Center for Internet Security Benchmark for Debian Linux v1.0

August, 2007

Editor: Blake Frantz
Leviathan Security Group

http://cisecurity.org
cis-feedback@cisecurity.org

Table of Contents

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**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, or 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 the Products or the Recommendations. 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:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. 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;
4. 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;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. 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:

1. 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;
2. 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.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

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.

Terms of Use Agreement Version 2.1 – 02/20/04

Introduction

Conventions
The following typographical conventions are used in this document:

Roman font	normal text
`Courier`	`used to indicate either a command or a standard UNIX parameter or file.`
Italics	*used for a question that you must evaluate before continuing*

Root Shell Environment Assumed
The actions listed in this document are written with the assumption that they will be executed by the root user running the bash shell and without `noclobber` set. Also, the following directories are assumed to be in root's path:
`/bin:/sbin:/usr/bin:/usr/sbin`

Executing Actions

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

Reboot Required
Rebooting the system is required after completing all of the actions below 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, you may have to reboot more than once.

Vulnerabilities
In addition to any specific issues presented by a particular service or protocol, **every** service has the potential of being an entry point into a system if a vulnerability is found. This is why we recommend that some services are disabled even though there is no clear way to exploit them, and there has never been a problem with the service. If you are running an unnecessary service, you add additional risks of a vulnerability being found in the service in the future.

Backup Key Files
Before performing the steps of this benchmark 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 script provided in Appendix B of this document will automatically back

up all files that may be modified by the actions below. Note that an executable copy of this 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 `/root/do-restore.sh`, