectory under `/tmp` is created, and with secure permissions to temporarily hold work-in-progress files. This temporary directory is to be removed at the end of the Benchmark-compliant hardening process. It is established as follows (using the `mktemp` command to avoid insecure race conditions):

```
tmpdir=`mktemp -d -t cis.XXXXXXXXXX`
mkdir          $tmpcis
chown root:root $tmpcis
chmod 0700      $tmpcis
```

THIS PAGE INTENTIONALLY LEFT BLANK

2 Patches, Packages and Initial Lockdown

2.1 Apply Latest OS Patches

Description:
Developing a standard procedure for keeping up-to-date with vendor patches is critical for the security and reliability of the system. Vendors issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues, but it is up to their customers to actually download and install these patches.

When Red Hat publishes an update, they include with it the procedures for updating the packages. This usually entails downloading the new RPMs from Red Hat, and making them available to the individual servers. Enterprises make these packages available over a Red Hat Satellite server, an NFS share, an internal anonymous FTP/HTTP server, or a `yum` repository – the Enterprise may follow this practice or do something entirely unique/different.

Red Hat offers automated internet patch download and installation, via Red Hat `yum`. In lieu of an existing local Enterprise Standard, consider installing `yum` and using it on a regular schedule, and whenever Red Hat announces a vulnerability. For RHEL5, updates via the internet require a valid support subscription.

If the local Enterprise has several servers, consider installing a Red Hat Satellite Update Server that can locally be used in place of Red Hat's Internet yum servers – the updates will go much faster, use much less bandwidth from the ISP, and will reduce the load on Red Hat's servers. When `yum` is used locally, it should be used on a lab server and the patches validated and the system regression tested before going to live/production systems.

Some RPMs may need to be installed before others. For the most part, RPM understands and resolves dependencies during the system build phase. Red Hat creates separate instructions for special cases, like the replacement of the kernel or the general C library glibc. Examine the list of updates to check for any of these cases.

There is some risk to using a non-patched, non-hardened machine to download the patches, as this involves connecting a system with unresolved security vulnerabilities on an Internet-connected network, which is not in conformance with Industry Best Practices. Please consider these issues carefully.

It is also important to observe that the mission applications work properly after patching. Though problems in patches are quite rare in Red Hat Enterprise Linux, it is generally recommended that any patch be deployed to a non-production system first for testing. Once it passes testing, then apply it to the production system(s).

The Center for Internet Security and Red Hat specifically encourages system owners, to the greatest extent possible, to upgrade/migrate systems to the latest release of the OS. It will contain all the merged/updated packages.

Remediation:
Update this system per local enterprise update procedures. This can be accomplished manually by executing the following command when the system is connected to the internet (or local `yum` repo):

```
yum update
```

Another strong recommendation would be to simply enable the `yum-updatesd` service:

```
service    yum-updatesd  start
chkconfig  yum-updatesd  on
```

Additional and/or separate procedures may be necessary to patch/update the system from a local Red Hat Satellite server, or some other method that is functional for the environment the system is in.

Scoring Status: **Not Scorable**

2.2 Validate The System Before Making Changes

Description:
Ensuring the system is functioning properly before making a change is a prudent system administration best practice and will save hours of aggravation. Applying this Benchmark to a system that already has issues makes troubleshooting very difficult and may incorrectly indicate the Benchmark is at fault.

Examine the system and application logs (found within `/var/log`). Key words to look for include, but are not limited to, "`error`", "`warning`", "`critical`", and "`alert`". These are terms to search for, should the system or an application be using them, and many do. This is a good place to start.

Remediation:

```
cd /var/log
egrep  -i  "(crit|alert|error|warn)"  *  |  less
```

Resolve all issues before continuing.

Scoring Status: **Not Scorable**

2.3 Configure SSH

Description:
OpenSSH is a popular free distribution of the industry standard SSH protocols which has become the best-practice implementation for secure communications on Linux distributions. For more information on OpenSSH, see http://www.openssh.org.
The settings in this section ensure safe defaults for both the SSH client and the SSH server. Specifically, both the `SSH` client and the `sshd` server are configured to use only SSH protocol 2, as long-standing serious security vulnerabilities have been found in the first SSH protocol. This may cause compatibility issues at sites still using the vulnerable SSH protocol 1; these sites should endeavor to configure all systems to use only SSH protocol 2 and rapidly migrate away from SSH protocol 1.

The hardening script below is divided into changes applicable to the use client for SSH (the first one) and then the SSH Daemon server (SSH). A future edition of the Benchmark will separate these into two separate items. The options to `SSH` that are hardened here, are done so as to explain their various

options. Please read the man pages, a wealth of internet resources, and Reference AN, as identified in Appendix D.

Some of the entries below duplicate defaults as installed natively by RHEL5. Since these are deemed critical to protecting system security, they are spelled out here as acceptable default behavior.

Client SSH (`ssh_config`):

- **Host**; Begins a section, so multiple such sections can exist. This indicates a *host specification*, identifying what host or hosts the following options are applicable to when initiating SSH communications.
- **Protocol**; The older protocol version 1 (one) has *significant* well-known vulnerabilities and available exploits, therefore it is not to be used. "**2**" (two) is a more recent version of the SSH protocol and is more robust and safer to use. Whereas version 1 lacks a strong mechanism for ensuring the security of the communications connection.
- **Port**; A default of '**22**' is recommended and is the default. Another Port can be stated here and is permissible. However, doing so requires additional configuration within the production environment, which is beyond the scope of this Benchmark. Do so with caution.
- ***PubkeyAuthentication***; *Public Key Authentication is stronger than password authentication. Enabling this (set to '**yes**') is the recommended default. It requires the establishment and exchange of public and private key pairs.*
  This entry is now subordinated to a Level II Benchmark issue and no longer a requirement.
  Note: The native `ssh_config` file might not already have this included in the file, by default.

Server SSH (`sshd_config`):

- **Port**; same as above.
- **Protocol**; same as above.
- **LogLevel**; Numerous logging levels are provided to log greater and greater details of SSH sessions. Note that "`DEBUG`" is specifically *not* recommended other than strictly for debugging SSH communications. "`INFO`" is the basic level that will record login's of SSH users. "**`VERBOSE`**" will record login and logout activity and is the minimum Benchmark recommendation level, though higher levels are acceptable, depending upon site/system policy.
- **PermitRootLogin**; The secure answer for this is '**no**'. By default, users should login to the system with their own non-privilege userID, and either utilize `sudo` or `su` to root to perform administrative functions. The preference there, is for `sudo`.
- **RhostsRSAAuthentication**; This is focused on protocol 1, and should be set to '**no**'.
- **HostbasedAuthentication**; Protocol 2-based and should be set to '**no**'. If it were enabled, it would be less secure then public/private key usage.
- **IgnoreRhosts**; Will be set to '**yes**' and thus deny usage of insecure host-based authentication via `.rhost` files.
- ***PasswordAuthentication***; *Will be set to '**no**', denying insecure usage of passwords from the `/etc/passwd` file for allowed users, thus leveraging the emphasis on public/private keys.*
  This entry is now subordinated to a Level II Benchmark issue and no longer a requirement.
- **PermitEmptyPasswords**; Will be set to '**no**' to prevent userIDs with blank passwords on this system from being accessed remotely.
- **Banner**; Will be used, pointing to `/etc/issue.net`, to provide all SSH users with a consent-to-use message.

Note: Display of a *consent-to-use* banner is added to the `sshd_config` file – this hardening process will create this banner later and it is discussed in detail in Section 10. If it is decided to choose not to implement a notification banner, remove the reference to `/etc/issue` from `sshd_config` manually. Please read the man page section on the legal use and benefits of banners before deciding to remove it.

At least one non-root user account should exist on the system, to avoid access/connectivity problems once this section of the Benchmark is applied, and especially if managing/hardening it remotely via SSH. At a minimum the process would be one of:

- To add a user account (which will be used to `su` to root for administrative access):
  `useradd <username>`
- Establish the password for the userID, ensuring it is compliant with password complexity rules:
  `passwd <username>`
- Next, include this userID in membership of the `wheel` group so they can switch users (`su`) to root:
  `usermod -G wheel <username>`

Remediation:

```
SSH_CONFIG='/etc/ssh/ssh_config'
SSHD_CONFIG='/etc/ssh/sshd_config'
if [ -e $SSH_CONFIG ]; then
   echo "Securing $SSH_CONFIG"
   grep -v "^Host \*" /etc/ssh/ssh_config-preCIS | grep -v "#   Protocol 2,1" \
           > $tmpcis/ssh_config.tmp
   awk '/^#.* Host /               { print "Host *"; print "Protocol 2"; next };
        /^#.*Port /                { print "Port 22"; next };
                                   { print }' $tmpcis/ssh_config.tmp  \
                                           > $tmpcis/ssh_config.tmp2

   if [ "`egrep -l ^Protocol $tmpcis/ssh_config.tmp2`" == "" ]; then
        echo 'Protocol 2' >> $tmpcis/ssh_config.tmp2
   fi
   /bin/cp -pf $tmpcis/ssh_config.tmp2 $SSH_CONFIG
   chown root:root $SSH_CONFIG
   chmod 0644      $SSH_CONFIG
   echo "diff $SSH_CONFIG-preCIS $SSH_CONFIG"
         diff $SSH_CONFIG-preCIS $SSH_CONFIG
else
   echo "OK - No $SSH_CONFIG to secure."
fi

if [ -e $SSHD_CONFIG ]; then
   echo "Securing $SSHD_CONFIG"
   # Had to put the " no" in for the RhostsRSAAuthentication source pattern
   # match, as otherwise the change was taking place twice so the file ended
   # up with TWO records like that.  The " no" pattern made the one unique.
   # That 2nd record was a combination of comments in the default original file.
   # Some lines ARE duplicated in the original config file, one is commented
   # out, the next one isn't.
   # Also, the spacing below is a little off so lines fit on the page.
   awk '/^#.*Port /                    { print "Port 22"; next };
        /^#.*Protocol /                { print "Protocol 2"; next };
        /^#.*LogLevel /                { print "LogLevel VERBOSE"; next };
        /^#PermitRootLogin /           { print "PermitRootLogin no"; next };
     /^#RhostsRSAAuthentication no / { print "RhostsRSAAuthentication no"; next };
        /^#HostbasedAuthentication / { print "HostbasedAuthentication no"; next };
```

```
        /^#.*IgnoreRhosts /             { print "IgnoreRhosts yes"; next };
        /^#.*PermitEmptyPasswords /     { print "PermitEmptyPasswords no"; next };
        /^#.*Banner /                   { print "Banner /etc/issue.net"; next };
                                        { print }' /etc/ssh/sshd_config-preCIS  \
                                                > $SSHD_CONFIG
   chown root:root $SSHD_CONFIG
   chmod 0600      $SSHD_CONFIG
   echo "diff $SSHD_CONFIG-preCIS $SSHD_CONFIG"
         diff $SSHD_CONFIG-preCIS $SSHD_CONFIG
else
   echo "OK - No $SSHD_CONFIG to secure."
fi
chmod -R 0400 $tmpcis/*
unset SSH_CONFIG SSHD_CONFIG CONFIGITEM
```

Scoring Status: **Scorable**

2.4 Enable System Accounting

Description:
System accounting is an optional process which gathers baseline system data (CPU utilization, disk I/O, etc.) every 10 minutes, by default. The data may be accessed with the `sar` command, or by reviewing the nightly report files named `/var/log/sa/sar*`. Once a normal baseline for the system has been established, with frequent monitoring - unauthorized activity (password crackers and other CPU-intensive jobs, and activity outside of normal usage hours) may be detected due to departures from the normal system performance curve.

Understandably system accounting provides benefits to System Administrators in regards to system functionality, performance, utilization, etc… as a monitoring activity (i.e. NOT prevention). An SysAdmin will use it to keep tabs on how well a system is functioning, and/or review such history as a normal part of their routine. When abnormalities occur here, it might be an understandable change, or an out-of-band indicator that some malicious activity has taken place. So this function can support normal auditing (i.e. auditd) not supplant it.

Note: By default, this data is only archived for one week before being automatically removed by the regular nightly `cron` job. Administrators may wish to independently archive the `/var/log/sa` directory on a regular basis to preserve this data for longer periods.
It is highly recommended to initiate a regular policy and procedure to utilize and review system accounting data to monitor system activity and prevent compromise.

Remediation:
Install package sysstat.

```
yum install sysstat
```

The tools provided include sar and iostat.

Scoring Status: **Scorable**

THIS PAGE INTENTIONALLY LEFT BLANK

3 Minimize xinetd network services

3.1 Disable Standard Services

Description:
On Linux, `inetd` has outpaced `xinetd` as the default network *superserver*. `xinetd` is no longer automatically installed, though is available for installation from the original media. `rpcbind`, for example, can execute without needing `xinetd`. Red Hat Enterprise Linux continues the Red Hat tradition of having `xinetd` available for some of the outdated and deprecated services, though it is reaching the point of being deprecated. The CIS Benchmarks recommend discontinuing its use as soon as possible.

Note: Not all of these services are deprecated, nor do some of them have ready secure alternatives.

3.1t - Table of xinetd services (generally, usage of these are deprecated)

// table current as of RHEL5.2 // {2009/03/17}		Default State	CIS Benchmark
	xinetd Service Name	(from Red Hat)	Recommendation
1	amanda	off	off
2	amandaidx	off	off
3	amidxtape	off	off
4	auth	off	off
5	chargen-dgram	off	off
6	chargen-stream	off	off
7	cvs	off	off
8	daytime-dgram	off	off
9	daytime-stream	off	off
10	discard-dgram	off	off
11	discard-stream	off	off
12	echo-dgram	off	off
13	echo-stream	off	off
14	eklogin	off	off
15	ekrb5-telnet	off	off
16	gssftp	off	off
17	klogin	off	off
18	krb5-telnet	off	off
19	kshell	off	off
20	ktalk	off	off
21	ntalk	off	off
22	rexec	off	off
23	rlogin	off	off
24	rsh	off	off
25	rsync	off	off
26	talk	off	off
27	tcpmux-server	off	off
28	telnet	off	off
29	tftp	off	off
30	time-dgram	off	off
31	time-stream	off	off
32	uucp	off	off

Description (cont'd):
The stock `inetd` and `xinetd` configurations have gotten better and better with each major release over the past years. In 1999, at the time of Red Hat 5.2 (this was *long* before RHEL 5.2), distributions offered many services which were either rarely-used or for which there were more secure alternatives. After enabling SSH, it is possible to do away with all `xinetd`-based services, since SSH provides both a secure login mechanism and a means of transferring files to and from the system. The hardening below will disable all standard services normally enabled in the Red Hat xinetd configuration.

When running these commands, one or more errors like this may be displayed:
```
error reading information on service xxx: No such file or directory
```

This is perfectly acceptable, as all it means is the software for that service was not installed.
The rest of the actions in this section give the administrator the option of re-enabling certain services. Rather than disabling and then re-enabling these services, experienced administrators may wish to simply disable only those services that they know are unnecessary for their systems. One size does not fit all---therefore, not all services shall have the same setting across all the systems in any given enterprise. If there is any doubt, it is better to disable everything, then re-enable one-by-one the necessary services based on the function of the server.

Remediation:
```
for SERVICE in    \
    amanda        \
    chargen       \
    chargen-udp   \
    cups          \
    cups-lpd      \
    daytime       \
    daytime-udp   \
    echo          \
    echo-udp      \
    eklogin       \
    ekrb5-telnet  \
    finger        \
    gssftp        \
    imap          \
    imaps         \
    ipop2         \
    ipop3         \
    klogin        \
    krb5-telnet   \
    kshell        \
    ktalk         \
    ntalk         \
    rexec         \
    rlogin        \
    rsh           \
    rsync         \
    talk          \
    tcpmux-server \
    telnet        \
    tftp          \
    time-dgram    \
    time-stream   \
    uucp;
```

```
do
    if [ -e /etc/xinetd.d/$SERVICE ]; then
         echo "Disabling SERVICE($SERVICE) - `ls -la /etc/xinetd.d/$SERVICE`."
         chkconfig ${SERVICE} off
    else
         echo "OK.  SERVICE doesn't exist on this system ($SERVICE)."
    fi
done
```

Scoring Status: **Scorable**

3.2 Configure TCP Wrappers and Firewall to Limit Access

Description:
Question:
Is there a reason to allow unlimited network access to this server?
If the answer to this question is no, then perform the remediation.
TCP Wrappers and Host-Based Firewalls are presented together as they are similar and complementary in functionality.

TCP Wrappers
By limiting access to the server, exposure to threats from attackers on remote systems is reduced. For Internet-connected servers that provide service to the whole Internet, limiting access may not make sense. Intranet servers, limited-access servers, and workstations should limit access to only authorized networks. To display which services are compiled with TCPwrappers support included, do this:

```
egrep libwrap /sbin/* /usr/sbin/* | sort
```

Many daemons (SSH for example) are compiled with TCP Wrapper support built-in, so use `/etc/hosts.allow` and `/etc/hosts.deny` to limit SSH access to the systems. The portmap daemon also uses TCP wrappers and there is a specific note to this effect in the default TCP wrappers config files.

Note: It is important to be aware that TCP wrappers looks at `hosts.allow` first, then `hosts.deny`, and controls access based on the first match. Omitting entries in `hosts.allow` and deny access to ALL in `hosts.deny`, will result in all access being blocked to all network clients.

Host-Based Firewalls
Host-based firewalls (also known as personal firewalls) have the following benefits:
Protection from compromised systems on the local network;
Defense in depth where an attacker must overcome both the border firewall and the host-based firewall to attack a system; extremely fine tuned control over what systems may or may not access the system.
The Center for Internet Security recommends installing a host-based firewall on workstations, and suggests end-users consider installing them on servers as well.
Workstations are defined as Red Hat Linux systems that offer no services to any external network or system. For example, a workstation that is running Apache and serving up content to the local network segment is not a workstation.

Host-based firewalls are available in `iptables` (installed by default) or via other commercial offerings. The Center for Internet Security makes no recommendations for a vendor or even a specific firewall configuration, as firewalls are very complex. Entire books have been written on `iptables` and are

outside the scope of this Benchmark. The default Red Hat `iptables` configuration is suitable for workstations and is a good starting point for servers. The Center for Internet Security does recommend using a tool (graphical- or text-based) to configure the `iptables` firewall, as manual rule configuration is extremely error-prone and you may end up with a false sense of security and have a less secure system.

The default system tool to configure the iptables-based firewall is `system-config-securitylevel`. This simple tool allows the administrator to manage (permit/deny) connections via a few services. By default, SSH is the only service enabled, when this is used.

See the following iptables resources:
Web-Based:
Linux Firewall Design Tool - http://linux-firewall-tools.com/linux/firewall/index.html

Package-Based:
FireHOL - http://firehol.sourceforge.net
Firewall Builder - http://sourceforge.net/projects/fwbuilder
GuardDog - http://www.simonzone.com/software/guarddog

Note: Inclusion of a tool on this list is not an endorsement or recommendation by the Center for Internet Security.

Remediation:

Note: Positively ensure remote access to the system is allowed, before configuring and implementing `deny-access` rules. Complete both parts of this section.

TCP Wrappers
To allow access from the authorized networks, refer to the `hosts.allow` man page and enter the service and the network in `/etc/hosts.allow`. At a minimum, allow `localhost` traffic. The following script will create a sample `hosts.allow` file that will allow access to the locally connected networks. Tailor this further to narrow traffic down to only what is appropriate for the network.

```
printf "ALL: localhost" >> /etc/hosts.allow
for I in `ifconfig | grep "inet addr" | cut -f2 -d: | cut -f1-3 -d"." \
    | grep -v ^127 | sort -n`
do
    echo   "Adding (, $I) to /etc/hosts.allow."
    printf ", $I." >> /etc/hosts.allow;
done
echo  >> /etc/hosts.allow
chown  root:root  /etc/hosts.allow
chmod  0644       /etc/hosts.allow
echo "diff /etc/hosts.allow-preCIS  /etc/hosts.allow"
      diff /etc/hosts.allow-preCIS  /etc/hosts.allow
```

Note: The above script assumes a netmask of `255.255.255.0`. If the system being worked on is within a different network context, then adjust `/etc/hosts.allow` for the environment.

Note: The above script ignores IPv6 networking. Additional hardening is necessary for any system/network which requires IPv6. The SNAC guidance from NSA (refer to Reference G, in Appendix D) has excellent coverage of IPv6 protections for RHEL5. IPv6 is enabled by default in RHEL5. To disable IPv6, add "`install ipv6 /bin/true`" into the "`/etc/modprobe.d/blacklist`" file, as that will prevent the ipv6 module from loading.

The following is an alternative script to get at the correct networks for the `hosts.allow` file:

```
for I in `route -n | tail -n +3 | sed -e 's/  */ /g'| cut -f1,3 -d ' '  \
      --output-delimiter=/ | grep -vE "^(0|169)" | sort -n`; do
      printf ", $I" >> /etc/hosts.allow;
done
echo >> /etc/hosts.allow
chown  root:root  /etc/hosts.allow
chmod  0644       /etc/hosts.allow
echo "diff /etc/hosts.allow-preCIS  /etc/hosts.allow"
      diff /etc/hosts.allow-preCIS  /etc/hosts.allow
```

Deny access to this server from all networks:

```
xyz="`tail -1 /etc/hosts.deny`"
if [ "$xyz" != "ALL: ALL" ]; then
     # Only make the change once
     echo  "ALL: ALL"  >>  /etc/hosts.deny
fi
chown  root:root  /etc/hosts.deny
chmod  0644       /etc/hosts.deny
echo "diff   /etc/hosts.deny-preCIS /etc/hosts.deny"
      diff   /etc/hosts.deny-preCIS /etc/hosts.deny
```

Review the resulting `/etc/hosts.allow` file to ensure it meets mission application needs. Test the configuration by logging in remotely.

It is recommended to further customize/harden the system configuration, though doing so is not further included in the scoring. For example, if the requirement is to ensure that only one IP address, 192.168.50.4, can access SSH on the server at 192.168.50.2, then follow the example below.
Change `/etc/hosts.allow` from:

```
ALL: localhost, 192.168.50.2/255.255.255.0
```

to:

```
sshd : 192.168.50.4
ALL EXCEPT sshd: localhost, 192.168.50.4/255.255.255.255
```

Further customization of TCP Wrappers is beyond the scope of this Benchmark.

Scoring Status: **Scorable**

3.3 Only Enable telnet If Absolutely Necessary

Description:
Question:
Is there a mission-critical reason that requires users to access this system via telnet, rather than the more secure SSH protocol?
If the answer to this question is yes, then perform the remediation.

`telnet` uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system.

The freely-available SSH utilities that ship with Red Hat Enterprise Linux (see http://www.openssh.com) provide encrypted network logins and should be used instead.

To aid in the migration to SSH, there is a freely available SSH client for Windows called `putty`, which is available from Simon Tatham (see http://www.chiark.greenend.org.uk/~sgtatham/putty). Additionally, there are numerous viable open-source and commercially supported SSH clients as well – check to see if the local Enterprise already has an Enterprise SSH client.

Some Enterprises are using `telnet` over SSL, however, the simpler and more standard solution is to use SSH. Configuring `telnet` over SSL is beyond the scope of a Level 1 Benchmark and will not be addressed here.

It is understood that large Enterprises deeply entrenched in using `telnet`, it may take considerable effort in migrating from `telnet` to `ssh`, so `telnet` may have to be enabled. When it can be disabled, simply run `chkconfig telnet off` to turn it off again.

This Benchmark scores `telnet` as a failure when it is active.

Remediation:
`chkconfig telnet on`

Scoring Status: **Scorable**

3.4 Only Enable FTP, If Absolutely Necessary

Description:
Question:
Is this machine an FTP server, or is there a mission-critical reason why data must be transferred to and from this system via an ftp server, rather than sftp or scp?
If the answer to this question is yes, then perform the remediation.

Note: Red Hat switched from distributing `wu-ftpd` to `vsftpd` after RHEL2.1 was released. For security reasons, as well as consistency with future Red Hat versions, consider replacing `wu-ftpd` with `vsftpd`. `vsftpd` is available on the Red Hat Enterprise Linux distribution media and is the standard, fully supported `ftp` daemon for RHEL5.

Like `telnet`, the `ftp` protocol is unencrypted, which means passwords and other data transmitted during the session can be captured by sniffing the network, and that the `ftp` session itself can be hijacked by an external attacker. Anonymous `ftp` servers are common for providing fast and easy downloading of publicly available files, however anonymous access should be configured to not allow uploading of files to the `ftp` server. `ftp` servers are also commonly used for Web Servers, but should be replaced by sftp if possible. `ftp` / `sftp` access should be chrooted to include the document root of the web site or the portion of the web site that the individual is responsible for. Of course, access to

the system configuration files and other web files is to be excluded from the chrooted environment. This is especially important if there are multiple web sites.

SSH provides two different encrypted file transfer mechanisms – `scp` and `sftp` – either of which should be used instead of the vanilla `ftp` client. Even if `ftp` is required, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols. For further information on restricting `ftp` access to the system, see section 8.2 below.
`

Note: Any directory writable by an anonymous `ftp` server should have its own partition. This helps prevent an `ftp` server from filling a hard drive used by other services.

To aid in the migration away from `ftp`, there are a number of freely available scp and sftp client for Windows, such as FileZilla from http://sourceforge.net/projects/filezilla and WinSCP available from http://winscp.sourceforge.net/eng/index.php which provides for a Graphical interface to putty, and pscp, which is a part of the previously mentioned putty package.

Some Enterprises are using `ftp` over SSL, however, the simpler and more standard solution is to use sftp. Configuring `ftp` over SSL, as well as demonstrating how to employ sftp, is beyond the scope of a Level 1 Benchmark and will not be addressed here.

Remediation:
```
chkconfig --levels 35 vsftpd on
```

Scoring Status: **Scorable**

3.5 Only Enable rlogin/rsh/rcp, If Absolutely Necessary

Description:
The r-commands suffer from the same hijacking and sniffing issues as telnet and ftp, and in addition have a number of well-known weaknesses in their authentication scheme. SSH was designed to be a drop-in replacement for these protocols. Given the wide availability of free SSH implementations, it seems unlikely that there is ever a case where these tools cannot be replaced with SSH (again, see http://www.openssh.com).

If these protocols are left enabled, please also see section 8.1 for additional security-related configuration settings.

Remediation:
Question:
Is there a mission-critical reason why rlogin/rsh/rcp must be used instead of the more secure ssh/scp?
If the answer to this question is yes, then perform the remediation.
```
chkconfig login on
chkconfig rlogin on
chkconfig rsh on
chkconfig shell on
```

Scoring Status: **Scorable**

3.6 Only Enable TFTP Server, If Absolutely Necessary

Description:
TFTP is typically used for network booting of diskless workstations, X-terminals, and other similar devices. Routers and other network devices may copy configuration data to remote systems via TFTP for backup. However, unless this system is needed in one of these roles, it is best to leave the TFTP service disabled.

Note: The tftp-server software is not installed by default on Red Hat Enterprise Linux. It must be manually selected for installation to use it. After installing it, perform the actions below.

Remediation:
Question:
Is this system a boot server or is there some other mission-critical reason why data must be transferred to and from this system via TFTP?
One possibility is a system used to serve OS builds over the network, via Red Hat PXEboot and anaconda/kickstart. In that case, the tftp service is necessary for initial PXE load of the boot image across the network.
If the answer to this question is yes, then perform the remediation.

```
chkconfig tftp on
if [ -e "/tftpboot" ] ; then
     chown -R root:root /tftpboot
     chmod -R 0744      /tftpboot
else
     mkdir -m 0744 /tftpboot && chown root:root /tftpboot
fi
```

Scoring Status: **Scorable**

4 Minimize boot services

The following table illustrates each of the services potentially available, natively, within RHEL5. The first nine (9) columns describe the service, by name and the default state per runlevel, as distributed by Red Hat. The next two rows show the CIS Benchmark recommendation for run levels 3 and 5, the multi-user modes for text and graphical environment respectively. This table accounts for services available natively through release 5.1---and is subject to change in future editions distributed by Red Hat. Services are recommended to be one of three states: "ON" (i.e. provides an essential function), "OFF" (i.e. recommended to be off as a general rule, unless production environment requires it) and "UD" (i.e. User Defined, which means that there isn't, necessarily, a security benefit either way if it is on or off).

Certainly many production environments will require additional services. The CIS Recommended defaults for each service are based upon a security, not operational, perspective. Arguably, some of these services can be installed to facilitate a successful production environment, but not universally across the enterprise. The basis for each CIS Recommendation is to heighten awareness of services being employed and to ensure each is for a valid, mission-critical, purpose. In other words, it isn't CIS's Recommendation to enable additional services just because it is convenient, or serves a need. Unless, that 'need' is **directly** tied to operational mission-criticality. Just because a desired service is not known to have a vulnerability or exploit does not means it is just 'ok' to install/use it. One of the main points of the Benchmark is to concentrate on including and securing *necessary* services and eliminating everything else.

Report on enabled services (that CIS Recommends be disabled) so that System Owners can make conscious decisions regarding what services are mission-critical and which might not be necessary, though convenient.

4t Table of RHEL5 inetd/boot Services

// table current as of RHEL5.1 // {2009/03/17}		Default State (from Red Hat)							CIS Benchmark Recommendation	
	inetd/boot Services	**boot state applicable to each runlevel**							**3**	**5**
1	acpid	0:off	1:off	2:off	3:on	4:on	5:on	6:off	UD	UD
2	amd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
3	**anacron**[2]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
4	apmd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
5	arptables_jf	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
6	arpwatch	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
7	atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
8	**auditd**	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
9	autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
10	avahi-daemon	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
11	avahi-dnsconfd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
12	bgpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
13	bluetooth	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
14	bootparamd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
15	capi	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off

[2] CIS recommends disabling anacron for systems which operate continuously

// table current as of RHEL5.1 // {2009/03/17}		Default State (from Red Hat)							CIS Benchmark Recommendation	
	inetd/boot Services	boot state applicable to each runlevel							3	5
16	conman	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
17	cpuspeed	0:off	1:on	2:on	3:on	4:on	5:on	6:off	off	off
18	**crond**	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
19	cups	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
20	cyrus-imapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
21	dc_client	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
22	dc_server	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
23	dhcdbd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
24	dhcp6s	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
25	dhcpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
26	dhcrelay	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
27	dovecot	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
28	dund	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
29	**firstboot**	0:off	1:off	2:off	3:on	4:off	5:on	6:off	**on**	**on**
30	gpm	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
31	haldaemon	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
32	hidd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
33	hplip	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
34	httpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
35	ibmasm	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
36	innd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
37	ip6tables[3]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
38	ipmi	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
39	**iptables**[4]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
40	irda	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
41	**irqbalance**[5]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
42	iscsi	0:off	1:off	2:off	3:on	4:on	5:on	6:off	UD	UD
43	iscsid	0:off	1:off	2:off	3:on	4:on	5:on	6:off	UD	UD
44	isdn	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
45	kadmin	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
46	kdump	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
47	kprop	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
48	krb524	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
49	krb5kdc	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
50	kudzu	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
51	ldap	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
52	lisa	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
53	lm_sensors	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
54	mailman	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
55	mcstrans	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
56	mdmonitor	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
57	mdmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
58	**messagebus**	0:off	1:off	2:off	3:on	4:on	5:on	6:off	**on**	**on**

[3] Enable ip6tables for systems with IPv6 network connectivity; its use is UD=User Defined
[4] Enable iptables for systems utilizing IPv6, but should leave it disabled for systems with only IPv4 network connectivity
[5] Preferably *on* for any multi-core or multi-processor system, optional for single-core/single processor systems

// table current as of RHEL5.1 // {2009/03/17}		Default State (from Red Hat)							CIS Benchmark Recommendation	
	inetd/boot Services	boot state applicable to each runlevel							3	5
59	microcode_ctl[6]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
60	multipathd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
61	mysqld	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
62	named	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
63	netfs	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
64	netplugd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
65	network[7]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
66	NetworkManager[8]	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
67	**NetworkManagerDispatcher**	0:off	1:off	2:off	3:off	4:off	5:off	6:off	**on**	**on**
68	nfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
69	nfslock	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
70	nscd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
71	**ntpd**	0:off	1:off	2:off	3:off	4:off	5:off	6:off	**on**	**on**
72	openibd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
73	ospf6d	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
74	ospfd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
75	pand	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
76	pcscd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
77	portmap	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
78	postfix	0:off	1:off	2:on	3:on	4:off	5:on	6:off	off	off
79	postgresql	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
80	privoxy	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
81	psacct	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
82	radiusd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
83	radvd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
84	rarpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
85	rdisc	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
86	**readahead_early**	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
87	**readahead_later**	0:off	1:off	2:off	3:off	4:off	5:on	6:off	UD	UD
88	**restorecond**[9]	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
89	rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	UD	UD
90	ripd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
91	ripngd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
92	rpcgssd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
93	rpcidmapd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
94	rpcsvcgssd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
95	rstatd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
96	rusersd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
97	rwhod	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
98	saslauthd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
99	sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD
100	setroubleshoot	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
101	smartd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	UD	UD

[6] Use of microcode_ctl is User Defined (UD) {*might only be necessary for x32 bit systems*--researching}
[7] The network is user defined, as CIS supports utilizing whichever state is appropriate for the mission (UD=User Defined)
[8] Preferably *off* for all systems without wireless NIC cards; enable it for systems with wireless connectivity
[9] Natively restores the SELinux context/condition to files; prevents files from being mis-labeled in their security context

// table current as of RHEL5.1 // {2009/03/17}		Default State (from Red Hat)							CIS Benchmark Recommendation	
	inetd/boot Services	**boot state applicable to each runlevel**							**3**	**5**
102	smb	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
103	snmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
104	snmptrapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
105	spamassassin	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
106	squid	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
107	**sshd**	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
108	**syslog**	0:off	1:off	2:on	3:on	4:on	5:on	6:off	**on**	**on**
109	**sysstat**	0:off	1:off	2:on	3:on	4:off	5:on	6:off	**on**	**on**
110	tog-pegasus	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
111	tomcat5	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
112	tux	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
113	vncserver	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
114	vsftpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
115	winbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
116	wpa_supplicant	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
117	xend	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
118	xendomains	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
119	xfs	0:off	1:off	2:on	3:on	4:on	5:on	6:off	off	off
120	xinetd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	off	off
121	ypbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
122	yppasswdd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
123	ypserv	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
124	ypxfrd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off
125	**yum-updatesd**	0:off	1:off	2:off	3:on	4:on	5:on	6:off	**on**	**on**
126	zebra	0:off	1:off	2:off	3:off	4:off	5:off	6:off	off	off

<end of table>

4.1 Set Daemon umask

Description:
This is a Level-II Benchmark recommendation in order to protect against Confidentiality leaks.

The system default `umask` should be set to at least `027` (allowed to be as high as `077`, with testing in the local environment) in order to prevent daemon processes (such as the `syslog` daemon) from creating world-writable files by default. If a particular daemon needs a less restrictive `umask`, consider editing that specific daemon startup script to grant that daemon the required `umask` while maintaining the increased server security posture for all the others.

Remediation:

```
sed 's/022/027/'  /etc/rc.d-preCIS/init.d/functions > /etc/rc.d/init.d/functions
echo "umask 027"  >> /etc/sysconfig/init

chown root:root   /etc/sysconfig/init
chmod 0755        /etc/sysconfig/init
echo "diff /etc/sysconfig/init-preCIS  /etc/sysconfig/init"
      diff /etc/sysconfig/init-preCIS  /etc/sysconfig/init
```

Scoring Status: **Scorable**

4.2 Disable xinetd, If Possible

Description:
If the actions in Section 3 of this Benchmark resulted in no services being enabled in the `inet` super daemon `/etc/xinetd.d`, then the `xinetd` service may be disabled completely on this system.

Experienced SysAdmins have learned the `inet` super daemon should be restarted after a change to its configuration file. This is not necessary in this case as the system will be rebooted and the change will take effect at that time.

This service is automatically ON by default, when it is installed.

Remediation:

```
echo "The 'chkconfig' status of 'xinetd' is shown before it is turned off and"
echo "then after so it can visually be compared."
echo "Note: The remaining chkconfig checks, in this hardening script, do the"
echo "same thing."
chkconfig  --list   xinetd
chkconfig  --level  12345  xinetd  off
chkconfig  --list   xinetd
```

Scoring Status: **Scorable**

4.3 Ensure sendmail is only listening to the localhost, If Possible

Description:
By default, the sendmail daemon on Red Hat systems listens on port 25/tcp for email messages from the local machine only. If the machine is not acting as an email server, then there should not be a reason for this system to receive incoming email messages from other hosts on the network. The check below ensures that the sendmail daemon is listening only on the internal "loopback" network for outgoing messages generated on the local system. This configuration prevents direct access to the sendmail daemon from external network devices and greatly reduces the impact of future sendmail vulnerabilities on the local machine.

Leaving sendmail in local-only mode permits mail to be sent out from the local system. If the local system will not be processing or sending any electronic mail, then the sendmail service should be completely disabled. If you completely disable sendmail for local use, messages sent to the root account, such as for cron job output or audit daemon warnings, will fail to be delivered properly unless submitted to a central email server.
That mail server must be configured to correctly handle email addressed directly to root, as well as to other users from the local machine.

As a viable alternative to sendmail, '`postfix`' is recommended for installation and use. Currently the inclusion and hardening of `postfix` is not included within this Benchmark.

(1) It is possible to run a Unix system with the `sendmail` daemon disabled and still allow users on that system to send email out from that machine.

(2) Although recent versions of Red Hat have set `sendmail` to listen only to the loopback network interface, this document still deactivates sendmail from operating in "daemon mode". Listening on the loopback interface still presents a slightly higher level of exposure to miscreant attack than not listening at all. Experienced administrators will understand that a chroot-jailed user or program can still properly interact with a `sendmail` process listening on the loopback interface.

Note: If the system is an email server, the administrator is encouraged to search the Web for additional insight on Sendmail security issues. Some information is available at:
http://www.deer-run.com/~hal/sysadmin/sendmail.html
http://www.deer-run.com/~hal/sysadmin/sendmail2.html
http://www.deer-run.com/~hal/sysadmin/greet_pause.html
http://www.deer-run.com/~hal/sysadmin/Sendmail-Unprivileged.html
http://www.sendmail.org

(3) When mail MTA services are not needed on the host, disable the mail server (sendmail, postfix, qmail, etc.). If mail services are required only to relay locally generated messages then configure the mail server to listen *only* on the loopback interface. When this host will act as a full fledged mail server then secure the configuration of the mail server as appropriate (insert links and pointers to secure configuration guidelines for various types of mail servers).

When sendmail is not configured in the site as the default site MTA, then bind the MTA to *only* the loopback device.

Audit:

```
grep MTA /etc/mail/sendmail.cf | grep "Addr=127.0.0.1, " | wc -l
```

Returns "1" when set up correctly (for the following context line from the `sendmail.cf` file)

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

Remediation:

Question:

Is this system a mail server – that is, does this machine receive and process email from other hosts?

Proceed with the appropriate actions below.

Yes – employment of sendmail:

```
cd /etc/sysconfig
cp -pf sendmail-preCIS sendmail
chown root:root sendmail
chmod 0644 sendmail
```

No – sendmail is not required:

```
echo "DAEMON=no"  > /etc/sysconfig/sendmail
echo "QUEUE=1h"  >> /etc/sysconfig/sendmail
chkconfig  --list   sendmail
chkconfig  --level  12345  sendmail off
chkconfig  --list   sendmail
chown root:root     /etc/sysconfig/sendmail
chmod 0644          /etc/sysconfig/sendmail
echo "diff /etc/sysconfig/sendmail-preCIS /etc/sysconfig/sendmail"
      diff /etc/sysconfig/sendmail-preCIS /etc/sysconfig/sendmail
```

Note: The email server need not be running to send outgoing mail.

Scoring Status: **Scorable**

4.4 Disable GUI Login, If Possible

Description:

There is usually no reason to run X Windows on a dedicated server machine, such as a dedicated web server. This action disables the graphical login, if present, leaving the user to login via SSH or a local text-based console. Even if the GUI login screen is deactivated (going back to run level 3), unprivileged users can still run X Windows by typing `startx` at the shell prompt. Doing so assumes the `xfs` service is running (which must be accomplished by root; see section 4.5).

In Red Hat Enterprise Linux, there are two predominant runlevels for operation. Runlevel 5 boots directly into X Windows, so as to allow graphical login or easy use of specialized X terminals and other convenient graphical tools. Otherwise, for normal text-based console login, runlevel 3 is desirable. GUI login is activated or deactivated by changing this runlevel in `/etc/inittab`.

Note: runlevel 3 allows a user to run X Windows (assuming the `xfs` service is running) by typing:

```
startx
```

Permissions on the `/etc/inittab` file are recommended at 0600, though they can be as open as 0644, if the system or a local application requires it, though this should be a rare exception.

Remediation:
Question:
Is there a mission-critical reason to run a GUI login program on this system?
If the answer to this question is no, proceed with the actions below.

```
echo "RunLevel was (`grep initdefault /etc/inittab | grep -v NOT`)."
sed  -e  's/id:5:initdefault:/id:3:initdefault:/'  /etc/inittab-preCIS  >
/etc/inittab
chown  root:root  /etc/inittab
chmod  0600       /etc/inittab
echo "diff /etc/inittab-preCIS /etc/inittab"
      diff /etc/inittab-preCIS /etc/inittab
echo "New runLevel will be (`grep initdefault /etc/inittab | grep -v NOT`)."
```

Scoring Status: **Scorable**

4.5 Disable X Font Server, If Possible

Description:
There's usually no reason to run X Windows on a dedicated server machine, like a dedicated web server. If an X server is not necessary on this machine, this action will deactivate the X font server (`xfs`) upon which X Windows is dependent. The X font server isn't used by any other process. An unprivileged user cannot start the X font server, though. This must be accomplished by root.

Remediation:
Question:
Is there a mission-critical reason to run X Windows on this system?
If the answer to this question is no, proceed with the actions below.

```
chkconfig  --list   xfs
chkconfig  --level  12345  xfs  off
chkconfig  --list   xfs
```

Scoring Status: **Scorable**

4.6 Disable Standard Boot Services

Description:
Every system daemon should have a clear and compelling purpose, in order to be executing on the host. Otherwise it should be deactivated, and to the greatest extent possible, removed. This greatly reduces the chances that the machine will be running a vulnerable daemon when the next vulnerability is discovered in its operating system.

Red Hat Enterprise Linux uses a facility called chkconfig to manage all the SysV rc-scripts. `chkconfig` adds or deletes links in each of the appropriate runlevel directories (`/etc/rc.d/rc*.d`) to activate or deactivate each of the rc-scripts.

This process "`chkconfig's`" all of the rc-scripts off, so that the local administrator can easily reactivate any of these scripts upon discovery of a mission-critical need for one of these services. One could reactivate the daemon script by typing `chkconfig` daemon on in most cases, which activates it in runlevels 2 through 5. If one of these runlevels is undesirable, like runlevel 2 for the NFS script, or the script needs to run in one of the other available runlevels, `chkconfig` takes the argument "`--level <levels>`" where one can explicitly specify runlevels that it should act on.

Note: The vendor patches may restore some of the original entries in the startup script directories `/etc/rc.d/rc*.d` – it is always a good idea to check these boot directories and remove any scripts that may have been added by the patch installation process. This would be a good time to ensure this check is in the local Enterprise OS Upgrade Procedure.

The rest of the actions in this section give the administrator the option of re-enabling certain services – in particular, the services that are disabled in the second loop in the "Action" section below. Rather than disabling and then re-enabling these services, experienced administrators may wish to simply disable only those services that they know are unnecessary for their systems.

The third loop in the "Action" section locks daemon-user accounts related to servers that we examine by setting a lockout password. This will not prevent a given daemon from running as these users – it simply confirms that these users are not available for human login. It also changes the shell to `/sbin/nologin` (standard for most service accounts under RHEL5) for an additional layer of security as long as shell access is not necessary.

Note: Not all of the scripts listed below will exist on all systems, as this is a superset of the available rc-scripts in the various Red Hat distribution versions. The Benchmark's recommended action will register some trivial errors on each distribution version as a result – these are not cause for alarm.

Note: Be very careful in regards to the `network` service if/when performing these hardening activities remotely or for systems that require connectivity. Generally, for any system that requires network connectivity at all, leave the `network` service enabled and active.

Remediation:

```
telinit 3
```

Once logged back in as root:

```
echo " When doing this from within X windows the display will slow to a horrible"
echo " crawl as soon as the xfs service is disabled.  Recommend doing this"
echo " script from init 3 (runlevel 3)."
# From a scripted perspective, this will be backwards from what the CIS Benchmark
# recommends.  Philosophy is to leave the few known/necessary services on, that
# do remain in the minimialized baseline, and then as each other step/procedure
# below is covered, it will disable what we know we don't need for a secure and
# hardened baseline.
#
# The following services ARE stopped/disabled using the following effort for the
# baseline:
#
# This affects network/NFS mapping during system building and/or during kickstart
# %post processing.
#     autofs
#     automount
#     iptables
#     portmap
#     NFS services
#     NFS statd
#     system message bus
```

```
# ** Warning** Disabling 'nfs' at this point in the script forcefully unmounts
#              any NFS network mounts.
# The following services should normally be enabled, unless there is a compelling
# reason not to:  (which is why this hardening section does not alter their state)

   for SERVICE in                \
       acpid                     \
       amd                       \
       anacron                   \
       apmd                      \
       arptables_jf              \
       aprwatch                  \
       atd                       \
       autofs                    \
       avahi-daemon              \
       avahi-dnsconfd            \
       bpgd                      \
       bluetooth                 \
       bootparamd                \
       capi                      \
       conman                    \
       cups                      \
       cyrus-imapd               \
       dc_client                 \
       dc_server                 \
       dhcdbd                    \
       dhcp6s                    \
       dhcpd                     \
       dhcrelay                  \
       dovecot                   \
       dund                      \
       firstboot                 \
       gpm                       \
       haldaemon                 \
       hidd                      \
       hplip                     \
       httpd                     \
       ibmasm                    \
       ip6tables                 \
       ipmi                      \
       irda                      \
       iscsi                     \
       iscsid                    \
       isdn                      \
       kadmin                    \
       kdump                     \
       kprop                     \
       krb524                    \
       krb5kdc                   \
       kudzu                     \
       ldap                      \
       lisa                      \
       lm_sensors                \
       mailman                   \
       mcstrans                  \
       mdmonitor                 \
       mdmpd                     \
       microcode_ctl             \
       multipathd                \
```

```
    mysqld                  \
    named                   \
    netfs                   \
    netplugd                \
    NetworkManager          \
    nfs                     \
    nfslock                 \
    nscd                    \
    ntpd                    \
    openibd                 \
    ospf6d                  \
    ospfd                   \
    pand                    \
    pcscd                   \
    portmap                 \
    postgresql              \
    privoxy                 \
    psacct                  \
    radvd                   \
    rarpd                   \
    rdisc                   \
    readahead_early         \
    readahead_later         \
    rhnsd                   \
    ripd                    \
    ripngd                  \
    rpcgssd                 \
    rpcidmapd               \
    rpcsvcgssd              \
    rstatd                  \
    rusersd                 \
    rwhod                   \
    saslauthd               \
    setroubleshoot          \
    smartd                  \
    smb                     \
    snmpd                   \
    snmptrapd               \
    spamassassin            \
    squid                   \
    tog-pegasus             \
    tomcat5                 \
    tux                     \
    winbind                 \
    wine                    \
    wpa_supplicant          \
    xend                    \
    xendomains              \
    ypbind                  \
    yppasswdd               \
    ypserv                  \
    ypxfrd                  \
    zebra;
do
     if [ -e /etc/init.d/$SERVICE ]; then
          # Doing business this way causes less needless errors that a
          # reviewer of the hardening process doesn't need to deal with.
          service $SERVICE stop
          chkconfig  --level  12345  $SERVICE  off
```

```
        else
             echo "SERVICE doesn't exist on this system ($SERVICE)."
        fi
done
```

Scoring Status: **Scorable**

4.7 Only Enable SMB (Windows File Sharing) Processes, If Absolutely Necessary

Description:
Red Hat Enterprise Linux includes the popular Open Source Samba server for providing file and print services to Windows-based systems. This allows a Unix system to act as a file or print server in on a Windows network, and even act as a Domain Controller (authentication server) to older Windows operating systems. However, if this functionality is not required by the site, the service should be disabled.
This section removes the SMB client software as well. If there is a mission-oriented reason to mount Windows Shares, do not remove the packages: `samba-client` and `samba-common`.

Remediation:
Question:
Is this machine sharing files via the Windows file sharing protocols?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig smb on
```

Scoring Status: **Scorable**

4.8 Only Enable NFS Server Processes, If Absolutely Necessary

Description:
NFS is frequently exploited to gain unauthorized access to files and systems. Clearly there is no need to run the NFS server-related daemons on hosts that are not NFS servers of vital mission application filesystems. If the system *is* an NFS server, the administrator should take reasonable precautions when exporting file systems, including restricting NFS access to a specific range of local IP addresses and exporting file systems "read-only" to the greatest extent possible. For more information, consult the `exports` manual page. Additionally, the following services are necessary to be enabled: `nfs`, `nfslock`, `portmapper` and `rpc`.

Remediation:
Question:
Is there a mission-critical reason why this machine must serve as an NFS file server?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig --level 35 nfs on
chkconfig --level 35 nfslock on
chkconfig --level 35 portmapper on
chkconfig --level 35 rpc on
```

Scoring Status: **Scorable**

4.9 Only Enable NFS Client Processes, If Absolutely Necessary

Description:
Again, unless there is a significant need for this system to acquire data via NFS, administrators should disable NFS-related services.

Note: Other file transfer schemes (such as `rdist` via SSH) can often be preferable to NFS for certain applications.

Remediation:
Question:
Is there a mission-critical reason why this system must access file systems from remote servers via NFS?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig --level 35 nfslock on
```

Scoring Status: **Scorable**

4.10 Only Enable NIS Client Processes, If Absolutely Necessary

Description:
Unless this site must use NIS, it should really be avoided. While it can be very useful for simplifying and transparently scaling the management for a large number of workstations (and servers), it's not well designed for security. Even Sun Microsystems is phasing out NIS+ in favor of LDAP for naming services – NIS and NIS+ are now reaching end of life. Where possible, utilize LDAP.

Remediation:
Question:
Is there a mission-critical reason why this machine must be an NIS client?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig ypbind on
```

Scoring Status: **Scorable**

4.11 Only Enable NIS Server Processes, If Absolutely Necessary

Description:
Unless this site must use NIS, it should be avoided. While it can be very useful for transparently scaling the number of workstations, it is not well designed for security.

Remediation:
Question:
Is there a mission-critical reason why this machine must be an NIS server?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig ypserv on
chkconfig yppasswdd on
```

Scoring Status: **Scorable**

4.12 Only Enable RPC Portmap Process, If Absolutely Necessary

Description:
RPC-based services typically use very weak or non-existent authentication and yet may share very sensitive information. Unless one of the services listed above is required on this machine, best to disable RPC-based tools completely. If there is uncertainty in whether or not a particular third-party application requires RPC services, consult with the application vendor.

Remediation:
Question:
Are any of the following statements true?
• This machine is an NFS client or server. This machine is an NIS (YP) or NIS+ client or server
• The machine runs a third-party software application which is dependent on RPC support

If the answer to both of these questions is yes, proceed with the actions below.
```
chkconfig --level 35 portmap on
```

Scoring Status: **Scorable**

4.13 Only Enable netfs Script, If Absolutely Necessary

Description:
If there are no network file sharing protocols being used, one can deactivate the `netfs` script. This script mounts network drives on the client. Though this is not a persistent daemon and thus not so dangerous, thinning out the `/etc/rc.d/rcN.d` directories makes the system much easier to audit.

Remediation:
Question:
Is this machine sharing files via the NFS, Novell Netware or Windows file sharing protocols?
If the answer to this question is yes, proceed with the actions below.
```
chkconfig --level 35 netfs on
```

Scoring Status: **Scorable**

4.14 Only Enable Printer Daemon Processes, If Absolutely Necessary

Description:
If users will never print files from this machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable the print daemon, `lpd` or `cupsd`, and removed the relevant packages from the system. The Unix print servers have generally had a poor security record – be sure to keep up-to-date on vendor patches, if such services are required.

Note: This item also sets `cupsd`, when present, to run as a non-root user and group, namely user `lp` and group `sys`; which is more secure.

Remediation:
Question:
Is this system a print server, or is there a mission-critical reason why users must submit print jobs from this system?

If the answer to this question is yes, proceed with the actions below.

```
if [ -e /etc/init.d/cups ]; then
    echo "Enable appropriate cups permissions and ownership"
    sed -e 's/^\#User lp/User lp/' -e 's/^\#Group sys/Group sys/'  \
           /etc/cups/cupsd.conf-preCIS  >  /etc/cups/cupsd.conf
    chown lp:sys /etc/cups/cupsd.conf
    chmod 0600   /etc/cups/cupsd.conf
    echo "diff /etc/cups/cupsd.conf-preCIS /etc/cups/cupsd.conf"
          diff /etc/cups/cupsd.conf-preCIS /etc/cups/cupsd.conf
    chkconfig cups on
fi

# If this system does need printing capabilities, but does not need to act as a
# print server, then configure the /etc/cups/client.conf file with the
# "ServerName" directive, pointing to a system running the cups server
echo "ServerName printserver.yourdomain.com" >> /etc/cups/client.conf
chown root:lp /etc/cups/client.conf
chmod 0644    /etc/cups/client.conf
echo "diff /etc/cups/client.conf-preCIS /etc/cups/client-conf"
      diff /etc/cups/client.conf-preCIS /etc/cups/client-conf
```

Replace "printserver.yourdomain.com" with an appropriate FQDN.

If the answer to this question is no, then remove the following, though some of these packages might or might not be installed, depending upon how the system was built:

```
rpm -e bluez-utilz-cups
rpm -e cups
rpm -e libgnomecups
rpm -e cups-libs
rpm -e hal-cups-utils
```

Scoring Status: **Scorable**

4.15 Only Enable Web Server Processes, If Absolutely Necessary

Description:
Even if this machine is a web server, the local site may choose not to use the web server provided with Linux in favor of a locally developed and supported Web environment.

Remediation:
Question:
Is there a mission-critical reason why this system must run a Web server on this system?

Web Servers should be run on dedicated systems serving only as web server. Unfortunately web servers tend to be enabled on many systems that don't need the web service, and are often not properly secured and administered. If Apache (the default web server) is required, review and apply the CIS Apache Benchmark available at http://www.cisecurity.org/bench_apache.html.

Note: The Red Hat Enterprise Linux uses `piranha` to administer the Linux Virtual Server software, which requires `httpd` and `php`.

If this is not a web server, and are not using `piranha`, the answer is no.

If the answer to this question is yes, proceed with the actions below.

When Apache is used, apply appropriate recommendations from the CIS Apache Benchmark.

Please read the discussion before executing these commands and select the appropriate one(s).
`chkconfig httpd on`

Scoring Status: **Scorable**

4.16 Only Enable SNMP Processes, If Absolutely Necessary

Description:
If SNMP is used to monitor the hosts on this network, experts recommend changing the default community string used to access data via SNMP. On Red Hat Enterprise Linux systems, this parameter has already been changed to a reasonably secure setting in the file `/etc/snmp/snmpd.conf`:
`com2sec notConfigUser default public`

No further action is required.

Note: In a large Enterprise that relied heavily on SNMP, it was discovered during the Linux rollout that SNMP was not a critical service, and not having it enabled increased the security posture of the servers. When using HP hardware with the HP provided health monitoring tools, SNMP and WBEM are the only options for reporting currently (and SNMP is the more granular). Because of this some organizations may require it.

Remediation:
Question:
Are hosts at this site remotely monitored by a tool (e.g., HP OpenView, MRTG, Cricket) that relies on SNMP? If the answer to this question is yes, proceed with the action:
`chkconfig snmpd on`

Scoring Status: **Scorable**

4.17 Only Enable DNS Server Process, If Absolutely Necessary

Description:
Most of the machines in the organization do not need a DNS server running on the box. Unless this is one of the organization's name servers, it is safe to shut this down.

If this must be left active, please patch often and security harden the configuration according to the CIS BIND Benchmark which provides detailed implementation and configurations recommendations. Two highly suggested configuration is to bind the DNS server program in a chroot environment, and run it as a non-root user. This significantly restricts the resources that the DNS server has access to on the system, reducing this set to the minimum required for the program to function properly. Carefully consider the consequences that if a name server is compromised then traffic that depends on the name service such as web, ftp and e-mail can be redirected to malicious servers.

Additionally, consider the use of Access Control Lists (ACL's) in `/etc/named.conf` to limit who can query the name server. For example, Internal name servers should not respond to outside requests. Large Enterprises run multiple name servers so this should not be an issue. However, smaller organizations may not be able to deploy both internal and external name servers and should instead use an reputable externally hosted DNS service. Details on how to accomplish this are provided in the CIS BIND Benchmark, available at http://www.cisecurity.org/bench_bind.html

Remediation:
Question:
Is this machine a DNS server, or name server, for this site?
If the answer to this question is yes, proceed with the actions below.
Download and following the appropriate configurations from the CIS BIND Benchmark, then enable the BIND as follows.

```
chkconfig named on
```

Scoring Status: **Scorable**

4.18 Only Enable SQL Server Processes, If Absolutely Necessary

Description:
If this machine does not need to run the mainstream database (SQL) servers PostgresSQL or MySQL, it is safe to deactivate them. If they must be enabled, issue the command (below) for the database that is installed.

Additional hardening of SQL functionality and security can and should be accomplished, though are outside the scope of this Level I Benchmark. Such actions include utilizing a strong password of sufficient complexity, limiting access to the database administrative accounts, etc…

Remediation:
Question:
Is this machine an SQL (database) server?
If the answer to this question is yes, proceed with the actions below.
Please read the discussion before executing these commands and select the appropriate command.

```
chkconfig postgresql on
chkconfig mysqld on
```

Scoring Status: **Scorable**

4.19 Only Enable Squid Cache Server, If Absolutely Necessary

Description:
Squid can actually be beneficial to security, as it imposes a proxy between the client and server. On the other hand, if it is not being used, it should be deactivated and removed. This deactivation decreases the risk of system compromise should a security vulnerability later be discovered in Squid. Finally, for any site that uses Squid, configure it carefully. Many Squid caches are badly configured to either allow outsider attackers to probe internal machines through the firewall or to use the cache to hide their true source IP address from their target hosts. Each site should configure Squid to not allow people outside their perimeter to use the cache without authentication of some sort. A better

deployment for squid is on a server with no external-facing network interface (unless using it for a reverse web proxy, which is a very specific installation, and beyond the scope of this Benchmark).

Remediation:
Question:
Do you use the squid web cache to speed up web transactions?
If the answer to this question is yes, proceed with the actions below.

```
chkconfig squid on
```

Scoring Status: **Scorable**

4.20 Only Enable Kudzu Hardware Detection, If Absolutely Necessary

Description:
`kudzu` and `hald`/`udev` are Red Hat's hardware detection programs, which are normally set to run during system startup. Their functionality detects changes in hardware and, without demanding authentication of any sort, allows the user at the console to configure that hardware. This lack of authentication presents the primary danger – meaning, that any user sitting at the console during a reboot can configure any new devices added to the system, potentially in malicious ways.

This configuration is an unnecessary risk for most sites, with the exception of those that need to allow users to easily make hardware changes without having a root password. Sites in the exception class might need to allow students to connect external hard drives, backup drives or other potentially common external devices.
Even if this rc-script is deactivated, `kudzu` is still accessible. To run kudzu after installing new hardware, run `/etc/rc.d/init.d/kudzu start` at the shell prompt while logged in as root.

Another, security benefit would be to limit the runlevels `kudzu` is permitted to function at. Those systems normally operating at runlevel 3, should then only enable `kudzu` at the same runlevel.

Remediation:
Question:
Does the site absolutely need to allow users at the console to add hardware to the system?
If the answer to this question is yes, then perform the action below.

```
chkconfig --level 35 kudzu on
```

Scoring Status: **Scorable**

4.21 Only Enable cyrus-imapd, If Absolutely Necessary

Description:
{Formerly `IMAP`} {Formerly CIS 3.7, in v1.1}
Remote mail clients (like Eudora, Netscape Mail and Kmail) may retrieve mail from remote mail servers using IMAP, the Internet Message Access Protocol, or POP, the Post Office Protocol. If this system is a mail server that must offer this protocol, `cyrus-imapd` may be activated. `cyrus-imapd` activates an SSL-encrypted, and thus much safer, version of IMAP. Standard IMAP is not encrypted and allows an attacker to eavesdrop on all e-mails being transferred or to take over the connection. It may, based on which authentication method is used, allow an attacker to steal user passwords as well. It is recommended to generate a new SSL certificate.

Remediation:
Question:
Is this machine a mail server with a mission-critical reason to use imap to serve mail to remote mail clients? If the answer to this question is yes, proceed with the actions below.

```
chkconfig cyrus-imapd on
```

Scoring Status: **Scorable**

Additional References:
For more information, consult:
http://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/Deployment_Guide-en-US/s1-email-mua.html#s2-email-security.

4.22 Only Enable dovecot, If Absolutely Necessary

Description:
{Formerly `POP`} {Formerly CIS 3.8, in v1.1}
Remote mail clients (like Eudora, Netscape Mail and Kmail) may retrieve mail from remote mail servers using IMAP, the Internet Message Access Protocol, or POP, the Post Office Protocol. If this system is a mail server that must offer the POP protocol, `dovecot` may be activated.
`dovecot` activates an SSL-encrypted, and thus much safer, version of POP. Standard POP is not encrypted and thus allows an attacker to eavesdrop on all e-mails being transferred or to take over the connection. It may – based on which authentication method is used – allow an attacker to steal user passwords as well. POP-SSL suffers none of these problems. It is recommended to generate a new SSL certificate.

Remediation:
Question:
Is this machine a mail server with a mission-critical reason to use pop to serve mail to remote mail clients? If the answer to this question is yes, proceed with the actions below.

```
chkconfig dovecot on
```

Scoring Status: **Scorable**

Additional References:
For more information, consult:
http://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/Deployment_Guide-en-US/s1-email-mua.html#s2-email-security

THIS PAGE INTENTIONALLY LEFT BLANK

5 System Network Parameter Tuning

5.1 Network Parameter Modifications

Description:
For an explanation of some of these parameters, see `/Documentation/networking/ip-sysctl.txt` in the local copy of the kernel source (requires installing the kernel source RPMs); or read the latest from the cross-referencing Linux site:
http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt.

- **net.ipv4.tcp_max_syn_backlog = 4096**
  tcp_max_syn_backlog specifies the maximum number of incomplete tcp connection requests that will be remembered. When this system is under a syn flood, a larger number will increase its chance of being able to handle legitimate requests.

- **net.ipv4.tcp_syncookies = 1**
  With syncookies enabled, if we reach a point where there are more than 4096 incomplete connections (highly unlikely under normal loads), this system will change how it responds to new connection requests. Instead of remembering all new connections, it sends out a coded response (the "syncookie") and completely forgets that the connection request came in at all. If the client actually completes the connection request with the third ACK packet, the server can see the cookie coming back and can then rebuild the connection in memory. The remaining connection requests (the syn flood packets) will never send this third ACK packet, so the server now has a way to hold legitimate conversations without tying up huge amounts of memory and processor time handling the flood. When syncookies are turned on and we overflow the above backlog, the excess connections are completed, but we lose the ability to use TCP extensions for those connections. This may result in some performance hit for those connections, but the damage here is far less than the damage from the syn flood itself.

- **net.ipv4.conf.all.rp_filter = 1**
  Arriving packets get a simple check; is the packet arriving on the correct interface for its source address? In other words, would a response to this packet go back out the same interface? This simple routing table check can quickly handle some attempts at spoofing source addresses. The only reason why this might need to be left off is if your network using asymmetric routing. One example might be a satellite link where incoming packets arrive on an Ethernet interface, but outgoing packets go out through a modem.

- **net.ipv4.conf.all.accept_source_route = 0**
  This IP option specifies how incoming and outgoing packets get routed. While originally intended as a troubleshooting technique, it is used almost exclusively to exploit IP trust relationships with spoofed source packets, and should be disabled.

- **net.ipv4.conf.all.accept_redirects = 0**
  When disabled, this system will no longer accept ICMP Redirect messages. While these can be occasionally be legitimately used to temporarily patch an incorrect routing table on a host machine, malicious hosts can use these to force packets through a sniffer or invalid gateway. For hosts with correct routing tables, this type of packet only has malicious uses. For hosts with incorrect routing tables, ignoring these packets will only slightly impact network performance.

- **net.ipv4.conf.all.secure_redirects = 0**
  When enabled, this would allow redirects from local routers. It's disabled for the same reasons as the above; malicious hosts could lie about the source address for the redirect.

- **net.ipv4.conf.default.rp_filter = 1**
- **net.ipv4.conf.default.accept_source_route = 0**
- **net.ipv4.conf.default.accept_redirects = 0**
- **net.ipv4.conf.default.secure_redirects = 0**
  The previous settings (the "**net.ipv4.conf.all.***" settings) affect all interfaces that exist when the change is implemented at boot time. These "**net.ipv4.conf.default.***" make the same changes for any additional interfaces that are created later, such as hotplug USB or PCMCIA network cards.

- **net.ipv4.icmp_echo_ignore_broadcasts = 1**
  When set to ignore, this system will not respond to broadcast pings such as those used in Smurf attacks. The system will continue to respond to normal ping packets, just not participate in creating floods of echo replies.

Remediation:

```
cat <<END_SCRIPT  >>  /etc/sysctl.conf
# The following 11 lines added, per CIS Red Hat Enterprise Linux Benchmark sec 5.1:
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
END_SCRIPT
chown root:root /etc/sysctl.conf
chmod 0600      /etc/sysctl.conf
echo "diff /etc/sysctl.conf-preCIS /etc/sysctl.conf"
      diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Scoring Status: **Scorable**

See also SN.9 for additional security-related network tunings to be considered.

For additional insights, consult the following links:
http://ipsysctl-tutorial.frozentux.net/ipsysctl-tutorial.html
http://lwn.net/Articles/45386
http://www.gossamer-threads.com/lists/linux/kernel/653569
http://www.eth0.us/sysctl

5.2 Additional Network Parameter Modifications

Description:
For an explanation of some of these parameters, see `/Documentation/networking/ip-sysctl.txt` in the local copy of the kernel source or read the latest from the cross-referencing Linux site: http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt.

Remediation:
Question:
Is this system going to be used as a firewall or gateway to pass network traffic between different networks?
If the answer to this question is no, then perform the action below.

```
cat <<END_SCRIPT  >>  /etc/sysctl.conf
# The following 4 lines added, per CIS Red Hat Enterprise Linux Benchmark sec 5.2:
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.icmp_ignore_bogus_error_responses = 1
END_SCRIPT
chown root:root /etc/sysctl.conf
chmod 0600      /etc/sysctl.conf
echo "diff /etc/sysctl.conf-preCIS /etc/sysctl.conf"
      diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Scoring Status: **Scorable**

THIS PAGE INTENTIONALLY LEFT BLANK

6 Logging

The items in this section cover enabling various different forms of system logging in order to keep track of activity on the system. Because it is often necessary to correlate log information from many different systems (particularly after a security incident) experts recommend establishing some form of time synchronization 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.

6.1 Capture Messages Sent To syslog AUTHPRIV Facility

Description:
A great deal of important security-related information is sent via logging channels (e.g., network service startups, commands like `usermod` and `chage`, etc). The below action causes this information to be captured in the `/var/log/secure` file (which is only readable by the superuser). This file should be reviewed and archived on a regular basis.

The priority, within `syslog.conf` is one of the following words, in ascending order: `debug`, `info`, `notice`, `warning`, `warn` (same as `warning`), `error`, `err` (same as `error`), `crit`, `alert`, `emerg`, and `panic` (same as `emerg`).

Remediation:

```
if [ `grep -v '^#' /etc/syslog.conf | grep -v authpriv\.none | grep -c  \
     'authpriv'` -eq 0 ]; then
      echo "Established the following record in /etc/syslog.conf"
      echo "authpriv.*\t\t\t\t/var/log/secure"
      echo -e "authpriv.*\t\t\t\t/var/log/secure" >> /etc/syslog.conf
else
      echo "syslog OK.  Didn't have to change syslog.conf for authpriv; the"
      echo "following record is good:"
      grep "^authpriv" /etc/syslog.conf | grep '/var/log/secure'
fi
# Add record for 'auth.*', too, placing it after the authpriv record
if [ `grep -v '^#' /etc/syslog.conf | grep -c 'auth.\*'` -eq 0 ]; then
     ed /etc/syslog.conf  <<END_SCRIPT
1
/^authpriv
a
auth.*                                          /var/log/messages
.
w
q
END_SCRIPT
else
      echo "syslog OK.  Didn't have to change syslog.conf for auth.*; the"
      echo "following record is good:"
      grep 'auth.\*' /etc/syslog.conf
fi
chown root:root /etc/syslog.conf
# Original/default permissions are 0644.
chmod 0600      /etc/syslog.conf
echo "diff /etc/syslog.conf-preCIS /etc/syslog.conf"
      diff /etc/syslog.conf-preCIS /etc/syslog.conf
# Create the log file if it doesn't already exist.
```

```
touch /var/log/secure
chown root:root /var/log/secure
chmod 0600      /var/log/secure
echo "Restarting syslog service to immediately implement the latest configuration."
service syslog stop
service syslog start
```

Scoring Status: **Scorable**

6.2 Turn On Additional Logging For FTP Daemon

Description:
Red Hat Enterprise Linux already logs connections and all files transferred in vsftpd. The modifications below ensure all commands sent to the server are logged.

Remediation:

```
FILE=""
if [ -f /etc/vsftpd.conf ]; then
     FILE="/etc/vsftpd.conf"
else
     FILE="/etc/vsftpd/vsftpd.conf"
fi
if [ -f $FILE ]; then
    awk '/^#?xferlog_std_format/ \
        { print "xferlog_std_format=NO"; next };
    /^#?log_ftp_protocol/ \
        { print "log_ftp_protocol=YES"; next };
    { print }' ${FILE}-preCIS > ${FILE}
    if [ `egrep -c log_ftp_protocol ${FILE}` == 0 ]; then
        echo "log_ftp_protocol=YES" >> ${FILE}
    fi
    chown root:root $FILE
    chmod 0600      $FILE
    echo "diff ${FILE}-preCIS $FILE"
          diff ${FILE}-preCIS $FILE
else
     echo "OK - No /etc/vsftpd.conf."
fi
```

Scoring Status: **Scorable**

Additional References:
More information on NTP can be found at http://www.ntp.org and http://www.ibiblio.org/pub/Linux/docs/HOWTO/otherformats/html_single/TimePrecision-HOWTO.html.

6.3 Confirm Permissions On System Log Files

Description:
It is critical to protect system log files from being modified by unauthorized individuals. Also, certain logs contain sensitive data that should only be available to the System Administrator.

If any of the services that affect the below logs are required, please revisit this section to ensure the logs have the correct/secure permissions.
Note: The `chmod` command will display errors, when the file does not exist.

Remediation:

```
echo "Some errors MAY appear here for directories, logs and/or files not installed
on this system."
cd /var/log

# Part 1
echo "Extra---Ensure the btmp log file for 'lastb' is in place and with proper"
echo "        permissions."
touch /var/log/btmp
chown root:root  /var/log/btmp
chmod 0600       /var/log/btmp

echo "Before listing of the log directory [explicit]."
ls -la /var/log

# Part 2
echo "LogPerms Part 1."
for LogFile in \
    boot.log         \
    btmp             \
    cron             \
    dmesg            \
    ksyms            \
    httpd            \
    lastlog          \
    maillog          \
    mailman          \
    messages         \
    news             \
    pgsql            \
    rpmpkgs          \
    sa               \
    samba            \
    scrollkeeper.log \
    secure           \
    spooler          \
    squid            \
    vbox             \
    wtmp
do
    # This check allows only entries that exist to have permissions set.
    # Visually cleaner for the person running it.
    if [ -e ${LogFile} ]; then
         # Utilizing recursive here is harmless when applied to a single file.
         chmod -R  o-rwx  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done
echo "LogPerms Part 2."
for LogFile in \
    boot.log          \
    cron              \
    dmesg             \
    gdm               \
    httpd             \
    ksyms             \
    lastlog           \
```

```
    maillog           \
    mailman           \
    messages          \
    news              \
    pgsql             \
    rpmpkgs           \
    samba             \
    sa                \
    scrollkeeper.log  \
    secure            \
    spooler           \
    squid             \
    vbox
do
    if [ -e ${LogFile} ]; then
         chmod -R  g-w  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done

echo "LogPerms Part 3."
for LogFile in \
    boot.log          \
    cron              \
    httpd             \
    lastlog           \
    maillog           \
    mailman           \
    messages          \
    pgsql             \
    sa                \
    samba             \
    secure            \
    spooler
do
    if [ -e ${LogFile} ]; then
         chmod -R  g-rx  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done

echo "LogPerms Part 4."
for LogFile in \
    gdm         \
    httpd       \
    news        \
    samba       \
    squid       \
    sa          \
    vbox
do
    if [ -e ${LogFile} ]; then
         chmod -R  o-w  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done
```

```
echo "LogPerms Part 5."
for LogFile in \
    httpd      \
    samba      \
    squid      \
    sa
do
    if [ -e ${LogFile} ]; then
         chmod -R  o-rx  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done

echo "LogPerms Part 6."
for LogFile in \
    kernel     \
    lastlog    \
    mailman    \
    syslog     \
    loginlog
do
    if [ -e ${LogFile} ]; then
         chmod -R  u-x  ${LogFile}*
    else
         echo "LogFile didn't exist ($LogFile)."
    fi
done

echo "LogPerms Part 7."
# Removing group write permissions to btmp and wtmp
chgrp utmp btmp
chmod g-w btmp
chgrp utmp wtmp
chmod g-w wtmp
# Fixing "/etc/rc.d/rc.sysinit", as it unsecures permissions for wtmp.
awk '( $1 == "chmod" && $2 == "0664" && $3 == "/var/run/utmp" && $4 ==
"/var/log/wtmp" ) {
       print "chmod 0600 /var/run/utmp /var/log/wtmp"; next };
     ( $1 == "chmod" && $2 == "0664" && $3 == "/var/run/utmpx" && $4 ==
"/var/log/wtmpx" ) {
       print "  chmod 0600 /var/run/utmpx /var/log/wtmpx"; next };
     { print }'  /etc/rc.d-preCIS/rc.sysinit  >  /etc/rc.d/rc.sysinit
chown root:root /etc/rc.d/rc.sysinit

chmod 0700      /etc/rc.d/rc.sysinit
echo "diff /etc/rc.d-preCIS/rc.sysinit /etc/rc.d/rc.sysinit"
      diff /etc/rc.d-preCIS/rc.sysinit /etc/rc.d/rc.sysinit

echo "LogPerms Part 8."
[ -e news ]    && chown -R news:news news
[ -e pgsql ]   && chown postgres:postgres pgsql
[ -e squid ]   && chown -R squid:squid squid
[ -e lastlog ] && chmod 0600 lastlog
chown -R root:root .
echo ""

echo "Follow-on listing of the log directory [explicit]."
ls -la /var/log
```

Scoring Status: **Scorable**

6.4 Configure syslogd to Send Logs to a Remote LogHost

Description:
Remote logging is essential in detecting intrusion and monitoring several servers operating in concert. An intruder – once he/she has obtained root – can edit the system logs to remove all traces of the attack. If the logs are stored off the machine, those logs can be analyzed for anomalies and used for prosecuting the attacker.

Remediation:
In the script below, replace loghost with the proper name (FQDN, as necessary) of the loghost in this systems environment.

```
printf "# Following 6 lines added per CIS RHEL5 Benchmark sec 6.4  \
        kern.warning;*.err\t\t\t@loghost\n                          \
        *.info;mail.none;authpriv.none;cron.none\t@loghost\n       \
        *.emerg\t@loghost\n                                        \
        auth.*\t\t\t\t@loghost\n                                   \
        authpriv.*\t\t\t\t@loghost\n                               \
        local7.*\t@loghost\n "                  >>  /etc/syslog.conf
chown root:root /etc/syslog.conf
chmod 0600      /etc/syslog.conf
echo "diff /etc/syslog.conf-preCIS /etc/syslog.conf"
      diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Scoring Status: Scorable

7 File and Directory Permissions/Access

7.1 Add 'nodev' Option To Appropriate Partitions In /etc/fstab

Description:
Placing "nodev" on these partitions prevents non-administrative users from mounting unauthorized devices on any partitions that should not contain devices. There should be little need to mount devices on any partitions other than device entries established subordinate to /dev.

One notable exception, of course, is the case where system programs are being placed into "chroot jails" - these often require that several devices be created in the chroot directory. If using chroot jails on any of the machines, be careful with the nodev option.

Configuring filesystems to prevent abuse is an important step in securing a system. Where feasible filesystems should be mounted with the most restrictive set of permissions possible that still allows normal operation. The three most important restrictions are nodev (prevent devices from being created on this filesystem), nosuid (do not respect the suid bit on this filesystem) and noexec (do no execute files from this filesystem).

At a minimum the nodev option should be applied to all filesystems except / to prevent users from mounting unauthorized devices. There should be little need to mount devices on any filesystems other than /dev.

Remediation:
```
awk '( $3 ~ /^ext[23]$/ && $2 != "/" ) { $4 = $4 ",nodev" };          \
     { printf "%-26s %-22s %-8s %-16s %-1s %-1s\n",$1,$2,$3,$4,$5,$6 }' \
       /etc/fstab  >  $tmpcis/fstab.tmp2
# Kept  $tmpcis/fstab.tmp2  as input to the next step (CIS 7.2).
chown root:root /etc/fstab
chmod 0644      /etc/fstab
# Note: the diff IS not for the same pair of files, as this step is treated
# as an intermediary.  But, we'll show the users the damage done so far and
# they see the progress.
# When accomplishing this step standalone, send it to the /etc/fstab file.
echo "diff  /etc/fstab-preCIS  /etc/fstab"
      diff  /etc/fstab         $tmpcis/fstab.tmp2
chmod -R 0400 $tmpcis/*
```

Scoring Status: **Scorable**

7.2 Add 'nosuid' and 'nodev' Option For Removable Media In /etc/fstab

Description:
Removable media is one vector by which malicious software can be introduced onto the system. By forcing these file systems to be mounted with appropriate secure options, the administrator prevents users from bringing hostile programs onto the system via CDROMs, floppy disks, USB drives, etc.

Generally, many usb devices can be implemented and the OS will ignore settings in 'console.perms'. Therefore, the only solid way of preventing usb drives from mounting is via udev. On some Linux systems all mountable devices may be handled by /etc/fstab. In this case the instructions for

securing removable file systems are the same as in Section 7.1, the nodev, nosuid and optionally the noexec option should be added to each entry for a removable device in /etc/fstab.

RHEL 5 uses udev and the Hardware Abstraction Layer (HAL) daemon software to update the filesystem description table (/etc/fstab) based on a series of SGML policies located in /usr/share/hal/fdi. Editing these SHML files manually is beyond the scope of this Benchmark.

Some clarification on RHEL 5 behavior: because the action has changed significantly from RHEL 4. In RHEL 5 udev and hal cooperatively interact to mount inserted removable media. The policies governing the mounting come from a combination of the udev and hal config files. udev 's primary contribution is to create the device node, set device permissions and alert hal. hal executes the mount after referencing it's rules list. hal uses the /usr/libexec/hal-storage-mount program to perform the mount.

RHEL 5, by default, does the "right thing" when mounting removable media (mounts with nodev, nosuid and noexec options), however, auditing the behavior can be a challenge. The default mount options that are applied to all removable media mounts do _not_ appear in any of the hal rule files. The reason is that the mount options are coded into the /usr/libexec/hal-storage-mount program that executes the mount (review the source, or run strings on the binary and see the mount options "noexec, nosuid, nodev"). It appears that unless the mount option is specifically allowed for a given media type in the 20-storage-methods.fdi file then an unprivileged user cannot mount with that mount option. Therefore, since there does not appear to be any allowed mount options in the stock file to allow the overriding of the nodev and nosuid options it should be impossible for an unprivileged user to mount a device, even with suid or dev support.

Remediation:

```
# Part 1
# Additional devices this section 'might' consider could be a DVD or cd recorder
awk '( $2 ~ /^\/m.*\/(floppy|cdrom|corder)$/ )  &&  ( $4 !~ /,nodev,nosuid/ )  \
     { $4 = $4 ",nodev,nosuid" };                                               \
     { printf "%-26s%-22s%-8s%-16s %-1s %-1s\n",$1,$2,$3,$4,$5,$6 }'           \
     $tmpcis/fstab.tmp2  >  $tmpcis/fstab.tmp3
mv   $tmpcis/fstab.tmp3     /etc/fstab
chown root:root  /etc/fstab
chmod 0644       /etc/fstab
echo "diff /etc/fstab-preCIS /etc/fstab"
      diff /etc/fstab-preCIS /etc/fstab


# Part 2
fdiPATH='unknown'
if [ -e /usr/share/hal/fdi/95userpolicy ]; then
     # Apply this to RHEL AS4 system
     fdiPATH="/usr/share/hal/fdi/95userpolicy"
else
     if [ -e /usr/share/hal/fdi/policy/20thirdparty ]; then
          # apply this for RHEL5
          fdiPATH="/usr/share/hal/fdi/policy/20thirdparty"
     fi
fi
if [ "$fdiPATH" == 'unknown' ]; then
     echo "Neither path was available, fdi for hal NOT secured."
```

```
     echo "RHEL AS4: /usr/share/hal/fdi/95userpolicy"
     echo "RHEL5:    /usr/share/hal/fdi/polilcy/20thirdparty"
else
     echo "Placing floppycdrom.fdi at: ($fdiPATH)."
     cat <<END_SCRIPT >> $fdiPATH/floppycdrom.fdi
<?xml version="1.0" encoding="ISO-8859-1"?> <!-- -*- SGML -*- -->
<deviceinfo version="0.2">
  <!-- Default policies merged onto computer root object  -->
  <device>
    <match key="info.udi" string="/org/freedesktop/Hal/devices/computer">
      <merge key="storage.policy.default.mount_option.nodev"
type="bool">true</merge>
      <merge key="storage.policy.default.mount_option.nosuid"
type="bool">true</merge>
    </match>
  </device>
</deviceinfo>
END_SCRIPT
     chown root:root   $fdiPATH/floppycdrom.fdi
     chmod 0640        $fdiPATH/floppycdrom.fdi
     echo "Established $fdiPATH/floppycdrom.fdi"
fi
```

Scoring Status: **Scorable**

7.3 Disable User-Mounted Removable File Systems

Description:
In Red Hat Enterprise Linux, the pam_console PAM module gives the user at the console (the machine's true physical keyboard) temporarily enhanced privileges. This is configured through the `/etc/security/console.perms` file or `console.perms.d/50-default.perms`. Under the Red Hat-shipped settings, the console user is given ownership of the floppy and CD-ROM drive, along with a host of other devices.

Many of these devices correspond to removable media and thus represent a security risk. This item disables the enhanced privileges on these devices. Be aware that allowing users to mount and access data from removable media drives makes it easier for malicious programs and data to be imported onto the network or data to be removed from the server.

Remediation:
Question:
Is there a mission-critical reason to allow unprivileged users to mount CD-ROMs and floppy disk file systems on this system? If the answer to this question is no, then perform the action below.

```
cd /etc/security
   CONS_PERM_FILE="console.perms"
   DEF_FILE="console.perms.d/50-default.perms"
   # If the test below passes, the 2nd file is changed, not the first.
   # Need to protect both.
   test -f $DEF_FILE && CONS_PERM_FILE="$DEF_FILE"
# Each entry listed below will NOT be commented out in the "console.perms" file.
# The remaining entries in that file WILL be commented out and thus disabled
# post-reboot.
# Further, "memstick" and "diskonkey" were not part of the original CIS
# specification to be left alone, but have been included to tailor the hardened
```

```
# build for usage of normal system USB requirements (such as keyboards and mice).
awk '( $1 == "<console>" ) && ( $3 !~
/sound|fb|kbd|joystick|v4l|mainboard|gpm|scanner|memstick|diskonkey/ ) \
    { $1 = "#<console>" }; { print }' ${CONS_PERM_FILE}-preCIS > $CONS_PERM_FILE
# Virgin default permissions were 0644 & 0600 respectively...  Just noting the
difference.
chown root:root $CONS_PERM_FILE
chmod 0600      $CONS_PERM_FILE
echo "diff  ${CONS_PERM_FILE}-preCIS  $CONS_PERM_FILE"
      diff  ${CONS_PERM_FILE}-preCIS  $CONS_PERM_FILE
cd $cishome
```

Scoring Status: **Scorable**

7.4 Verify passwd, shadow, and group File Permissions

Description:
These are the default owners and access permissions for these files. It is worthwhile to periodically check these file permissions as there have been package defects that changed `/etc/shadow` permissions to 0644. Tripwire (http://www.tripwire.org/downloads/index.php) though it hasn't been updated since 2001, AIDE (http://sourceforge.net/projects/aide) – a successor to Tripwire, and zlister (http://www.ibiblio.org/pub/linux/system/admin/zlisterProduction-1.7a) are excellent products for alerting to changes in these files, and others throughout the filesystem.

Remediation:

```
ls -la /etc/group /etc/gshadow /etc/passwd   /etc/shadow
chown root:root   /etc/group   /etc/gshadow  /etc/passwd   /etc/shadow
chmod 0644        /etc/group   /etc/passwd
chmod 0400                                   /etc/gshadow  /etc/shadow

ls -la /etc/group /etc/gshadow /etc/passwd /etc/shadow
```

Scoring Status: **Scorable**

7.5 Ensure World-Writable Directories Have Their Sticky Bit Set

Description:
When the so-called "sticky bit" is set on a directory, then only the owner of a file may remove that file from the directory (as opposed to the usual behavior where anybody with write access to that directory may remove the file). Setting the sticky bit prevents users from overwriting each other's files, whether accidentally or maliciously, and is generally appropriate for most world-writable directories. However, consult appropriate vendor documentation before blindly applying the sticky bit to any world writable directories found in order to avoid breaking any application dependencies on a given directory. Alternatively, ensure such directories are not world-writeable.

Remediation:
The automated tool supplied with this Benchmark will flag world-writable directories that do not have the sticky bit set.

Administrators who wish to obtain a list of these directories may execute the following commands:

```
for PART in `awk '( $3 ~ "ext[23]" ) { print  $2 }'  /etc/fstab`;
do
     find $PART -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned.
Scoring Status: **Scorable**

7.6 Find Unauthorized World-Writable Files

Description:
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.

Generally removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation in order to avoid breaking any application dependencies on a given file.

Remediation:
Administrators who wish to obtain a list of the world-writable files currently installed on the system may run the following commands to identify them:

```
for PART in $( grep -v '^#' /etc/fstab | awk '( $3 ~ "ext[23]" ) { print $2 }' );
do
    find $PART -xdev -type f  \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned. If `grub.conf` shows up, its permissions will be adjusted in section 8.8.

Scoring Status: **Scorable**

7.7 Find Unauthorized SUID/SGID System Executables

Description:
The administrator should take care to ensure that no rogue or inappropriate set-UID programs/scripts have been introduced into the system. In addition, if possible, the administrator should accomplish a set-UID audit and reduction/elimination of those unnecessary to the systems functioning

The script below has the list of those binaries/scripts which come by default in the distributed OS as having SUID (**- --s --- ---**) and/or GUID (**- --- --s ---**) enabled.
All users primary group should be their user private group they are then granted membership in other groups as needed. Depending on the level of group interaction and security/integrity requirements of the documents all users are then set with an `007` or `027` default umask. File sharing spaces are designated by creating a folder owned by the group with the SGID bit set. This causes all files placed

in that folder to assume the group ownership of the folder regardless of the primary group of the creator. Ex. Jane, a member of the accounting group, creates a spreadsheet. The permissions on the spreadsheet in her home folder are `jane:jane 0640`. She then moves the file to the "`accounting`" folder which has permissions `root:accounting 4770`. The spreadsheet's new permissions should be `jane:accounting 0640`.

Remediation:
The automated testing tool supplied with this Benchmark will flag unexpected set-UID and set-GID applications on the system. Administrators who wish to obtain a list of the set-UID and set-GID programs currently installed on the system may run the following commands:

```
# Part1
echo "Generate list of SUID/SGID files that exist on the system..."
for PART in $( grep -v '^#' /etc/fstab | awk '($3 ~ "ext[23]" ) { print $2 }' );
do
    find $PART -xdev \( -perm -04000 -o -perm -02000 \) -print | sort  \
         >>  $tmpcis/CIS_7.7_f1
done

# Part2
for FILE in                             \
    /bin/mount                          \
    /bin/ping                           \
    /bin/ping6                          \
    /bin/su                             \
    /bin/traceroute                     \
    /bin/traceroute6                    \
    /bin/umount                         \
    /media/.hal-mtab-lock               \
    /sbin/mount.nfs                     \
    /sbin/mount.nfs4                    \
    /sbin/netreport                     \
    /sbin/pam_timestamp_check           \
    /sbin/pwdb_chkpwd                   \
    /sbin/umount.nfs                    \
    /sbin/umount.nfs4                   \
    /sbin/unix_chkpwd                   \
    /usr/X11R6/bin/Xorg                 \
    /usr/bin/at                         \
    /usr/bin/chage                      \
    /usr/bin/chfn                       \
    /usr/bin/chsh                       \
    /usr/bin/crontab                    \
    /usr/bin/cu                         \
    /usr/bin/gataxx                     \
    /usr/bin/glines                     \
    /usr/bin/gnibbles                   \
    /usr/bin/gnobots2                   \
    /usr/bin/gnomine                    \
    /usr/bin/gnotravex                  \
    /usr/bin/gnotski                    \
    /usr/bin/gpasswd                    \
    /usr/bin/gtali                      \
    /usr/bin/iagno                      \
    /usr/bin/kgrantpty                  \
    /usr/bin/kon                        \
```

```
/usr/bin/kpac_dhcp_helper           \
/usr/bin/locate                     \
/usr/bin/lockfile                   \
/usr/bin/lppasswd                   \
/usr/bin/mahjongg                   \
/usr/bin/newgrp                     \
/usr/bin/newvc                      \
/usr/bin/passwd                     \
/usr/bin/rcp                        \
/usr/bin/rlogin                     \
/usr/bin/rsh                        \
/usr/bin/same-gnome                 \
/usr/bin/screen                     \
/usr/bin/sg                         \
/usr/bin/slocate                    \
/usr/bin/sperl5.8.5                 \
/usr/bin/ssh-agent                  \
/usr/bin/sudo                       \
/usr/bin/sudoedit                   \
/usr/bin/uucp                       \
/usr/bin/uuname                     \
/usr/bin/uuname                     \
/usr/bin/uustat                     \
/usr/bin/uux                        \
/usr/bin/wall                       \
/usr/bin/write                      \
/usr/bin/xterm                      \
/usr/kerberos/bin/ksu               \
/usr/lib/amanda/amqde               \
/usr/lib/amanda/calcsize            \
/usr/lib/amanda/dumper              \
/usr/lib/amanda/killpgrp            \
/usr/lib/amanda/planner             \
/usr/lib/amanda/rundump             \
/usr/lib/amanda/runtar              \
/usr/lib/cyrus-imapd/deliver        \
/usr/lib/mc/cons.saver              \
/usr/lib/mgetty+sendfax/faxq-helper \
/usr/lib/news/bin/inndstart         \
/usr/lib/news/bin/rnews             \
/usr/lib/news/bin/startinnfeed      \
/usr/lib/vte/gnome-pty-helper       \
/usr/libexec/openssh/ssh-keysign    \
/usr/libexec/pt_chown               \
/usr/libexec/utempter/utempter      \
/usr/lib64/vte/gnome-pty-helper     \
/usr/bin/locate                     \
/usr/bin/screen                     \
/usr/bin/Xorg                       \
/usr/lib/squid/ncsa_auth            \
/usr/lib/squid/pam_auth             \
/usr/libexec/libvirt_proxy          \
/usr/libexec/mc/cons.saver          \
/usr/libexec/openssh/ssh-keysign    \
/usr/libexec/utempter/utempter      \
/usr/sbin/amcheck                   \
/usr/sbin/ccreds_validate           \
/usr/sbin/exim                      \
/usr/sbin/gnome-pty-helper          \
```

```
    /usr/sbin/lockdev                   \
    /usr/sbin/postdrop                  \
    /usr/sbin/postqueue                 \
    /usr/sbin/sendmail.sendmail         \
    /usr/sbin/suexec                    \
    /usr/sbin/userhelper                \
    /usr/sbin/userisdnctl               \
    /usr/sbin/usernetctl                \
    /usr/sbin/utempter                  \
    /usr/sbin/uucico                    \
    /usr/sbin/uuxqt                     \
    /usr/sbin/utempter
do
    # Valid files with either SUID or SGID set are listed above, so this
    # next piece will remove them from what's been found.
    grep -v ${FILE} $tmpcis/CIS_7.7_f1 > $tmpcis/CIS_7.7_f2
    # Put the file back and continue searching
    /bin/cp -pf $tmpcis/CIS_7.7_f2 $tmpcis/CIS_7.7_f1
done
x=`wc -c $tmpcis/CIS_7.7_f1 | cut -d" " -f1`
if [ $x == 0 ]; then
     echo "($x) OK - No inappropriate SUID or SGID files found."
else
     sed 's/^.*/ls -lad &/'  $tmpcis/CIS_7.7_f1 > $tmpcis/CIS_7.7_f2
     echo "The following files have either the SUID and/or the SGID bit set."
     echo "These are not in the list of approved files/executables to have either"
     echo "of those bits set.  Recommend removing the SUID/SGID bits on them."
     /bin/bash $tmpcis/CIS_7.7_f2
fi
```

Scoring Status: **Scorable**

7.8 Find All Unowned Directories and Files

Description:
Investigate and do not allow any unowned directories and/or files on the system. Unowned entities may be an indication an intruder has accessed the system or improper package maintenance or installation. Sometimes a package removal results in unowned files or directories related to this software as the user/group associated with that package is removed, but that user's files (i.e., files changed after the package was installed) are left behind.

When users are removed from the system, a check for unowned directories and files should occur at that time, so that someone responsible for such information (programs, data, etc…) can rightfully assume ownership.

Another common cause is the installation of software that does not properly set file ownerships. Files in any NFS mounts should be investigated/researched as the user ID mapping between systems may be out of sync. If the local Enterprise uses a central user management system (NIS or LDAP), the presence of unowned files may indicate some other problem and should be investigated.

Remediation:

```
for PART in $(grep -v '^#' /etc/fstab | awk '( $3 ~ "ext[23]" ) { print $2 }' );
do
    find $PART -xdev -nouser -o -nogroup -print > $tmpcis/CIS_7.8_f1
done
sed 's/^.*/ls -lad &/'  $tmpcis/CIS_7.8_f1 > $tmpcis/CIS_7.8_f2
cat $tmpcis/CIS_7.8_f2
chmod -R 0400 $tmpcis/*
```

There should be no entries returned.
Scoring Status: **Scorable**

7.9 Disable USB Devices

Description:
USB drives and memory devices represent another attack vector against a system. The prices for a 1GB USB memory device, or larger, have become very affordable, and is enough storage to transport vast quantities of data off a system. Few servers have need for USB devices and this whole avenue should be disabled.

Another possible attack would be to have a bootable Linux system installed on the USB device. Most modern BIOS' allow booting from USB devices, so this would let a person with physical access to a server an extremely easy way take over a system and bypass some of the security being set up. See the discussion regarding floppy and CD-ROM drives in section 7.2.

For these reasons, should also disable USB in the system BIOS if possible.

Note: Hotplugger is required by `udev`, which is required by several other required packages, making very unlikely to be able to remove it. Therefore, for new Red Hat versions the `nousb` kernel boot argument should be employed to disable USB devices. The script below uses `grubby` to add the nousb kernel boot argument to the default kernel image. Adding nousb to other kernel images is also recommended. The `/etc/grub.conf` symbolic link may also be viewed or edited as well. The nousb argument is placed at the end of the lines starting with kernel, as shown below.

```
kernel /vmlinuz-2.6.xx ro root=LABEL=/  nousb
```

'The "`nousb`" argument to the kernel may also disable USB keyboards and mice. A potentially serious problem on legacy free systems that do not have PS2 connections or for systems using USB KVMs. An alternative remediation would be to insert the line "`install usb-storage /bin/true`" into `/etc/modprobe.conf`. This will disable USB storage devices by preventing the kernel module from loading".

Remediation:

```
DEF_KERN=$( grubby --default-kernel)
grubby --update-kernel=$DEF_KERN --args="nousb"
```

Scoring Status: **Scorable**

THIS PAGE INTENTIONALLY LEFT BLANK

8 System Access, Authentication, and Authorization

8.1 Remove .rhosts Support In PAM Configuration Files

Description:
Used in conjunction with the BSD-style "r-commands" (`rlogin`, `rsh`, `rcp`), the `.rhosts` files implement a *weak* form of authentication based on the network address or host name of the remote computer (which can be spoofed by a potential attacker to exploit the local system). Disabling .rhosts support helps prevent users from subverting the system's normal access control mechanisms. On a system with RHEL5, PAM documentation can be found under "`/usr/share/doc/pam-0.99.7.1/txts`".

If `.rhosts` support is required for some reason, some basic precautions should be taken when creating and managing `.rhosts` files. Never use the "`+`" wildcard character in `.rhosts` files. In fact, `.rhosts` entries should always specify a specific trusted host name along with the user name of the trusted account on that system (e.g., "trustedhost alice" and not just "trustedhost"). Avoid establishing trust relationships with systems outside of the organization's security perimeter and/or systems not controlled by the local administrative staff. Firewalls and other network security elements should actually block `rlogin`/`rsh`/`rcp` access from external hosts.

Finally, make sure that `.rhosts` files are only readable by the owner of the file (i.e., these files should be mode `0600`).

Remediation:
```
ls -la  /etc/pam.d/*  >  $tmpcis/CIS_8.1.Before.tmp
cd /etc/pam.d
for FILE in `find .  -type f -exec grep -l rhosts_auth {} \;`; do
    echo "Removing .rhosts support in ${FILE}."
    grep -v rhosts_auth $FILE > $tmpcis/${FILE}.tmp
    /bin/cp -f $tmpcis/${FILE}.tmp $FILE
    chown root:root $FILE
    chmod 0644      $FILE
done
ls -la  /etc/pam.d/*  >  $tmpcis/CIS_8.1.After.tmp
echo "The following entries changed under '/etc/pam.d'"
echo "diff $tmpcis/CIS_8.1.Before.tmp $tmpcis/CIS_8.1.After.tmp"
      diff $tmpcis/CIS_8.1.Before.tmp $tmpcis/CIS_8.1.After.tmp
chmod -R 0400 $tmpcis/*
cd $cishome
```

Scoring Status: **Scorable**

8.2 Create ftpusers Files

Description:
`/etc/ftpusers` and `/etc/vsftp.ftpusers` contain a list of users who are not allowed to access the system via WU-FTPd and vsftpd, respectively. Generally, only normal users should ever access the system via FTP-there should be no reason for "system" type accounts to be transferring information via this mechanism. Certainly the root account should never be allowed to transfer files directly via FTP.

If vsftpd is used, it may be desirable to reverse the usage of the users file to be a list of users who ARE able to ftp to the server, instead of a list of users who are NOT able to ftp into the server. This provides greater control and safety in denying the ftp usage by default for users NOT listed. To reverse the meaning of the vsftpd users list file set userlist_deny=NO in the vsftpd.conf file. The script below attempts to check for the userlist_deny vsftpd setting and will not create or modify the default vsftpd user list file if the value is NO. It is important to carefully test the configuration after these changes to be sure that only the expected users are allowed to login via ftp.

Remediation:

```
if [ -f /etc/ftpaccess ]; then
   for NAME in `cut -d: -f1 /etc/passwd`; do
       if [ `id -u $NAME` -lt 500 ]; then
            echo $NAME >> /etc/ftpusers
       fi
   done
   chown root:root /etc/ftpusers
   chmod 0600      /etc/ftpusers
   echo "diff /etc/ftpusers-preCIS /etc/ftpusers"
         diff /etc/ftpusers-preCIS /etc/ftpusers

   VSFTP_CONF="/etc/vsftpd/vsftpd.conf"
     ALT_CONF="/etc/vsftpd/vsftpd.conf"
   test -f $ALT_CONF && VSFTP_CONF=$ALT_CONF
   if [ -e $VSFTP_CONF ] && ! grep -q "^userlist_deny=NO" $VSFTP_CONF; then
        /bin/cp -fp /etc/ftpusers /etc/vsftpd.ftpusers
        chown root:root /etc/vsftpd/vsftpd.conf
        chgrp 0600      /etc/vsftpd/vsftpd.conf
        [ -e /etc/vsftpd.ftpusers-preCIS ] && echo "diff /etc/vsftpd.ftpusers-
preCIS /etc/vsftpd.ftpusers"
        [ -e /etc/vsftpd.ftpusers-preCIS ] &&       diff /etc/vsftpd.ftpusers-
preCIS /etc/vsftpd.ftpusers
   fi
else
     echo "OK - No /etc/ftpaccess to tailor."
fi
```

Scoring Status: **Scorable**

8.3 Prevent X Server From Listening On Port 6000/tcp

Description:

X servers listen on port 6000/tcp for messages from remote clients running on other systems. However, X Windows uses a relatively insecure authentication protocol and an attacker who is able to gain unauthorized access to the local X server can easily compromise the system.

Invoking the "-nolisten tcp" option causes the X server not to listen on port 6000/tcp by default. This prevents authorized remote X clients from displaying windows on the local system as well. However, the forwarding of X events via SSH will still happen normally. This is the preferred and more secure method transmitting results from remote X clients in any event.

Remediation:

```
if [ -e /etc/X11/xdm/Xservers ]; then
    cd /etc/X11/xdm
    awk '( $1 !~ /^#/ && $3 == "/usr/X11R6/bin/X" ) { $3 = $3 " -nolisten tcp" };
    { print }' Xservers-preCIS > Xservers
    chown root:root Xservers
    chmod 0444      Xservers
    echo "diff Xservers-preCIS Xservers"
          diff Xservers-preCIS Xservers
    cd $cishome
else
    echo "No /etc/X11/xdm/Xservers file to secure."
fi
if [ -d /etc/X11/xinit ]; then
    cd /etc/X11/xinit
    if [ -e xserverrc ]; then
         echo "Fixing /etc/X11/xinit/xserverrc"
         awk '/X/ && !/^#/ { print $0 " :0 -nolisten tcp \$@"; next }; \
         { print }' xserverrc-preCIS > xserverrc
    else
         cat <<END_SCRIPT > xserverrc
#!/bin/bash
exec X :0 -nolisten tcp \$@
END_SCRIPT
    fi
    chown root:root xserverrc
    chmod 0755      xserverrc
    [ -e xserverrc-preCIS ] && echo "diff xserverrc-preCIS xserverrc"
    [ -e xserverrc-preCIS ] &&       diff xserverrc-preCIS xserverrc
    cd $cishome
else
    echo "No /etc/X11/xinit file to secure."
fi
```

Scoring Status: **Scorable**

8.4 Restrict at/cron To Authorized Users

Description:

The cron.allow and at.allow files are a list of users who are allowed to run the `crontab` and at commands to submit jobs to be run at scheduled intervals. On many systems, only the SysAdmin needs the ability to schedule jobs.

Note: Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user. `cron.allow` only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Remediation:

```
# With x.allow only users listed can use 'at' or 'cron'
# {where 'x' indicates either 'at' or 'cron'}
# Without x.allow then x.deny is checked, members of x.deny are excluded
# Without either (x.allow and x.deny), then only root can use 'at' and 'cron'
# At a minimum x.allow should exist and list root
echo "Attempting to list the following files for the 'before' picture."
echo "Any 'errors' are alright, as we are simply looking to see what exists."
```

```
ls -la /etc/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny
rm -f /etc/at.deny /etc/cron.deny
echo  root  >  /etc/at.allow
echo  root  >  /etc/cron.allow
chown  root:root  /etc/at.allow  /etc/cron.allow
chmod  0400       /etc/at.allow  /etc/cron.allow
if [ -e /etc/at.allow-preCIS ]; then
   echo "diff /etc/at.allow-preCIS  /etc/at.allow"
   diff /etc/at.allow-preCIS        /etc/at.allow
fi
if [ -e /etc/cron.allow-preCIS ]; then
   echo "diff /etc/cron.allow-preCIS  /etc/cron.allow"
   diff /etc/cron.allow-preCIS  /etc/cron.allow
fi
echo "Listing the state of these AFTER imposing restrictions..."
echo "Missing file 'errors' are ok here too."
ls -la /etc/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny
```

Scoring Status: **Scorable**

8.5 Restrict Permissions On crontab Files

Description:
The system `crontab` files are accessed only by the `cron` daemon (which runs with superuser privileges) and the `crontab` command (which is set-UID to root). Allowing unprivileged users to read or (even worse) modify system `crontab` files can create the potential for a local user on the system to gain elevated privileges.

Remediation:

```
ls -lad /etc/cron* /var/spool/cron*
chown  root:root  /etc/crontab
chmod  0400       /etc/crontab
chown  -R  root:root  /var/spool/cron
chmod  -R  go-rwx     /var/spool/cron
cd /etc
ls | grep cron | grep -v preCIS | xargs chown -R root:root
ls | grep cron | grep -v preCIS | xargs chmod -R go-rwx
cd $cishome
ls -lad /etc/cron* /var/spool/cron*
```

Scoring Status: **Scorable**

8.6 Restrict Root Logins To System Console

Description:
Anonymous `root` logins should *never* be allowed, except on the system console, and then, ONLY in emergency situations. At all other times, every administrator should access the system via an unprivileged account and use some authorized mechanism (such as the `su` command, or the freely-available `sudo` package) to gain additional privileges. These mechanisms provide an audit trail in the event of errors, problems and/or compromise.

Many Enterprises – who use serial port concentrators to connect to a server in a data center without physically having to use the keyboard – consider the serial port a console. This is in keeping with the

Unix server tradition of controlling headless Unix machines using a serial port console. Just like the virtual consoles, this one needs to be strongly protected as well. If this applies to the organization, execute either, or both of these lines, as needs dictate:

```
echo ttyS0 >> /etc/securetty
echo ttyS1 >> /etc/securetty
```

Remediation:

```
echo console > /etc/securetty
# These are acceptable for the GUI and runlevel 3, when trimmed down to 6
for i in `seq 1 6`; do
     echo vc/$i >> /etc/securetty
done
#
#### Commented this out to be more secure as it denies root logins to the physical
TEXT console.
#    Check pg 14 in Hardening Linux for additional safety in the /etc/inittab
file.
# Do we want this as a required argument submitted on the command line?
#
#  for i in `seq 1 6`; do
#       echo tty$i >> /etc/securetty
#  done
chown  root:root  /etc/securetty
chmod  0400       /etc/securetty
echo "diff /etc/securetty-preCIS /etc/securetty"
      diff /etc/securetty-preCIS /etc/securetty

# Part 2
# Second modification of gdm.conf, if it exists.
if [ -e /etc/X11/gdm/gdm.conf ]; then
     #### There is another file to consider: "/etc/X11/gdm/gdm.conf"
     # "AllowRoot=true" should be set to false to prevent root from logging in to
the gdm GUI.
     # "AllowRemoteRoot=true" should be set to false to prevent root logins from
remote systems.
     # Doing this change is supportive of logging in as a regular user and using
'su' to get to root.
     # Before allowing a reboot, ensure at least one account is created for a
SysAdmin type.
     cd /etc/X11/gdm
     /bin/cp -pf gdm.conf $tmpcis/gdm.conf.tmp
     sed -e 's/AllowRoot=true/AllowRoot=false/'             \
         -e 's/AllowRemoteRoot=true/AllowRemoteRoot=false/' \
         -e 's/^#Use24Clock=false/Use24Clock=true/'
         $tmpcis/gdm.conf.tmp  >  gdm.conf
     chown root:root gdm.conf
     chmod 0644      gdm.conf
     echo "diff gdm.conf-preCIS gdm.conf"
           diff gdm.conf-preCIS gdm.conf
     cd $cishome
else
    echo "No /etc/X11/gdm/gdm.conf file to further secure."
fi

# Part 3
echo "The following is only required when a serial console is used for this
server."
```

```
echo "Either of these would be added manually post-baseline compliance, depending"
echo "on the COM port the serial cable is physically attached to."
echo "#    echo ttyS0 >> /etc/securetty"
echo "#    echo ttyS1 >> /etc/securetty"
chmod -R 0400 $tmpcis/*
```

Scoring Status: **Scorable**

8.7 Set GRUB Password

Description:
An unprotected GRUB boot loader prompt allows an attacker with physical access to subvert the normal boot process very easily. The action below will allow the system to boot normally, only requiring a password when the anyone attempts to modify the boot process by passing commands to GRUB. Make sure to replace <password> in the actions below with an md5-hashed password (check the `man` page for `/sbin/grub-md5-crypt`).

Remediation:
1. Add this line to `/etc/grub.conf` before the first uncommented line:

```
password <password>
```

Replace <password> with an md5 encrypted password.
2. Execute the following commands as root:

```
chown root:root /boot/grub/grub.conf
chmod 0600      /boot/grub/grub.conf
```

Scoring Status: **Scorable**

8.8 Require Authentication For Single-User Mode

Description:
By default on Red Hat Enterprise Linux, a SysAdmin can enter single user mode simply by typing "`linux single`" at the GRUB boot-editing menu. Some believe that this is left in to ease support of users with lost root passwords. In any case, it represents a clear security risk – authentication should *always* be required for root-level access. It should be noted that it is extremely difficult to prevent compromise by any attacker who has knowledge, tools, and full physical access to a system.

This kind of measure, in a simple way, increases the difficulty of compromise by requiring more of each of these factors. These last two items have attempted to address concerns of physical/boot security. To make these preparations more complete, one should consider setting the BIOS to boot only from the main hard disk and locking this setting with a BIOS password.

For more information on reducing the threat posed by an attacker with physical/boot access, consider the article "Anyone with a Screwdriver Can Break In," available at:
http://www.bastille-linux.org/jay/anyone-with-a-screwdriver.html.

Remediation:

```
cd /etc
if [ "`grep -l sulogin inittab`" = "" ]; then
     awk '{ print }; /^id:[0123456sS]:initdefault:/ { print
"~~:S:wait:/sbin/sulogin" }' \
          inittab > $tmpcis/inittab.tmp
```

```
     /bin/cp -pf $tmpcis/inittab.tmp inittab
     chown root:root inittab
     chmod 0600      inittab
     echo "diff inittab-preCIS inittab"
          diff inittab-preCIS inittab
else
     echo "OK.  /etc/inittab already properly configured for Single-User"
     echo "Mode Authentication."
fi
cd $cishome
chmod -R 0400 $tmpcis/*
```

Scoring Status: **Scorable**

8.9 Restrict NFS Client Requests To Privileged Ports

Description:
Setting the secure parameter causes the NFS server process on the local system to ignore NFS client requests that do not originate from the privileged port range (ports less than 1024); and this is the default behavior for RHEL5. This should not hinder normal NFS operations but may block some automated NFS attacks that are run by unprivileged users.

Remediation:
Add the secure option to all entries in the `/etc/exports` file. The following embedded Perl code will perform this action automatically. This isn't necessary if there are no NFS exported filesystems.

```
echo "/etc/exports size is (`wc -c /etc/exports | cut -d' ' -f1`)."
if [ `wc -c /etc/exports | cut -d' ' -f1` == 0 ]; then
     echo "Ok - No changes were necessary to /etc/exports."
else
     echo "Size (for /etc/exports) is greater than 0"
     ls -la  /etc/export*
     perl -i.orig -pe 'next if (/^\s*#/ || /^\s*$/);
          ($res, @hst) = split(" ");
          foreach $ent (@hst) {
          undef(%set);
          ($optlist) = $ent =~ /\((.*?)\)/;
          foreach $opt (split(/,/, $optlist)) {
          $set{$opt} = 1;
          }
          delete($set{"insecure"});
          $set{"secure"} = 1;
          $ent =~ s/\(.*?\)//;
          $ent .= "(" .  join(",", keys(%set)) .  ")";
          }
          $hst[0] = "(secure)" unless (@hst);
          $_ = "$res\t" .  join(" ", @hst) .  "\n";'    /etc/exports
fi
chown root:root /etc/exports
chmod 0644      /etc/exports
echo "diff /etc/exports-preCIS /etc/exports"
      diff /etc/exports-preCIS /etc/exports
```

Scoring Status: **Scorable**

8.10 Only Enable syslog To Accept Messages, If Absolutely Necessary

Description:
By default the system logging daemon, `syslogd`, in Linux systems, does not listen for logging messages from other systems on network port 514/udp, and thus by default is more secure.

It is considered a good security management practice to set up one or more machines as central "log servers" to aggregate log traffic from all machines at a site. However, unless a system is set up to be one of these "log server" systems, it should not be listening on 514/udp for incoming log messages as the protocol used to transfer these messages does not include any form of authentication, so a malicious outsider could simply barrage the local system's syslog port with spurious traffic either as a denial-of- service attack on the system, or to fill up the local system's logging file systems so that subsequent attacks will not be logged.

Note: A future edition of this Benchmark will see this section moved/combined within Section 6.

Remediation:
Question:
Is this machine a log server, or does it need to receive Syslog messages via the network from other systems?
If the answer to this question is yes, then perform the action below.

Recommend reading the `syslog` manpage to understand the -l, -r and -s options.

Edit `/etc/init.d/syslog` and look for the line that says:
```
SYSLOGD_OPTIONS="-m 0"
```
and add the entries that are appropriate for the site. An example entry would look like this:
```
SYSLOGD_OPTIONS="-m 0 -l loghost -r -s mydomain.com"
```

Scoring Status: **Scorable**

9 User Accounts and Environment

Note: The items in this section are tasks that the local administrator should undertake on a regular, ongoing basis perhaps in an automated fashion via cron. The automated host-based scanning tools provided from the Center for Internet Security can be used for this purpose. These scanning tools are typically provided with this document, but are also available for free download from http://www.CISecurity.org

9.1 Block Login of System Accounts

Description:
These accounts are non-human system accounts that should be made less useful to an attacker by locking them and setting the shell to a shell not in `/etc/shells`. They can even be deleted if the machines does not use the daemon/service that each is responsible for, though it is safest to simply deactivate them as is done here. To deactivate them, lock the password and set the login shell to an invalid shell. `/dev/null` is a good choice because it is not a valid login shell, and should an attacker attempt to replace it with a copy of a valid shell the system will not operate properly. In the remediation, 'sdiff' is used to display differences side-by-side.

Remediation:
```
echo "Basically change the '/sbin/nologin' portion to '/dev/null' in /etc/passwd"
echo "  and add an exclamation point to the password field in /etc/shadow."
cd /etc
for NAME in `cut -d: -f1 /etc/passwd`; do
     MyUID=`id -u $NAME`
     if [ $MyUID -lt 500 -a $NAME != 'root' ]; then
         usermod -L -s /dev/null $NAME
     fi
done
ls -la /etc/passwd
echo "sdiff passwd-preCIS passwd"
echo "--------------------------"
chown root:root /etc/passwd
chmod 0644      /etc/passwd
sdiff passwd-preCIS passwd

ls -la /etc/shadow
echo "sdiff shadow-preCIS shadow"
echo "--------------------------"
chown root:root  /etc/shadow
chmod 0400       /etc/shadow
sdiff shadow-preCIS shadow
cd $cishome
```

Scoring Status: **Scorable**

9.2 Verify That There Are No Accounts With Empty Password Fields

Description:
An account with an empty password field means that anybody may log in as that user without providing a password at all. All accounts should have strong passwords or should be locked by using a password string like "!!". By using "!!", passwd will warn when attempting to unlock an account with an empty password.

Remediation:
The command:

```
awk -F: '( $2 == "" ) { print $1 }' /etc/shadow
```

should not return any lines of output.

Scoring Status: **Scorable**

9.3 Set Account Expiration Parameters On Active Accounts

Description:
It is a good idea to force users to change passwords on a regular basis. The commands below will set all active accounts (except system accounts) to force password changes every 90 days (-M 90), and then prevent password changes for seven days (-m 7) thereafter. Users will begin receiving warnings 14 days (-W 14) before their password expires. Once the password expired, the account will be locked out after 7 days (-I 7). Finally, the instructions below set a minimum password length of 9 characters. These are recommended starting values. Some regulated industries require more restrictive values – ensure they comply with the local Enterprise security policy.

Remediation:

```
# The login.defs manpage indicates these functions are now # all handled by PAM.
# This changes the defaults applicable to new accounts added to the system after
# this point.
cd /etc
awk  '($1 ~ /^PASS_MAX_DAYS/)  { $2="90" }
      ($1 ~ /^PASS_MIN_DAYS/)  { $2="7" }
      ($1 ~ /^PASS_WARN_AGE/)  { $2="14" }
      ($1 ~ /^PASS_MIN_LEN/)   { $2="9" }
      { print }' login.defs-preCIS  >  login.defs
useradd  -D  -f  7
# This applies the same basis of changes to existing accounts.
# -m: (7)  The number of days between permitted password changes.
# -M: (90) The maximum number of days a password is valid.
# -W: (14) The maximum number of days of advanced warning before a password is no
# longer valid.
# -I: (7)  The maximum number of days of inactivity, after a password has expired,
# before the account is locked.
for  NAME  in  `cut  -d:  -f1  /etc/passwd`;  do
               uid=`id  -u  $NAME`
               if  [  $uid  -ge  500  -a  $uid  !=  65534 ];  then
                      chage  -m  7  -M  90  -W  14  -I  7  $NAME
               fi
done
cat <<END_SCRIPT  >> login.defs

# The following 2 lines added, per CIS Red Hat Enterprise Linux Benchmark sec 9.3
# Establish a forced five-second minimum delay between failed logins
FAIL_DELAY        5
END_SCRIPT
chown  root:root  login.defs
chmod  0640       login.defs
echo "diff shadow-preCIS shadow"
      diff shadow-preCIS shadow
cd $cishome
```

Scoring Status: **Scorable**

9.4 Verify No Legacy '+' Entries Exist In passwd, shadow, And group Files

Description:
Plus ('+') entries 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 may provide an avenue 41 for attackers to gain privileged access on the system, and should be deleted if they exist.

Remediation:
```
# Do a context specific diff to only show differences related to having plus signs
# in the file.
# Otherwise the output is too much
grep -v ^+:   /etc/group     > $tmpcis/group.tmp
grep -v ^+:   /etc/gshadow   > $tmpcis/gshadow.tmp
grep -v ^+:   /etc/passwd    > $tmpcis/passwd.tmp
grep -v ^+:   /etc/shadow    > $tmpcis/shadow.tmp
# Express the essence of what is compared.
echo "diff /etc/group-preCIS    /etc/group"
      diff /etc/group-preCIS    $tmpcis/group.tmp
echo "diff /etc/gshadow-preCIS  /etc/gshadow"
      diff /etc/gshadow-preCIS  $tmpcis/gshadow.tmp
echo "diff /etc/passwd-preCIS   /etc/passwd"
      diff /etc/passwd-preCIS   $tmpcis/passwd.tmp
echo "diff /etc/shadow-preCIS   /etc/shadow"
      diff /etc/shadow-preCIS   $tmpcis/shadow.tmp
chown root:root $tmpcis/group.tmp  $tmpcis/gshadow.tmp  $tmpcis/passwd.tmp
$tmpcis/shadow.tmp
chmod 0644      $tmpcis/group.tmp                        $tmpcis/passwd.tmp
chmod 0400                         $tmpcis/gshadow.tmp
$tmpcis/shadow.tmp
/bin/cp -pf  $tmpcis/group.tmp     /etc/group
/bin/cp -pf  $tmpcis/gshadow.tmp   /etc/gshadow
/bin/cp -pf  $tmpcis/passwd.tmp    /etc/passwd
/bin/cp -pf  $tmpcis/shadow.tmp    /etc/shadow
```

This should return no lines of output for each of the files evaluated.

Scoring Status: **Scorable**

9.5 No '.' or Group/World-Writable Directory In Root's $PATH

Description:
Including the current working directory '.' (dot) 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, run a script to delete all files, or other malicious activity.

Investigate and correct the cause of such errors.

Note: Errors occur when a directory specified in the path does not exist. For example, on a new RHEL5 build, the below find generated this error (which generally can be ignored):
`find: /root/bin: No such file or directory`

Remediation:
The automated testing tool supplied with this Benchmark will alert the administrator if action is required.

To find '.' in $PATH:
```
echo $PATH | egrep '(^|:)(\.|:|$)'
```

To find group- or world-writable directories in $PATH:
```
# Part 1
echo "Any entries listed here should be fixed (other than an error for missing
/root/bin)."
echo "PATH($PATH)."
echo "Any entries listed next indicated a period exists in the PATH environment
variable (BAD)."
echo $PATH | egrep '(^|:)(\.|:|$)'
# Part 2
echo "Here, are paths with group/world writeable directories in root's PATH
(BAD)."
echo "(roots PATH variable contains '/root/bin', even though that directory
doesn't exist, by default)"
echo "(Errors regarding /mnt/sysimage, are ghosts held over from a kickstarted
system build"
echo " implementation and can be safely ignored)"
find `echo $PATH | tr ':' ' '` -type d \( -perm -002 -o -perm -020 \) -ls
echo ""
```

These commands should produce no errors or output on a properly hardened system.

Scoring Status: **Scorable**

9.6 User Home Directories Should Be Mode 0750 or More Restrictive

Description:
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. Disabling "read" and "execute" access for users who are not members of the same group (the "other" access category) allows for appropriate use of discretionary access control by each user. While the below modifications are relatively benign, making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Also, consider special case home directories such as the sftp / ftp accounts used to transfer web content to a web server, typically need to be world readable (r) and searchable (x) as they contain documents for the web server.

User home directories are a potentially fragile area that foster human interaction with the system, ostensibly for the purpose of mission-oriented work. The hazards of weak passwords and numerous other insecurities potentially leave this area fertile for miscreant attention. One way to combat this is to tighten permission to `0700` for home directories. This would be in addition to what is recommended here (and not currently scored).

The `nfsnobody` user account has a UID of `65534`, and a home directory of `/var/lib/nfs`.

Remediation:
```
for DIR in `awk -F: '( $3 >= 500 ) { print $6 }' /etc/passwd`; do
```

```
    if [ $DIR != /var/lib/nfs ]; then
         chmod -R g-w   $DIR
         chmod -R o-rwx $DIR
    fi
done
```

Scoring Status: **Scorable**

9.7 No User Dot-Files Should Be World-Writable

Description:
World-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges. While the below modifications are relatively benign, making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users.

One option is to add protective commands into `/etc/profile` which execute as the user log's in every time to enforce user dot files not being world write-able. Though not scored or recommended empirically by CIS, it is an option if the user environment supports it.

Remediation:

```
for DIR in `awk -F: '($3 >= 500) { print $6 }' /etc/passwd`; do
    for FILE in $DIR/.[A-Za-z0-9]*; do
        if [ ! -h "$FILE" -a -f "$FILE" ]; then
             chmod go-w "$FILE"
        fi
    done
done
```

Scoring Status: **Scorable**

9.8 Remove User .netrc Files

Description:
`.netrc` files may potentially contain unencrypted passwords which may be used by a miscreant to attack it or other inter-connected systems. Applying global modifications to user home directories without alerting the user community first, can result in unexpected outages and/or very unhappy users.

Should the `find` command return any results, carefully evaluate the ramifications of removing those files (in active coordination with the affected users) before removing such `.netrc` files, as not doing so may impact a mission application, or operational users, that have not had time to revise their architecture to a more secure implementation. The output from the audit can lend further support to management and administrative efforts in those directions. CIS recommends that `.netrc` files should not have insecure password entries.

Audit:

```
find / -name .netrc -exec grep -il password {} \; > \
     $tmpcis/LISTof.netrcFiles 2>&1
```

Remediation:
Manual removal of any `.netrc` files with insecure 'password' entries by system administration personnel after coordination with the affected users.

Scoring Status: **Scorable**

9.9 Set Default umask For Users

Description:
With a default umask setting of `077` – a setting agreed to as part of a security consensus/discussion process with DISA and NSA – files and directories created by users should not be readable (by default) by any other human user on the system. 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. 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. A gentler umask value that many institutions use is `022`, due to the problems within their applications when set to `077`.

Note: This strict a setting (umask of 077) has been shown to occasionally cause problems with the installation of software packages where the installation script relies on a default umask – the directories are owned by root with `0700` permissions, and then the application and/or daemon cannot read its files. A simple fix to this problem is to manually issue a less restrictive umask (such as umask `022`) for the shell session doing the installation, or place such a umask command in the beginning to a less restrictive value before the installation, or in the beginning of the installation script. There are, of course, special cases to consider, for example the recommended umask setting of `077` interferes with the sftp and ftp users who need to have the web files transferred be world readable and directories world searchable. Typically, the umask setting needs to be `022` or occasionally `002` for sftp and ftp web transfer accounts. While the umask can be configured in the ftp server configuration file however for sftp users, a patch is required for the sftp server before umask control is available. The patch is available as part of the sftp logging patch http://sftplogging.sourceforge.net

The Benchmark will score for `022` as well as accept/test up to `077`. Therefore utilize what is best, yet strictest for the environment.

The Benchmark will adjust root's `umask` setting separately in this item, as root shells don't necessarily read the system-wide configuration files. For example, root sessions using bash doesn't get `umask` settings from `/etc/profile`. The same concerns and recommendations apply to root's umask setting.

Remediation:

```
# Forced umask assignment into /etc/skel/.bashrc for consistency
#   (though the CIS scoring tool doesn't check here yet)
CISum='077'
sed  -e  "s/002/$CISum/"  -e  "s/022/$CISum/"  /etc/bashrc-preCIS           >
/etc/bashrc
sed  -e  "s/002/$CISum/"  -e  "s/022/$CISum/"  /etc/csh.cshrc-preCIS        >
/etc/csh.cshrc
sed      "s/027/$CISum/"                       /etc/csh.login-preCIS        >
/etc/csh.login
sed      "s/027/$CISum/"                       /etc/profile-preCIS          >
/etc/profile
echo     "umask $CISum"                                                     >>
/etc/skel/.bashrc
sed      "s/027/077/"                          /root/.bash_profile-preCIS   >
/root/.bash_profile
echo "umask 077" >> /root/.bashrc
echo "umask 077" >> /root/.cshrc
echo "umask 077" >> /root/.tcshrc
chown root:root  /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/profile
chmod 0444       /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/profile
chown root:root  /root/.bash_profile /root/.bashrc /root/.cshrc /root/.tcshrc
chmod 0400       /root/.bash_profile /root/.bashrc /root/.cshrc /root/.tcshrc
echo "diff /etc/bashrc-preCIS /etc/bashrc"
      diff /etc/bashrc-preCIS /etc/bashrc
echo "diff /etc/csh.cshrc-preCIS /etc/csh.cshrc"
      diff /etc/csh.cshrc-preCIS /etc/csh.cshrc
echo "diff /etc/csh.login-preCIS /etc/csh.login"
      diff /etc/csh.login-preCIS /etc/csh.login
echo "diff /etc/profile-preCIS /etc/profile"
      diff /etc/profile-preCIS /etc/profile
echo "diff /root/.bash_profile-preCIS /root/.bash_profile"
      diff /root/.bash_profile-preCIS /root/.bash_profile
echo "diff /etc/skel/.bashrc-preCIS /etc/skel/.bashrc"
      diff /etc/skel/.bashrc-preCIS /etc/skel/.bashrc
echo "diff /root/.bashrc-preCIS /root/.bashrc"
      diff /root/.bashrc-preCIS /root/.bashrc
echo "diff /root/.cshrc-preCIS /root/.cshrc"
      diff /root/.cshrc-preCIS /root/.cshrc
echo "diff /root/.tcshrc-preCIS /root/.tcshrc"
      diff /root/.tcshrc-preCIS /root/.tcshrc
#
# Suggest a process that walks all existing user accounts (> 500) and force's the
same permissions
# into their profile scripts.
```

Scoring Status: **Scorable**

9.10 Disable Core Dumps

Description:

Core dumps can consume large volumes of disk space and may contain sensitive data. On the other hand, developers using this system may require core files in order to aid in debugging. The `limits.conf` file can be used to grant core dump ability to individual users or groups of users.
It should be noted that user accounts get this applied to them automatically, via `/etc/profile`. It sets this soft limit to zero, by default (via: `ulimit -S -c 0`).

Remediation:
Question:
Do developers need to debug crashed programs or send low-level debugging information to software developers/vendors?
If the answer to this question is no, then perform the action below:

```
awk '( $1 == "#*" && $2 == "soft" && $3 == "core" && $4 == "0" ) {  \
       print "*                soft    core            0";          \
       print "*                hard    core            0"; next  }  \
     { print }'  /etc/security/limits.conf-preCIS > /etc/security/limits.conf
chown root:root /etc/security/limits.conf
chmod 0644      /etc/security/limits.conf
echo "diff /etc/security/limits.conf-preCIS /etc/security/limits.conf"
      diff /etc/security/limits.conf-preCIS /etc/security/limits.conf
```

Scoring Status: **Scorable**

9.11 Limit Access To The Root Account From su

Description:
The `su` (Switch User) command allows a user or SysAdmin to become other users on the system when needed. This is commonly used to switch users (`su`) to "`root`" and execute commands as the super-user. CIS recommends that it is not desirable for general unconstrained users to have the freedom to `su` to `root`; therefore uncomment the following line in `/etc/pam.d/su`, by removing the leading pound sign:

```
# auth required /lib/security/$ISA/pam_wheel.so use_uid
```

Uncommenting this line allows ONLY the users specifically identified in the `wheel` group to become `root` by using the `su` command and entering the `root` password. All other users will receive a benign message stating the password is incorrect. Again, users who do not have `wheel` group membership will not be able to `su` into any other user account, not just into the `root` account.

By limiting access to the `root` account, even if a user knows the `root` password, they will not be able to become `root` unless that user has physical access to the server's console, or they are added to the `wheel` group. This adds another layer of security to the system and prevents unauthorized system access.

There are four parts in this recommended remediation, they are described as follows:
Part 1: Provides positive control over utilizing `su` to gain access to `root`. by requiring user membership in the `wheel` group. This is a change to how `pam` controls user access to `su`.
Part 2: An example, which facilitates, in an automated fashion, the adding of users to the system, and setting their appropriate login properties.
Part 3: Adds the named users into the `wheel` group in `/etc/group`.
Part 4: Adds the users into /etc/security/access.conf, thus allowing them permission to access the console, too.

Remediation:

WARNING: Ensure a legitimate administrative person has a valid user account listed in the `wheel` group before running the below script. Failure to do so will prevent anyone from using `su` to become `root`.

Note: Set the value for "$AdminsComma " to a local approved list of SysAdmins, and only separate each entity with commas. This first line here is an example, replace the userIDs with yours.

```
$AdminsComma="userID1,userID2,userID3"

# Part 1
echo "Note: By executing this ONLY members of the wheel group can su to root."
cd /etc/pam.d/
awk '( $1=="#auth" && $2=="required" && $3~"pam_wheel.so" ) \
     { print "auth\t\trequired\t",$3,"\tuse_uid"; next };
     { print }' /etc/pam.d/su-preCIS > /etc/pam.d/su
chown root:root /etc/pam.d/su
chmod 0644      /etc/pam.d/su
echo "diff /etc/pam.d/su-preCIS /etc/pam.d/su"
      diff /etc/pam.d/su-preCIS /etc/pam.d/su
cd $cishome

# Part 2
# The process is beneficial when using kickstart for building of systems, then
# deliberately go back to all those systems and forcefully change the
# root/SysAdmin passwords to be in new.
echo "(${AdminsComma}) are to be System Administrators for this system."

for USERID in `echo $AdminSP`
    do
      echo "1.  Dealing with userid($USERID)..."
      ID=`cat /etc/passwd | cut -d: -f1 | grep $USERID 2>&1`
      if [ "$ID" != "$USERID" ]; then
         # The user-id was NOT found
         echo "2a  Adding new user ($USERID) 'procedure-compliant'."
         # Use grub-md5-crypt to generate the encrypted password
         useradd -f 7 -m -p '$1$PyDA7$L81b0Sp1u.DyGnjbRUp/3/' $USERID
         chage  -m  7  -M  90  -W  14  -I  7  $USERID
      else
         echo "2b  User ($USERID) already in the system."
         chage  -m  7  -M  90  -W  14  -I  7  $USERID
      fi
      ls -la /home
    done
echo "Doing pwck -r"
pwck -r
echo ""

# Part 3
# Perform steps to ensure any users identified in $Admins are added to the "wheel"
# group.  This is probably only going to add the example 'tstuser' account, or
# whichever userID the system builder names during the initial system build.
# Note: /etc/group requires entries to be comma-separated.
if [ "$Admins" != "" ]; then
     echo "At least one AdminID has been identified to be added to the wheel
group."
     echo "Admins(${Admins}), AdminSP(${AdminSP}), AdminsComma(${AdminsComma})."
     cd /etc
     # Resultant /etc/group file is now nicely sorted as well
     /bin/cp -pf group $tmpcis/group.tmp
     awk -F: '($1~"wheel" && $4~"root") { print $0 "," Adds }; \
              ($1 != "wheel") {print}' Adds="`echo $AdminsComma`" \
            $tmpcis/group.tmp | sort -t: -nk 3 >  $tmpcis/group.tmp1
```

```
     chown root:root $tmpcis/group.tmp1
     chmod 0644      $tmpcis/group.tmp1
     /bin/cp -pf $tmpcis/group.tmp1  group
     echo "sdiff group-preCIS group"
           sdiff group-preCIS group
     cd $cishome
else
        echo "BAD.  No SysAdmin IDs were identified to be added to the wheel
group."
fi

# Part 4
echo "#### This is done in concert with Bastille that was executed before this
step in the"
echo "#### standard baseline hardening.  This will add SPACE-delimited SysAdmin
userIDs to"
echo "#### the /etc/security/access.conf file.  These are the same names as are
added to"
echo "#### the wheel group in the /etc/group file.  This action prohibits any user
NOT in"
echo "#### the wheel group from logging in to the system on the physical console."
echo "#### Can treat this as a known entity with one entry to deal with since the
state of"
echo "#### this system up to this point is well known."
echo "#### No differences may appear, if the same users are listed here, as were
added by Bastille."
#    The line in question resembles the following, 3 colon-separated fields:
#    -:ALL EXCEPT root tstuser:LOCAL
#    To be turned into something that looks like the following (sorted IDs are
#     easier to read):
#    -:ALL EXCEPT abc-Admin root def-Admin tstuser:LOCAL
#
cd /etc/security
# Check if there are any uncommented lines to ADD $Admins to.
x="`grep -v ^# access.conf | wc -l | cut -d: -f1`"
echo "x($x)"
if [ "$x" == "0" ]; then
     # Most likely the Bastille hardening hasn't been applied yet.
     # Must manually add the users, as the file is otherwise 'empty'.
     echo "Manually adding the ($Admins); none previously existed there."
     echo "-:ALL EXCEPT root" $AdminSP":LOCAL" >> access.conf
else
     # Extract just the userIDs
     x="`grep -v ^# access.conf | cut -d: -f2 | cut -d' ' -f3-`"
     # Bundle in the new SysAdmin IDs passed during script invocation, and sort
the names alphabetically.
     # Need a piece here to compare what's there with what we have to add, to
avoid duplicates.
          y="`echo $AdminsComma $x | tr -s ',' ' ' | tr ' ' '\012' | sort -u | tr
'\012' ' '`"
     echo "x($x), y($y)";echo ""
     # 2nd -e is to eliminate the extra space before the final colon, if one
exists.
       sed -e "s/$x/$y/" -e 's/ :L/:L/' access.conf-preCIS > access.conf
     # sed "s/$x/$y/" access.conf-preCIS | sed 's/ :L/:L/' > access.conf
fi
echo "diff /etc/security/access.conf-preCIS /etc/security/access.conf"
      diff /etc/security/access.conf-preCIS /etc/security/access.conf
chown root:root /etc/security/access.conf
```

```
chmod 0640      /etc/security/access.conf
cd $cishome
chmod -R 0400 $tmpcis/*
```

Scoring Status: Scorable

THIS PAGE INTENTIONALLY LEFT BLANK

10 Warning Banners

Presenting some sort of statutory warning message prior to the normal user logon may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect/benefit of hiding OS version information and other detailed system information from attackers attempting to target specific attacks at a system (though there are other mechanisms available for acquiring at least some of this information).

Guidelines published by the US Department of Defense require that warning message 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. Clearly, the organization's local legal counsel and/or site security administrator should 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.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm.

10.1 Create Warnings For Network And Physical Access Services

Description:
The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices. `/etc/motd` 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.

Edit the banner currently in `/etc/issue` – if empty, utilize copy provided below and it may need to be changed for the local Enterprise, based upon policy. Leave the words "COMPANYNAME" as this will be replaced in the next step with the name of the organization.

```
                        NOTICE TO USERS
                        ---------------
This computer system is the private property of COMPANYNAME, whether
individual, corporate or government.  It is for authorized use only.  Users
(authorized & unauthorized) have no explicit/implicit expectation of privacy

Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and disclosed
to your employer, to authorized site, government, and/or law enforcement
personnel, as well as authorized officials of government agencies, both
domestic and foreign.

By using this system, the user expressly consents to such interception,
monitoring, recording, copying, auditing, inspection, and disclosure at the
discretion of such officials.  Unauthorized or improper use of this system
may result in civil and criminal penalties and administrative or disciplinary
action, as appropriate.  By continuing to use this system you indicate your
awareness of and consent to these terms and conditions of use.  LOG OFF
IMMEDIATELY if you do not agree to the conditions stated in this warning.
```

Remediation:
Create banners for console access:

Note: Change the colored "The Company" in the text below to an appropriate value for the organization (don't use any special characters like single or double quote marks).

```
unalias cp mv
cd /etc
# Remove OS indicators from banners
for FILE in issue motd; do
    cp -f ${FILE} ${FILE}.tmp
    egrep -vi "red hat|kernel|fedora|centos" ${FILE}.tmp > ${FILE}
    rm -f ${FILE}.tmp
done
# Change name of owner
# Remember to enter name of your company/organization here:
COMPANYNAME="The Company"
cp -f issue issue.tmp
sed -e "s/its owner/${COMPANYNAME}/g" issue.tmp > issue
rm -f issue.tmp
diff issue-preCIS issue
if [ "`grep -i authorized /etc/issue`" == "" ]; then
     echo "Authorized uses only.  All activity may be \
     monitored and reported." >> /etc/issue
fi
if [ "`grep -i authorized /etc/motd`" == "" ]; then
     echo "Authorized uses only.  All activity may be \
     monitored and reported." >> /etc/motd
fi

# Create banners for network access:
/bin/cp -pf /etc/issue  /etc/issue.net
/bin/cp -pf /etc/issue  /etc/motd

# Protect banner files:
chown  root:root  /etc/issue  /etc/issue.net  /etc/motd
chmod  0644       /etc/issue  /etc/issue.net  /etc/motd
echo "diff /etc/issue-preCIS     /etc/issue"
      diff /etc/issue-preCIS     /etc/issue
echo "diff /etc/issue.net-preCIS /etc/issue.net"
      diff /etc/issue.net-preCIS /etc/issue.net
echo "diff /etc/motd-preCIS      /etc/motd"
      diff /etc/motd-preCIS      /etc/motd
```

Scoring Status: **Scorable**

10.2 Create Warnings For GUI-Based Logins

Description:
The standard graphical login program for Red Hat Enterprise Linux is `gdm`, which requires the user to enter their username in one text box and their password in a second text box. The commands below set the warning message on `xdm`, `kdm` and `gdm` – in case something other than the default X login GUI was chosen to be installed.

These are optional settings to make, if the X Windows interface it not installed (and it isn't required for Linux to be operational).

Remediation:

```
# 1st Part
if [ $Consent == "DoD" ]; then
     echo "Set for DoD"
     GreetMsg1='xlogin*greeting: This is a U.S.  Govt Computer - Authorized USE
only!'
     GreetMsg2='This is a U.S.  Govt Computer - Authorized USE only!'
else
     # Alternative is to be left as Generic/Anonymous
     echo "============================="
     echo "  Set for Generic/Anonymous"
     echo "============================="
     GreetMsg1='xlogin*greeting: This is a private system --- Authorized USE
only!'
     GreetMsg2='This is a private system --- Authorized USE only!'
fi

# 2nd Part
if [ -e /etc/X11/xdm/Xresources ]; then
    cd /etc/X11/xdm
    awk '/xlogin\*greeting:/ { print GreetValue; next };
         { print }' GreetValue="$GreetMsg1" Xresources-preCIS > Xresources
    chown root:root Xresources
    chmod 0644      Xresources
    echo "diff Xresources-preCIS Xresources"
    diff Xresources-preCIS Xresources
    cd $cishome
else
    echo "OK.  No '/etc/X11/xdm/Xresources'."
fi
echo ""

# 3rd Part
if [ -e /etc/X11/xdm/kdmrc ]; then
    cd /etc/X11/xdm
    awk '/GreetString=/ \
    { print "GreetString=" GreetString; next };
    { print }' GreetString="$GreetMsg2"  kdmrc-preCIS > kdmrc
    chown root:root kdmrc
    chmod 0644      kdmrc
    echo "diff kdmrc-preCIS kdmrc"
    diff kdmrc-preCIS kdmrc
    cd $cishome
else
    echo "OK.  No '/etc/X11/xdm/kdmrc'."
```

```
fi
echo ""

# 4th Part - Provided by Dave Mullins (RHCE), ProSync 20070206"
# This FORCES the user, upon successfully passing thru a credentialed GUI login,
# to positively acknowledge Consent-to-Use.
if [ -e /etc/gdm/PreSession/Default ]; then
     ed /etc/gdm/PreSession/Default  <<END_SCRIPT
1
/^SESSREG=
a
/usr/bin/xmessage -center -buttons " I acknowledge and consent to monitoring \
":2," Cancel Login ":3 -file /etc/issue
egxit="\$?"
if [ \$egxit != 2 ]; then
     # Immediately FORCE logout by killing the 'X' session process
     echo "Consent-To-Use: User (\$LOGNAME) cancelled login (\`date\`)." \
          >> /var/log/messages
     kill -9 \`ps -ef |grep /usr/bin/X |grep -v grep | tr -s ' ' | cut -d' ' -f2\`
fi
.
w
q
END_SCRIPT
     chown root:root /etc/gdm/PreSession/Default
     chmod 0755      /etc/gdm/PreSession/Default
     echo "diff /etc/gdm/PreSession/Default-preCIS  /etc/gdm/PreSession/Default"
          diff /etc/gdm/PreSession/Default-preCIS  /etc/gdm/PreSession/Default
else
    echo "Part 4-OK.  No '/etc/gdm/PreSession/Default file to harden'."
fi
```

Scoring Status: **Scorable**

10.3 Create "authorized only" Banners For vsftpd, proftpd, If Applicable

Description:
This item configures a `vsftpd` "authorized users only" banner messages.

Remediation:

```
cd /etc
if [ -d vsftpd ]; then
    cd vsftpd
fi
if [ -e vsftpd.conf ]; then
   echo "ftpd_banner=Authorized users only.  All activity may be monitored and \
         reported." >> vsftpd.conf
   echo "diff vsftpd.conf-preCIS vsftpd.conf"
   diff vsftpd.conf-preCIS vsftpd.conf
   chown root:root vsftpd.conf
   chmod 0600      vsftpd.conf
else
   echo "OK - No vsftpd to change."
fi
cd $cishome
```

Scoring Status: **Scorable**

11 Misc odds and ends

11.1 Configure and enable the auditd and sysstat services, if possible

Description:
System auditing and logging is an essential element to the defense-in-depth paradigm for system security hardening. The following remediation, composed in three parts, configures and enables the auditing service to collect meaningful and effective logging records. Also, the `sysstat` service is enabled.

Part 1: This section applies well-constructed audit rules into `/etc/audit/audit.rules`.
- The '-f 1' and '-f 2' sets the default action for handling audit failure mode. The safe mode is "1" by default. This can be set for higher critical systems, as local needs dictate.
- There are audit rules for both 32 and 64 bit architectures. This file can be implemented, as is, on 64 bit systems. On 32 bit systems, comment out all lines containing "`arch=b64`".

This file came from the audit.rpm from Red Hat and is included here with support and concurrence of Red Hat. Some lines from the original file are longer than the page width, even with the smaller font, and thus wrap. Where this occurs, the continuation of the previous line is indicated below with underlining.

Part 2: Strengthens `audit.conf` settings.
Part 3: This starts the `auditd` and `sysstat` services and ensures they persist across reboots.

Once this remediation is implemented, reboot the system as soon as possible afterwards.

Remediation:
```
echo "Configure and enable the auditd and sysstat services, if possible."
auditPATH='/etc/audit'
# Part 1
echo "Enforce auditing minimums."
# This will enforce auditing minimums.
/bin/cp -pf                  $auditPATH/audit.rules    $tmpcis/audit.rules.tmp
cat <<END_SCRIPT   >         $auditPATH/audit.rules
## This file contains the auditctl rules that are loaded
## whenever the audit daemon is started via the initscripts.
## The rules are simply the parameters that would be passed
## to auditctl.
##
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## Set failure mode to syslog notice {these two are mutually exclusive}
-f 1

## Set failure mode to panic {these two are mutually exclusive}
## -f 2

## NOTE:
## 1) if this is being used on a 32 bit machine, comment out the b64 lines
## 2) These rules assume that login under the root account is not allowed.
```

```
## 3) It is also assumed that 500 represents the first usable user account.
## 4) If these rules generate too much spurious data for your tastes, limit the
##    the syscall file rules with a directory, like -F dir=/etc
## 5) You can search for the results on the key fields in the rules
##
## (GEN002880: CAT II) The IAO will ensure the auditing software can
## record the following for each audit event:
##- Date and time of the event
##- Userid that initiated the event
##- Type of event
##- Success or failure of the event
##- For I&A events, the origin of the request (e.g., terminal ID)
##- For events that introduce an object into a user's address space, and
##  for object deletion events, the name of the object, and in MLS
##  systems, the object's security level.
##
## Things that could affect time
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
#-a always,exit -F arch=b32 -S clock_settime -k time-change
#-a always,exit -F arch=b64 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

## Things that affect identity
-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

## Things that could affect system locale
-a exit,always -F arch=b32 -S sethostname -S setdomainname -k system-locale
-a exit,always -F arch=b64 -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

## Things that could affect MAC policy
-w /etc/selinux/ -p wa -k MAC-policy

## The SysAdmin will configure the auditing system to audit the following events
## for all users and root:
## - Logon (unsuccessful and successful) and logout (successful)
##   This is handled by pam, sshd, login, and gdm
##   Might also want to watch these files if needing extra information
#    -w /var/log/faillog -p wa -k logins
#    -w /var/log/lastlog -p wa -k logins

##- Process and session initiation (unsuccessful and successful)
##
## The session initiation is audited by pam without any rules needed.
## Might also want to watch this file if needing extra information
#-w /var/run/utmp -p wa -k session
#-w /var/log/btmp -p wa -k session
#-w /var/log/wtmp -p wa -k session

##- Discretionary access control permission modification (unsuccessful
## and successful use of chown/chmod)
```

```
-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 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=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 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=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S
lremovexattr -S fremovexattr -F auid>=500 -F auid!=4294967295 -k perm_mod

##- Unauthorized access attempts to files (unsuccessful)
-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
-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=b64 -S creat -S open -S openat -S truncate -S ftruncate -F
exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

##- Use of privileged commands (unsuccessful and successful)
##  use find /bin -type f -perm -04000 2>/dev/null and put all those files in
##  a rule like this
-a always,exit -F path=/bin/ping -F perm=x -F auid>=500 -F auid!=4294967295 -k
privileged

##- Use of print command (unsuccessful and successful)

##- Export to media (successful)
## You have to mount media before using it. You must disable all automounting
## so that its done manually in order to get the correct user requesting the
## export
-a always,exit -F arch=b32 -S mount -F auid>=500 -F auid!=4294967295 -k export
-a always,exit -F arch=b64 -S mount -F auid>=500 -F auid!=4294967295 -k export

##- System startup and shutdown (unsuccessful and successful)

##- Files and programs deleted by the user (successful and unsuccessful)
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
auid>=500 -F auid!=4294967295 -k delete

##- All system administration actions
##- All security personnel actions
##
## Look for pam_tty_audit and add it to your login entry point's pam configs.
## If that is not found, use sudo which should be patched to record its
## commands to the audit system. Do not allow unrestricted root shells or
## sudo cannot record the action.
-w /etc/sudoers -p wa -k actions

## Optional - could indicate someone trying to do something bad or
## just debugging
#-a entry,always -F arch=b32 -S ptrace -k tracing
#-a entry,always -F arch=b64 -S ptrace -k tracing
```

```
## Optional - could be an attempt to bypass audit or simply legacy program
#-a always,exit -F arch=b32 -S personality -k bypass
#-a always,exit -F arch=b64 -S personality -k bypass

## Put your own watches after this point
# -w /your-file -p rwxa -k mykey

## Make the configuration immutable - reboot is required to change audit rules
-e 2
END_SCRIPT
chown root:root $auditPATH/audit.rules
chmod 0600      $auditPATH/audit.rules
echo "diff $auditPATH/audit.rules-preCIS  $auditPATH/audit.rules"
      diff $auditPATH/audit.rules-preCIS  $auditPATH/audit.rules

# Part 2
echo "Strengthen auditd.conf settings."
sed -e "s/num_logs = 4/num_logs = 5/"                          \
    -e "s/max_log_file = 5/max_log_file = 100/"                \
    -e "s/space_left = 75/space_left = 125/"                   \
    -e "s/admin_space_left = 50/admin_space_left = 75/"        \
    -e "s/space_left_action = SYSLOG/space_left_action = email/" \
       $auditPATH/auditd.conf-preCIS > $auditPATH/auditd.conf
chown root:root $auditPATH/auditd.conf
# Default permissions were originally 0640.
chmod 0600      $auditPATH/auditd.conf
echo "diff $auditPATH/auditd.conf-preCIS  $auditPATH/auditd.conf"
      diff $auditPATH/auditd.conf-preCIS  $auditPATH/auditd.conf

# Part 3
echo "Make auditd applicable across reboots."
chkconfig --list auditd
chkconfig --list sysstat
echo "-------"
chkconfig --level 35 auditd  on
chkconfig --level 35 sysstat on
echo "-------"
# Enable auditd and sysstat services, good even if rebooting soon
service auditd  restart
service sysstat restart
echo "-------"
chkconfig --list auditd
chkconfig --list sysstat
chmod -R 0400 $tmpcis/*
echo ""
```

Scoring Status: Scorable

11.2 Verify no duplicate userIDs exist

Description:
Eliminate duplicate userIDs, unless a mission application cannot function without them.

Remediation:

```
echo "Verify no duplicate userIDs exist."
#dup username
x=`cut -f1 -d: /etc/passwd | sort | uniq -d | tr "\n" " "`
if [ "x$x" != "x" ]
then
echo "The following duplicate usernames found: $x"
fi
#dup uid
x=`cut -f3 -d: /etc/passwd | sort | uniq -d | tr "\n" " "`
if [ "x$x" != "x" ]
then
echo "The following duplicate uids found: $x"
fi
#dup groupname
x=`cut -f1 -d: /etc/group | sort | uniq -d | tr "\n" " "`
if [ "x$x" != "x" ]
then
echo "The following duplicate group names found: $x"
fi
#dup uid
x=`cut -f3 -d: /etc/group | sort | uniq -d | tr "\n" " "`
if [ "x$x" != "x" ]
then
echo "The following duplicate gids found: $x"
fi
echo ""
```

Scoring Status: **Scorable**

11.3 Force permissions on root's home directory to be 0700

Description:
Protect the `root` home directory from non-administrative users.

Remediation:

```
ls -lad /root
chown root:root /root
chmod 0700      /root
ls -lad /root
```

Scoring Status: **Scorable**

11.4 Utilize PAM to Enforce UserID password complexity

Description:
This puts protections in place for PAM authentication, clearly defining password length and complexity. The minimum length for the number of required password characters is 1, though increasing this (say to 2 or even 3) is acceptable depending upon site/system policy. This metric applies to the number of uppercase, lowercase, digits and/or special characters combined to form a legitimate password. Additionally, the minimum length of 9 characters for a password increases the time required for various password cracking tools to execute in order to gain access.

Note: The password complexity enforcement changes made to `/etc/pam.d/system-auth` have been manually accomplished by using the scriptlet below. Such changes will be overwritten if `authconfig` is ever executed. The `authconfig` utility has no mechanism to recognize these changes nor to save or implement them in any other way.

Additional information can be found on the web:
http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

Remediation:

```
# Have to copy the file before modifying it, as its also worked on in CIS SN.8.
# dcredit is number of numerals/digits required                      (1)
# lcredit is number of lower-case characters required                (1)
# ocredit is number of other/special/punctuation characters required  (1)
# ucredit is number of upper-case characters required                (1)
cd /etc/pam.d
/bin/cp -pf /etc/pam.d/system-auth $tmpcis/system-auth.tmp
awk '( $1 == "password" && $2 == "requisite" && $3 == "pam_cracklib.so" ) \
     { print $0 " dcredit=-1 lcredit=-1 ocredit=-1 ucredit=-1 minlen=9";  \
       next };         \
     { print }' $tmpcis/system-auth.tmp  >  system-auth
chown root:root /etc/pam.d/system-auth
chmod 0644      /etc/pam.d/system-auth
echo "diff /etc/pam.d-preCIS/system-auth /etc/pam.d/system-auth"
      diff /etc/pam.d-preCIS/system-auth /etc/pam.d/system-auth
echo " system-auth {original contents} --------------------------------"
cat /etc/pam.d-preCIS/system-auth
echo " system-auth {updated contents} --------------------------------"
cat /etc/pam.d/system-auth
echo "----------------------------------------------------------------"
echo "Protecting a hardened copy of /etc/pam.d/system-auth"
/bin/cp -pf /etc/pam.d/system-auth  /etc/pam.d/system-auth.HardenedProtectedCopy
ls -la /etc/pam.d/system-auth*
cd $cishome
chmod -R 0400 $tmpcis/*
```

Scoring Status: **Scorable**

11.5 Ensure perms on man and doc pages prevent modification by unprivileged users

Description:
Ensure permissions on man pages and system documentation files prevent modification by unprivledged users. These are stable files, provided as a resource as part the Operating System, and in some cases by a particular package creator/developer, that users have no need for more than read access to.

Remediation:
```
echo "Restrict permissions to 0644 on /usr/share/man and /usr/share/doc content"
date
chmod -R go-w /usr/share/doc  /usr/local/share/doc
chmod -R go-w /usr/share/man  /usr/local/share/man
```

Scoring Status: **Scorable**

11.6 Reboot

Description:
Whenever making substantial changes that affect overall system security are complete, CIS recommends rebooting the hardened system. Some System Administrators believe any change to the init scripts warrant a reboot in order to monitor the system and verify it comes up as expected. Hours of lost productivity with extensive troubleshooting (not to mention lost revenue) have occurred because a system did not start up as expected. The root cause might have been an init problem that would have been detected had the reboot taken place, for example. Reviewing errors in the system log files, `dmesg` and your observations all have merit.

Many scriptlets executed from this Benchmark create new versions of many RHEL5 configuration files. In the process of hardening the system, such scriptlets will very likely cause the pre-existing SELinux context (as provided by Red Hat) to be lost (on the live version of the directory and/or file) as a consequence of copying, moving and/or modifying them. Touching (to create) the `/.autorelabel` file and subsequently rebooting the system will reapply the SELinux contexts globally. Though doing this isn't mandatory, CIS encourages its application.

Remediation:
```
touch  /.autorelabel
init 6
```

Scoring Status: **Scorable**

THIS PAGE INTENTIONALLY LEFT BLANK

12 Anti-Virus Consideration

Certain systems – such as mail servers and file servers – at a minimum, should have anti-virus software installed to protect the Windows clients that use the server. Few Linux focused viruses exist, though the greatest protection would be the ubiquitous nature of Windows clients, applications and data that pass to, from and through Linux servers.

The following table summarizes some popular anti-virus offerings which are optionally available for the Linux platform. The Center for Internet Security makes no endorsement for any particular product.

Vendor	Product Type
Avast; **http://www.avast.com**	Commercial
Computer Associates InoculateIT; **http://www.cai.com**	Commercial
Clam AV; **http://www.clamav.net**	GPL & Commercial
CyberSoft Vfiind; **http://www.cyber.com/products/masterprice.html**	Commercial
f-prot AntiVirus; **http://www.f-prot.com/products/corporate_users/unix**	Commercial
H+B edv (hbedv); **http://www.pintunet.com**	Commercial
McAfee; **http://www.mcafee.com**	Commercial
NAI Virus Scan; **http://www.nai.com**	Commercial
Sophos; **http://www.sophos.com**	Commercial
Trend Micro; **http://www.trendmicro.com**	Commercial

THIS PAGE INTENTIONALLY LEFT BLANK

13 Remove CIS Benchmark Hardening Backup Files

Description:
When the Benchmark hardening changes are successful and tested, remove the backup files as they will have insecure contents and/or permissions/ownerships. Further, they consume additional disk space. By leaving these files on the system, an attacker can use the backup files as if they were the originals thereby defeating much of the CIS security hardening efforts. The last entry removes temporary intermediary files utilized during hardening actions.

Remediation:

```
find / -xdev | grep preCIS | xargs rm -rf
rm  -rf  /etc/cron.d-preCIS
rm  -rf  /etc/cron.daily-preCIS
rm  -rf  /etc/cron.hourly-preCIS
rm  -rf  /etc/cron.monthly-preCIS
rm  -rf  /etc/cron.weekly-preCIS
rm  -rf  /etc/pam.d-preCIS
rm  -rf  /etc/rc.d-preCIS
rm  -rf  /etc/skel-preCIS
rm  -rf  /etc/xinetd.d-preCIS
rm  -rf  /var/spool/cron-preCIS
```

System cleanup:

At the beginning of the CIS RHEL5 Benchmark hardening process, a temporary place was created for storage of work files. Now is the time to clean up those insecure files.

```
rm -rf $tmpcis
```

Scoring Status: **Not Scorable**

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix A: Additional Security Notes

The items in this section are security configuration settings that have been suggested by several other resources and system hardening tools. However, given the other settings in the Benchmark document, the settings presented here provide relatively little incremental security benefit. Nevertheless, none of these settings should have a significant impact on the functionality of the system, and some sites may feel that the slight security enhancement of these settings outweighs the (sometimes minimal) administrative cost of performing them.

None of these settings will be checked by the automated scoring tool provided with the Benchmark document. They are purely optional and may be applied or not at the discretion of local site administrators.

Note: As a matter of performance, accomplish these actions prior to completion of hardening in Section 13 of this Benchmark.

SN.1 Create Symlinks For Dangerous Files

Description:
The `/root/.rhosts`, `/root/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control (see the discussion of `.rhosts` files below). Attackers will often target these files as part of their exploit scripts. By linking these files to `/dev/null`, any data that an attacker writes to these files is simply discarded (though an astute attacker can still remove the link prior to writing their malicious data).

Remediation:
```
for FILE in /root/.rhosts /root/.shosts /etc/hosts.equiv /etc/shosts.equiv; do
    rm -f $FILE
    ln -s /dev/null $FILE
done
```

Scoring Status: **Not Scorable**

SN.2 Change Default Greeting String For sendmail

Description:
The default SMTP greeting string displays the version of the Sendmail software running on the remote system. Hiding this information is generally considered to be good practice, since it can help attackers target attacks at machines running a vulnerable version of Sendmail. However, the actions in the Benchmark document completely disable Sendmail on the system, so changing this default greeting string is something of a moot point unless the machine happens to be an email server.

Remediation:
```
cd /etc/mail
awk '/O SmtpGreetingMessage=/ { print "O SmtpGreetingMessage=Mail Server Ready;
$b"; next}
    { print }' sendmail.cf-preCIS | sed 's/^O HelpFile=/#O HelpFile=/' >
sendmail.cf
chown root:bin sendmail.cf
chmod 0444     sendmail.cf
echo "diff sendmail.cf-preCIS sendmail.cf"
```

```
      diff sendmail.cf-preCIS sendmail.cf
cd $cishome
echo ""
# Part 2 - Deactivate the decode entry in the /etc/aliases file
echo "Fixed /etc/aliases without decode"
sed 's/^decode:/#decode:/'  /etc/aliases-preCIS  >  /etc/aliases
newaliases
chown root:root /etc/aliases
chmod 0644      /etc/aliases
echo "diff /etc/aliases-preCIS /etc/aliases"
      diff /etc/aliases-preCIS /etc/aliases
```

Scoring Status: **Scorable**

SN.3 Enable TCP SYN Cookie Protection

Description:
A "SYN Attack" is a denial of service (DoS) attack that consumes resources on the system forcing a reboot. This particular attack is performed by beginning the TCP connection handshake (sending the SYN packet), and then never completing the process to open the connection. This leaves the system with several (hundreds or thousands) of half-open connections. This is a fairly simple attack and should be blocked.

Note: A future edition of this Benchmark will probably combine this entry with CIS 5.1, and employ this fix via /etc/sysctl.conf.

Remediation:

```
echo "echo 1 > /proc/sys/net/ipv4/tcp_syncookies"  >>  /etc/rc.d/rc.local
chown root:root /etc/rc.d/rc.local
chmod 0600      /etc/rc.d/rc.local
echo "diff /etc/rc.d-preCIS/rc.local /etc/rc.d/rc.local"
      diff /etc/rc.d-preCIS/rc.local /etc/rc.d/rc.local
```

Scoring Status: **Scorable**

SN.4 Additional GRUB Security

Description:
Setting the immutable flag on the GRUB config files will prevent any changes (accidental or otherwise) to the grub.conf or menu.lst files. Preferably, to modify either file, unset the immutable flag using the `chattr` command with `-i` instead of `+i`.

Remediation:

```
[ -e /boot/grub/menu.lst ]  && echo "(set immutable) for /boot/grub/menu.lst"
[ -e /boot/grub/menu.lst ]  && /usr/bin/chattr +i        /boot/grub/menu.lst

[ -e /boot/grub/grub.conf ] && echo "(set immutable) for /boot/grub/grub.conf"
[ -e /boot/grub/grub.conf ] && /usr/bin/chattr +i        /boot/grub/grub.conf
```

Scoring Status: **Scorable**

SN.5 Evaluate Packages Associated With Startup Scripts

Description:
The most effective way to get rid of the much of the unused software is to look in the startup directory `/etc/init.d` and evaluate which of these remaining services are not necessary. Use `rpm -qf <scriptname>` to determine the package it belongs to, use `rpm -qi <packagename>` to read about it, then use `rpm -e <packagename>` to remove it.

For example, this server may not use Broadcom NIC drivers, and therefore will not need the bcm5820 package. `rpm -qf bcm5820` shows us bcm5820 belongs to bcm5820-1.17-6. `rpm -qi bcm5820` proves we do not need this package. `rpm -e bcm5820` takes care of it.

In some cases, it might not be desirable or possible remove a script/package – kdcrotate is a good example: it belongs to package krb5-libs, which is required by several packages, including sendmail and nss_ldap. In cases like this, use `chkconfig <servicename> off` to keep it from running.

Note: Consider configuring iptables to act as a server-level firewall. There is controversy over this technique as some organizations feel all they need is the perimeter firewall and others feel the perimeter is just the first line of defense.

Remediation:
Question:
How many of the startup scripts do you really need?

Perform the action below.
```
cd /etc/init.d
ls -la
```

Scoring Status: **Not Scorable**

SN.6 Evaluate Every Installed Package

Description:
The default Red Hat Enterprise Linux installation includes many packages that are usually not necessary in an Enterprise server environment (dosfstools, for example). This should be done as a precursor to any system installation, especially in a Configuration Managed environment.

Computer Security Industry Best Practices recommend removing unused services and software to minimize attack vectors on a system.
The following references suggest and discuss removing unused software:

- Common Sense Guide to Cyber Security for Small Businesses – Recommended Actions for Information Security, 1st Edition, March 2004, http://www.us-cert.gov/reading_room/CSG-small-business.pdf
- IUP System Administrator Security Guidelines and Best Practices, http://www.iup.edu/tsc/security/;
- Security Engineering Awareness for Systems Engineers , http://www.software.org/pub/externalpapers/SecEngAwareness.doc

This task can be performed fairly quickly by logging in twice (your userID, followed with `su`) and running:

```
rpm -qa | sort | less
```

in one shell, and then using the other shell to remove the packages.

Some packages are dependent upon others and the SysAdmin will have to remove several packages at once. In some cases, an unused package will be required by another useful package, and it will have to remain installed – for example, `dateconfig` relies upon `audiofile` (for RHEL 2,1).

If the features of dateconfig are required, then audiofile will have to remain. One may think that the functionality of dateconfig is not necessary, however, the Red Hat Enterprise Linux documentation uses this tool to adjust the date, timezone and NTP settings of the server, and some Enterprises will have problems making system changes to servers without using the vendor-recommended tools.

For services which are disabled, the relevant software should be removed for the following reasons:
1. Less software to maintain and monitor for security issues
2. The service cannot be inadvertently enabled by an errant administrator or miscreant
3. Minimize damage in an attack should the attacker gain (or already have) access to the server
4. Achieve a smaller attack surface from which to rebuff attacks

Removed software can always be reinstalled using the Enterprise procedures.

By using this methodology on a test server, a still functional basic server was produced with less than 230 packages installed (down from the original 350 packages) taking up under 350MB of disk storage. This was performed in under an hour. Further, can be stabilized in an automated way via anaconda/kickstart.

Remediation:
Question:
How much unused software was installed on your system?

Scoring Status: **Not Scorable**

SN.7 Install and Configure sudo

Description:
sudo is a package that allows the SysAdmin to delegate activities to groups of users. These activities are normally beyond the administrative capability of that user – restarting the web server, for example. If frequent web server configuration changes are taking place (or the system has a bug and the web server keeps crashing), it becomes very cumbersome to continually engage the SysAdmin just to restart the web server. `sudo` allows the Administrator to delegate just that one task which relies upon `root` authority without allowing that group of users any other `root` capability.

Once `sudo` is installed, configure it using `visudo` – do not `vi` the config file. `visudo` has error checking built in specific to the `sudo` configuration. Experience has shown that if `/etc/sudoers` gets botched (from using `vi` without `visudo`'s error checking feature), recovery may become very difficult. Resorting to the boot media RESCUE environment may then be necessary.
Remediation:

Using the local Enterprise process, install sudo., then configure it as follows:

```
# The /etc/sudoers file contains one line that can be uncommented out to suitably
# permit SysAdmins with membership in the wheel group (i.e.  the same ones who
# 'could' su to root) to utilize 'sudo' instead.  Note: file consists of TABs
# between fields.  'visudo' IS the proper command to manually change this file,
# yet the change below passes muster when visudo is next executed.
echo "Implementing permissions for members of the wheel group to utilize sudo;"
echo "This prevents any user from having to 'su' to root for common"
echo "administrative tasks.  Ideally now the root password would be changed to
echo "something very few would know (hint!)."
sed 's/# %wheel   ALL=(ALL)   ALL/%wheel  ALL=(ALL)   ALL/' \
    /etc/sudoers-preCIS  >  /etc/sudoers
chown root:root /etc/sudoers
chmod 0440      /etc/sudoers
echo "diff /etc/sudoers-preCIS /etc/sudoers"
      diff /etc/sudoers-preCIS /etc/sudoers

echo "More specifically, system owners are strongly encouraged to more tightly"
echo "restrict who can utilize sudo on a name by name basis (explicitly) as well"
echo "as further restrict what commands those SysAdmins are limited to using."
echo "Align this with least-privilege."
```

Scoring Status: **Scorable**

SN.8 Lockout Accounts After 3 Failures

Description:
A system policy of locking out an account that fails several successive authentication attempts is an industry best practice, and is easily implemented in this Benchmark. The below value (deny=3) will cause the account to be locked out after 3 successive failed login attempts. This value is chosen as it is a common value used in some Federally-regulated industries – it can be increased, if that is desired.

Note: The below command assumes account lockouts are not already implemented on the system. If they are already implemented, edit `/etc/pam.d/system-auth` manually.

To unlock a user that has been locked out, use the `faillog` command. For example, to unlock user oracle, issue this command:

```
faillog -u oracle -r
```

See also the discussion at http://www.puschitz.com/SecuringLinux.shtml

Remediation:

```
# Part 1
# The removal affects the 'auth' and 'password' service types in that file.
cd /etc/pam.d
sed 's/ nullok//' /etc/pam.d-preCIS/system-auth  > system-auth

# Part 2
# Adding this option to the service type 'password' line, for 'pam_unix'.
/bin/cp -pf system-auth $tmpcis/system-auth.tmp
awk '( $1 == "password" && $3 == "pam_unix.so" ) { print $0 " remember=5"; next };
                                                 { print }'  \
                                          $tmpcis/system-auth.tmp > system-auth
# Part 3
```

```
# Must be set AFTER the above fix, as it needs to be done first.
# In the official PAM documentation, "deny=n; Deny access if tally for this user
# EXCEEDS n".  Where 'n' equals the number of attempts permitted.
# Set deny=2, as opposed to what the Benchmark recommends of '3'.
# Setting it to '3' will allow a 4th login attempt after 3 failed ones.
# Setting it to '2' will permit a total of 3 attempts.
# Table of meaning (positively tested in practice for proof):
# "deny=1" means 2 local attempts before lockout, but only 1 from SSH {remotely}
# "deny=2" means 3 local attempts before lockout, but only 2 from SSH {remotely}
# "deny=3" means 4 local attempts before lockout, but only 3 from SSH {remotely}
# "deny=4" means 5 local attempts before lockout, but only 4 from SSH {remotely}

# These two extra lines were properly integrated 'into' the standard PAM stacks,
# vice just being added to the end of the file.
/bin/cp -pf system-auth $tmpcis/system-auth.tmp
awk '( $1 == "auth" && $2 == "required" && $3 == "pam_deny.so" ) {         \
     print "# The following line added, per CIS Red Hat Enterprise Linux   \
            Benchmark sec SN.8, to harden the baseline image:";           \
            print "auth        required      pam_tally2.so onerr=fail      \
                  no_magic_root";  print $0; next };                       \
          ( $1 == "account" && $2 == "required" && $3 == "pam_permit.so" ) \
          { print "# The following line added, per CIS Red Hat Enterprise  \
               Linux Benchmark sec SN.8, to harden the baseline image:";  \
               print "account     required      pam_tally2.so deny=2      \
               no_magic_root reset"; print $0; next };                     \
          { print }' $tmpcis/system-auth.tmp > system-auth
chown root:root system-auth
chmod 0644      system-auth
echo "diff /etc/pam.d-preCIS/system-auth /etc/pam.d/system-auth"
      diff /etc/pam.d-preCIS/system-auth /etc/pam.d/system-auth
cd $cishome
chmod -R 0400 $tmpcis/*
```

Scoring Status: **Scorable**

SN.9 Additional Network Parameter Tunings

Description:
Before implementing these changes, please review them with the local environment in mind. The below value for `tcp_max_orphans` is much lower than the default 16,384, and may be too low, depending on the server's use and environment.

Also be aware that logging all `tcp_max_orphans` may generate an excessive amount of audit log data, especially on multi-homed servers with at least one network interface on a hostile network (i.e., the border firewalls). You should ensure you have plenty of log space available as well as sending the logs to a remote logging host.

Remediation:

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# The following 02 lines added, per CIS Red Hat Enterprise Linux Benchmark sec
SN.9, to harden the baseline image:
net.ipv4.tcp_max_orphans = 256
net.ipv4.conf.all.log_martians = 1
END_SCRIPT
chown root:root /etc/sysctl.conf
```

```
chmod 0600 /etc/sysctl.conf
echo "diff /etc/sysctl.conf-preCIS /etc/sysctl.conf"
      diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Scoring Status: **Scorable**

SN.10 Remove All Compilers and Assemblers

Description:
C compilers, and others, pose a credible high-risk threat to production systems and should not be installed. Compilers should be installed on select development systems – those systems that have a legitimate business need for a compiler – and the resulting output binaries deployed onto other development and production systems using the existing Enterprise change processes.

Note: Some failed dependencies may result when removing compilers and assemblers. Remove `gcc`'s dependencies first before removing `gcc`.

Remediation:
Question:
Is there a mission-critical reason to have a compiler or assembler on this machine?
If the answer is no, perform the action below.

The following command will identify the packages installed on the system:

```
rpm -qa | egrep "^gcc|java|bin86|dev86|nasm|as"
```

Remove the following packages (gcc, gcc3, gcc3-c++, gcc3-g77, gcc3-java, gcc3-objc, gcc-c++, gcc-chill, gcc-g77, gcc-java, gcc-objc, bin86, dev86, nasm and as), if they exist on the system, with this commands:

```
rpm -e gcc gcc3 gcc3-c++ gcc3-g77 gcc3-java gcc3-objc gcc-c++ gcc-chill gcc-g77
rpm -e gcc-java gcc-objc bin86 dev86 nasm as
```

If the answer is yes, then carefully evaluate why this system is a mission-critical, as the inclusion of compilers and the risks to a mission critical system are contradictory.

Packages can be removed by:

```
rpm -e <package name>
```

Scoring Status: **Scorable**

SN.11 Verify That No Unauthorized/Duplicate UID 0 Accounts Exists

Description:
Any account with UID 0 has superuser privileges on the system. The preferred and best practice for administrators obtaining superuser privileges, is to login with an unprivileged account in the wheel group, and then use `sudo` for the operations that require `root` level access. The `sudo` software is typically installed by default with Red Hat Enterprise Linux distributions; for details see the `sudo`(8), `sudoers`(5) and `visudo`(8) `man` pages or http://www.sudo.ws

Given that `sudo` is industry-accepted best practice, there is still the recognized occasional need for direct administrative console access as provided for in item 8.7 "Restrict Root Logins To System Console" . For these situations, having multiple uid 0 accounts may be used by experienced

administrators to provide individually assigned superuser passwords to eliminate or reduce usage of a shared `root` password, and to increase accountability. However some tools and situations do not always handle multiple uid 0 accounts as expected or desired, therefore testing is required. Specifically when booting to single user mode Item 8.9 "Require Authentication For Single-User Mode" the system will prompt for the "root" password, and none of the other uid 0 passwords will work. Also most of the GUI X-windows administration tools, if run by a non-privileged user, will prompt for the "`root`" password. There may be other applications or tools that behave unexpectedly, so testing is required.

Remediation:
The commands:

```
echo "The only single authorized entry is 'root'; any other entries here, (or"
echo "duplicates of root) must either be removed, or documented by the ISSO in the
SSP:"
echo "The second set of lines searches for inappropriate GID 0 groups.  Again,"
echo "a single listing of root is the only acceptable output."
echo "------------------------------------------------------------"
awk -F: '$3 == "0" { print $1 }' /etc/passwd
echo "------------------------------------------------------------"
awk -F: '$3 == "0" { print $1 }' /etc/group
echo "------------------------------------------------------------"
```

should return only the word "root", unless additional uid 0 accounts have been specifically authorized. Having multiple uid 0 accounts are acceptable if the accounts are authorized, but not recommended for some situations; see the discussion for more detail.

Scoring Status: **Scorable**

Appendix B: File Backup Script

```
#!/bin/bash
cishome="/root/cis"
echo "Creating $cishome/do-restore.sh"
cat <<END_SCRIPT > $cishome/do-restore.sh
#!/bin/bash

# This script restores those files changed by hardening IAW the CISecurity
# Benchmark
# Built by the RHEL Linux Benchmark do-backup.sh script.
# Errors for unalias get sent to the console when not 'set'
unalias rm mv cp    2> /dev/null

/usr/bin/chattr  -i  /etc/fstab /boot/grub/menu.lst /boot/grub/grub.conf
sed -n "39,9999p" $cishome/do-restore.sh | while read LINE; do
    #
    ####  When a file didn't exist before doing the back up
    ####  then the REPAIR should ensure the existing one is removed.
    #
    FILE=\`echo \$LINE | awk '{print \$1}'\`
    PERMS=\`echo \$LINE | awk '{print \$2}'\`
    echo "Restoring \$FILE with \$PERMS permissions"
    [ -f \${FILE}-preCIS ] && /bin/cp -pf \${FILE}-preCIS \${FILE}
    /bin/chmod \${PERMS} \${FILE}
    [ -f \${FILE}-preCIS ] && /bin/rm \${FILE}-preCIS
done

echo "Completed file restoration - restoring directories"
# Manually sorted the CIS file/dir list alphabetically, removed duplicates, and
# corrected
#       spacing to ease the finding/adding of new ones.
for DIR in \
    /etc/cron.*      \
    /etc/pam.d       \
    /etc/rc.d        \
    /etc/skel        \
    /etc/xinetd.d    \
    /var/spool/cron;
do
    if [ -d \${DIR}-preCIS ]; then
        echo "Restoring \${DIR}"
        /bin/cp -pr \${DIR}-preCIS \${DIR}
        /bin/rm -rf \${DIR}-preCIS
    fi
done

echo "If you installed Bastille, please run "
echo "'/usr/sbin/RevertBastille'; and examine its list of changed files as well."
exit 0

### END OF SCRIPT.  DYNAMIC DATA FOLLOWS.  ###
END_SCRIPT
chown root:root $cishome/do-restore.sh
chmod 0700      $cishome/do-restore.sh
echo " "

echo "Performing a modified 'do-backup.sh' (taken from the CIS v1.0.6 Benchmark)."
```

```
echo "Backing up individual system files, `date`"
# Manually sorted the CIS file/dir list alphabetically, removed duplicates, and
# corrected
#       spacing to ease the finding/adding of new ones.
# Files that don't natively exist in a virgin RHEL5 system:
        # /etc/at.allow
        # /etc/audit.rules
        # /etc/auditd.conf
        # /etc/cron.allow
        # /etc/ftpaccess
        # /etc/ftpusers
        # /etc/vsftpd.conf
        # /etc/vsftpd.ftpusers
        # /etc/vsftpd/vsftpd.conf
        # /etc/X11/xdm/Xservers
        # /etc/X11/gdm/gdm.conf
        # /etc/X11/gdm/PreSession/Default
        # /etc/X11/xinit/xserverrc
        # /etc/X11/xdm/Xresources
        # /etc/X11/xdm/kdmrc
        # /etc/xinetd.conf
        # /var/spool/cron

for FILE in \
    /boot/grub/grub.conf                            \
    /etc/aliases                                    \
    /etc/at.allow                                   \
    /etc/at.deny                                    \
    /etc/audit.rules                                \
    /etc/auditd.conf                                \
    /etc/audit/audit.rules                          \
    /etc/audit/auditd.conf                          \
    /etc/bashrc                                     \
    /etc/cron.allow                                 \
    /etc/cron.deny                                  \
    /etc/crontab                                    \
    /etc/csh.cshrc                                  \
    /etc/csh.login                                  \
    /etc/cups/cupsd.conf                            \
    /etc/exports                                    \
    /etc/fstab                                      \
    /etc/ftpaccess                                  \
    /etc/ftpusers                                   \
    /etc/group                                      \
    /etc/grub.conf                                  \
    /etc/gshadow                                    \
    /etc/hosts.allow                                \
    /etc/hosts.deny                                 \
    /etc/inittab                                    \
    /etc/issue                                      \
    /etc/issue.net                                  \
    /etc/login.defs                                 \
    /etc/mail/sendmail.cf                           \
    /etc/motd                                       \
    /etc/pam.d/su                                   \
    /etc/pam.d/system-auth                          \
    /etc/passwd                                     \
    /etc/profile                                    \
    /etc/proftpd.conf                               \
```

```
    /etc/securetty                                  \
    /etc/security/access.conf                       \
    /etc/security/console.perms                     \
    /etc/security/console.perms.d/50-default.perms  \
    /etc/security/limits.conf                       \
    /etc/shadow                                     \
    /etc/skel/.bashrc                               \
    /etc/ssh/ssh_config                             \
    /etc/ssh/sshd_config                            \
    /etc/sudoers                                    \
    /etc/sysconfig/sendmail                         \
    /etc/sysctl.conf                                \
    /etc/syslog.conf                                \
    /etc/vsftpd.conf                                \
    /etc/vsftpd.ftpusers                            \
    /etc/vsftpd/vsftpd.conf                         \
    /etc/X11/xdm/Xservers                           \
    /etc/X11/gdm/gdm.conf                           \
    /etc/X11/gdm/PreSession/Default                 \
    /etc/X11/xinit/xserverrc                        \
    /etc/X11/xdm/Xresources                         \
    /etc/X11/xdm/kdmrc                              \
    /etc/xinetd.conf                                \
    /root/.bash_profile                             \
    /root/.bashrc                                   \
    /root/.cshrc                                    \
    /root/.tcshrc                                   \
    /usr/share/config/kdm/Xservers                  \
    /var/spool/cron;
    do
        if [ -f ${FILE} ]; then
             # Backup files that exist (some might not)
             echo "Protected: `ls -lad ${FILE}`"    >> $cishome/do-restore.savelog
             /bin/cp -pf ${FILE} ${FILE}-preCIS
             # Add it to the do-restore script
             echo ${FILE} `find ${FILE} -printf "%m"`    >> $cishome/do-restore.sh
        else
             # This helps to compare various OS updates for correctness.
             echo "FILE didnt exist on this system ($FILE)." | tee -a \
                  $cishome/do-restore.savelog
        fi
    done

echo "Completed CIS file backups - backing up applicable directories"

# Manually sorted the CIS-provided file/dir list alphabetically, removed
# duplicates, and corrected spacing to ease the finding/adding/organization of new
# ones.
for DIR in \
    /etc/cron.*     \
    /etc/pam.d      \
    /etc/rc.d       \
    /etc/skel       \
    /etc/xinetd.d   \
    /var/spool/cron;
do
    # echo ${DIR}
    [ -d ${DIR} ] && /bin/cp -pr ${DIR} ${DIR}-preCIS
done
```

```
echo "Completed CIS RHEL Benchmark directory backups."

echo "(CIS) Recording log permissions"
find /var/log -printf "%h/%f %m\n" >> $cishome/do-restore.sh

echo "CIS Red Hat Enterprise Linux Backup protections are complete---`date`"
echo ""
```

Appendix C: Benchmark Change History

04 February 2008 - Version 1.0

- Initial Public Release
- Rewritten (as a major overhaul, based on the CIS RHEL4 Benchmark) to concentrate on RHEL5 exclusively; and applied CIS Benchmark Formatting Guide.
- Implementation of permissions were standardized throughout to be 4 characters, 0644, as opposed to 644. Every time a system file is modified, even though in different checks, the permissions are also set, this way each instance can be used uniquely and independently. This allows the end-user to positively know what the recommended permissions are. diff'ing was added to a number of checks that didn't have it previously. The placement of setting permissions and diff'ing was standardized for consistency.

April 2008 - Version 1.1

- Removed erroneous/confusing change history entries (held over from CIS RHEL4 Benchmark)

28 May 2009 - Version 1.1.1

- Resolved, addressed, corrected and improved the Benchmark based upon input registered via numerous Bugzilla and CIS Member forum posts regarding errors and recommendations to date for RHEL Benchmark v1.1. Specifically, the following have been resolved (in order of Bugzilla #):
  - Bugzilla 381; CIS 2.1 - Corrected recommendation on automating system patching.
  - Bugzilla 382; CIS 1 - Removed incomplete SELinux comment regarding `/.autorelabel`; inserted in more appropriate place: CIS 11.6 Reboot.
  - Bugzilla 383; CIS 2.3 – Subordinated "PubkeyAuthentication" to being a Level II BM issue.
  - Bugzilla 384; CIS 3.2 - Corrected narrative and logic for establishing `hosts.allow` and `hosts.deny` files. Addressed 3 items in this bugzilla (the first recommendation is *deferred* until the next major Benchmark edition, anticipated to be v1.2).
  - Bugzilla 385; CIS 4t - Marked the first six services in the Bugzilla as User Defined (UD) the identified entries in the table. The last is marked as required.
  - Bugzilla 387; CIS 4.6 - Removed items as requested and added cautionary language.
  - Bugzilla 388; CIS 4.15 - Corrected `httpd` as the proper name for the web service.
  - Bugzilla 389; CIS 5.2 - Removed zero within comment (it was for consistent spacing).
  - Bugzilla 393; CIS 8.9 - Removed unnecessary comments.
  - Bugzilla 395; CIS 9.3 - Removed zero within comment (it was for consistent spacing).
  - Bugzilla 396; CIS 9.10 - Incorporated comment regarding the inclusion of this within `/etc/profile`.
  - Bugzilla 398; CIS 10.1 - Corrected identification of what/where to name the organization. Fixed script syntax errors.
  - Bugzilla 400; CIS 11.1 - Removed references to RHEL4, trimmed comment, replaced audit rules in `audit.conf` in consultation with Red Hat.
  - Bugzilla 402; CIS 11.4 - Removed narrative and script text related to DISA SRR, accomplished throughout the Benchmark.
  - Bugzilla 403; CIS 11.5 - Clarified language regarding protection of man pages & doc info files.
  - Bugzilla 404; CIS 11.7 - Changed "script'lets" to "scriptlet", applied change throughout the Benchmark, also clarified language in regards to SELinux.
  - Bugzilla 405; CIS 8.5 - Removed extraneous comments in script.

- Bugzilla 406; CIS 9.11 - Incorporated recommended text that clarifies the changes made to `/etc/pam.d/su`.
- Bugzilla 425; CIS 2.3 - Corrected narrative and script language regarding the proper answer to be set for the `IgnoreRhosts` configuration entry; and the associated hardening script. Should be set to 'yes'.
- Bugzilla 480; CIS 2.3 - Addressed checking of some default values and methodology for doing this bit of hardening remotely.
- Bugzilla 481; CIS 1.0 SELinux section - Clarified language regarding utilization of SELinux in enforcing mode.
- Bugzilla 486; CIS 4t - Changed CIS Benchmark recommendation for the `yum-updatesd` service to be on (enabled) for both runlevels 3 and 5.
- Bugzilla 489; CIS 4t - Changed CIS Benchmark recommendation for the `anacron` service to be on (enabled) for both runlevels 3 and 5.
- Bugzilla 490; CIS 4t - Changed CIS Benchmark recommendation for the `lm_sensors` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 491; CIS 4t - Changed CIS Benchmark recommendation for the `ip6tables` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 493; CIS 4t - Changed CIS Benchmark recommendation for the `network` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 494; CIS 4t - Changed CIS Benchmark recommendation for the `smartd` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 495; CIS 4t - Changed CIS Benchmark recommendation for the `mdmonitor` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 496; CIS 4t - Changed CIS Benchmark recommendation for the `apmd` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 497; CIS 4t - Changed CIS Benchmark recommendation for the `iscsid` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 498; CIS 4 - Duplicate of Bugzilla 499.
- Bugzilla 501; CIS 4t - Resolved and remains as is.
- Bugzilla 504; CIS root env - Resolved and remains as is.
- Bugzilla 505; First Section, "About Bastille", Removed language.
- Bugzilla 506; SN.7 - Revised script to remove comment hash mark from correct line in system file (so that the `NOPASSWD` like is not selected).
- Bugzilla 507; CIS 9.8 - Clarified language addressing the removal of `.netrc` files.
- Bugzilla 511; CIS 6.4 - Corrected script with leading hash for the comment (good catch!).
- Bugzilla 512; CIS 6.4 - Incorporated recommended change to the script.
- Bugzilla 513; CIS 2.3 - Duplicate of Bugzilla 425.
- Bugzilla 514; CIS 2.3 - Corrected language describing security of the Port option.
- Bugzilla 517; CIS 4.2 - Corrected language.
- Bugzilla 518; CIS 4.3 - Incorporated new language.
- Bugzilla 519; CIS 7.1 - Fixed script to avoid string concatenation when encountering longer than default fields.
- Bugzilla 520; CIS 3.7 & CIS 3.8 - These were not `xinetd` services. Moved them into section 4 where they belong (to 4.21 and 4.22, respectively).
- Bugzilla 521; CIS 3.1t - Included language about not all `xinetd` services are necessarily deprecated, nor do they all have secure alternatives.
- Bugzilla 524; CIS 4t - Changed CIS Benchmark recommendation for the `rhnsd` service to be User Defined (UD) for both runlevels 3 and 5.

- Bugzilla 525; CIS 4t - Changed CIS Benchmark recommendation for the `sendmail` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 526; CIS 4.3 - Removed incorrect and confusing language.
- Bugzilla 529; CIS 7.2 - Removed language in the narrative and script regarding "chattr +i".
- Bugzilla 532; First Section - Standardized capitalization for paragraph headers.
- Bugzilla 536; Corrected spelling mistakes; accomplished throughout the document.
- Bugzilla 537; First Section - Clarified explanation and usage of RPM commands in regards to service discovery and package exploration/research. Added link to Red Hat documentation for package management.
- Bugzilla 540; Housekeeping - Applied recommendation for dynamic/random creation of tmp directory used; applied throughout the Benchmark.
- Bugzilla 542; CIS 2.2 - Clarified language about errors and places to check when validating a system before accomplishing Benchmark Hardening.
- Bugzilla 543; CIS 2.3 - Clarified language regarding PubKey Authentication, versus passwords.
- Bugzilla 548; CIS 3.3 - Deleted comma in title.
- Bugzilla 551; CIS 3.8 (old #)/CIS 4.22 (new #) - corrected spelling for `dovecot`.
- Bugzilla 556; CIS 4.8 - Added language of services needed for NFS Server, and also added `nfslock` as a required service to enable at that time.
- Bugzilla 557; CIS 4t - Resolved, ensured all defaults were listed.
- Bugzilla 559; CIS 4t - Changed CIS Benchmark recommendation for the `mdmonitor` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 560; CIS 4t - Changed CIS Benchmark recommendation for the `lm_sensors` service to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 562; CIS 4t - Changed CIS Benchmark recommendation for the `readahead_early` and `readahead_later` services to be User Defined (UD) for both runlevels 3 and 5.
- Bugzilla 629; CIS 6.3 - Removed hash mark as recommended.
- Bugzilla 632; CIS 8.6 - Resolved
- Bugzilla 634; CIS 9.5 - Removed unnecessary comment.
- Bugzilla 635; CIS 9.11 - Applied recommendation.
- Bugzilla 637; CIS 11.1 - Cleaned up script as recommended.
- Bugzilla 638; CIS 11.4 - Cleaned up script as recommended.
- Bugzilla 639; CIS 11.6 - Removed section.
- Bugzilla 640; CIS 11.7 - Corrected unix case for 'touch' command.
- Bugzilla 641; CIS 12 - Updated license info for recommended A/V products.
- Bugzilla 647; CIS 11.2 - Replaced existing script with recommendation.
- Bugzilla 655; CIS 6.1 - Revised the script as recommended.
- Bugzilla 668; CIS 2.3 – Subordinated "PassowrdAuthentication no" as a Level II BM issue though leaving it in the same ‘section’ for the moment as a recommendation.

- Additional v1.1.1 changes include (not bugzilla related):
  - Partitioning Considerations - Massively revised the narrative and guidance recommendations, removed `/opt` and `/usr` as required partitions, and clarified focus on implementation of a `/home` partition.
  - Root Shell Environment Is Required - Clarified as an example the required path.
  - CIS 2.3 - Improved language for SSH Client and Server modules to be more specific.
  - CIS 3.2 - Standardized usage of "TCP Wrappers" consistently.
  - CIS 4t - Included `postfix` into the table of services.
  - CIS 4.18 - Standardized usage of "PostgresSQL" consistently.

- CIS 7.9 - Eliminated reference to "FC5" in this RHEL5 Benchmark.
- CIS 8.1 - Corrected filenames in the script to apply to this section.
- CIS 9.11 - Improved script and added usage for the admin userID list.
- CIS 9.5 - Elaborated on reasons why not to have a '.' in the `$PATH`.
- CIS 10.1 – Added '`centos`' into the `egrep` line for OS banner text.
- CIS 11.4 - Revised password complexity minimums to "`-1`" as a standard.
- Spelling corrections, line and paragraph alignment and tightened pagination. Also, did a better job of standardizing "SysAdmin" as the reference term for system administrators.

Appendix D: References

The Center for Internet Security

Free Benchmark documents and security tools for various OS platforms and applications:
http://www.cisecurity.org

Red Hat Software

Patches and related documentation:
https://www.redhat.com/security

Red Hat Update Manager tools:
yum:
https://rhn.redhat.com/help/latest-up2date.pxt
https://rhn.redhat.com
yum: http://www.linuxgazette.com/node/view/8835

HAL:
http://www. redhat.com/magazine/003jan05/features/hal

Other Misc Documentation

Various documentation on Linux security issues:
https://www. redhat.com/security

Primary source for information on NTP:
http://www.ntp.org

Information on MIT Kerberos:
http://web.mit.edu/kerberos/www

Apache "Security Tips" document:
http://httpd.apache.org/docs-2.0/misc/security_tips.html

Information on Sendmail and DNS:
http://www.sendmail.org
http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf

OpenSSH (secure encrypted network logins):
http://www.openssh.org

TCP Wrappers source distribution:
ftp.porcupine.org

PortSentry and Logcheck (port and log monitoring tools):
http://sourceforge.net/projects/sentrytools

Swatch (log monitoring tool):
http://www.oit.ucsb.edu/~eta/swatch

Open Source Sendmail (email server) distributions:
ftp://ftp.sendmail.org

LPRng (Open Source replacement printing system for Unix):
http://www.lprng.org
sudo (provides fine-grained access controls for superuser activity):
http://www.courtesan.com/sudo

Tripwire – file modification utility:
http://www.tripwire.org

Ref. #	Reference Books
A	Mike Shema, et al., **Anti-Hacker Tool Kit, 3rd Ed.**, Osborne & McGraw Hill Press, 2006
B	Center for Internet Security (CIS), **CIS Red Hat Linux Security Benchmark Scoring Tool v1.2 and Hardening Reference Guide, v1.0.5**, Nov 2006; www.cisecurity.org
C	Cricket Liu and Paul Albitz, **DNS and BIND, 5th Ed.**, O'Reilly and Associates, 2006
D	Aeleen Frisch, **Essential System Administration, 2nd Ed.**, O'Reilly and Associates, 1991
E	Richard Petersen, **Fedora 7 and Red Hat Enterprise Linux, The Complete Reference**, Osborne & McGraw Hill Press, 2007
F	Christopher Negus, Francios Caen, **Fedora Linux Toolbox**, Wiley, 2008
G	NSA, **Guide to the Secure Configuration of Red Hat Enterprise Linux 5, Rev 1**, System and Network Analysis Center, National Security Agency, Dec 13, 2007
H	Nitesh Dhanjani, **Hack Notes - Linux and Unix Security**, McGraw Hill/Osborne Press, 2003
I	James Turnbull, **Hardening Linux**, Apress publishing, 2005
J	National Security Agency/Central Security Service, **Information Assurance Technical Framework (IATF) v3.1**, Sep 2002
K	Evi Nemeth, et al., **Linux Administration Handbook, 2nd Ed.**, Prentice Hall, 2007
L	Michael Jang, **Linux Annoyances For Geeks**, O'Reilly and Associates, 2006
M	Mark G. Sobell, **Linux Commands, Editors and Shell Programming**, Prentice Hall, 2005
N	Steve Suehring, **Linux Firewalls, 3rd Ed.**, Novell Press, 2006
O	Jessica Perry Hekman, **Linux in a Nutshell**, O'Reilly and Associates, 1997
P	Roderick W. Smith, **Linux in a Windoze World**, O'Reilly and Associates, 2005
Q	Tony Bautts, **Linux Network Administrator's Guide, 3rd Ed.**, O'Reilly and Associates, 2005
R	Daniel J. Barrett, **Linux Security Cookbook**, O'Reilly and Associates, 2003
S	Bill von Hagen, et al., **Linux Server Hacks, Volume Two**, O'Reilly and Associates, 2006
T	Christopher Negus and Thomas Weeks, **Linux Troubleshooting Bible**, Wiley, 2004
U	James Kirkland, **Linux Troubleshooting for System Administrators and Power Users**, Prentice Hall/HP Press, 2006
V	Hal Stern, **Managing NFS and NIS**, O'Reilly and Associates, 1991
W	Kerry Cox, **Managing Security with SNORT and IDS Tools**, O'Reilly and Associates, 2004
X	Jeffrey E.F. Friedl, **Mastering Regular Expressions**, O'Reilly and Associates, 1997
Y	Chris McNab, **Network Security Assessment**, O'Reilly and Associates, 2004
Z	Mark G. Sobell, **A Practical Guide to Linux, 3rd Ed.**, Prentice Hall, 2005
AA	Mark G. Sobell, **A Practical Guide to Linux, Commands, Editors, and Shell Programming.**, Prentice Hall, April 2007
AB	Bob Toxen, **Real World Linux Security, 2nd Ed.**, Prentice Hall, 2003
AC	RedHat Network, **RedHat Enterprise Linux AS4 Documentation DVD**; RedHat, Inc., 2006
AD	Kapil Sharma, et al., **Red Hat Enterprise Linux 3, Professional**, WROX Publishing, 2004
AE	Tammy Fox, **Red Hat Enterprise Linux 5 Administration**, SAMS Publishing, 2007
AF	Paul Hudson, et al., **Red Hat Fedora Core 4, UNLEASHED**, SAMS Publishing, 2005
AG	Paul Hudson, et al., **Red Hat Fedora Core 5, UNLEASHED**, SAMS Publishing, 2006
AH	Christopher Negus, **Red Hat Fedora 7 and RedHat Enterprise Linux 5 Bible**, Wiley, 2007
AI	System Administration Network Security Organization (SANS), **SANS, Top 20 2007 (compilation of the 20 top exploited vulnerabilities)**, www.sans.org
AJ	Bryan Burns, et al., **Security Power Tools**, O'Reilly and Associates, 2007
AK	Bill Mccarty, SELinux; **SELinux - NSA's Open Source Security Enhanced Linux**, O'Reilly and Associates, 2005
AL	Chris Anley, et al., **Shellcoder's Handbook, The, 2nd Ed**, Wiley, 2007

Ref. #	Reference Books
AM	Amanda Andress, **Surviving Security, 2nd Ed**, Auerbach Publications, 2004
AN	Daniel J. Barrett, **SSH The Secure Shell, 2nd Ed.**, O'Reilly and Associates, 2005
AO	Gian-Paolo D. Musumeci, Mike Loukides, **System Performance Tuning**, O'Reilly and Associates, 2002
AP	National Security Agency/Central Security Service (NSA/CSS), **The 60 Minute Network Security Guide**, NSA/CSS, May 15, 2006
AQ	Arnold Robbins, **Unix in a Nutshell, 3rd Ed.**, O'Reilly and Associates, 1999
AR	Jerry Peek, Tim O'Reilly, Mike Loukides, **Unix Power Tools**, O'Reilly and Associates, 1993
AS	Defense Information Systems Agency (DISA), **DISA Unix Security Technical Implementation Guide (STIG)** (28 March 2006), and **Unix Checklist** (dated: 15 February 2009)
AT	Ellie Quigley, **Unix Shells by Example**, Prentice Hall, 2005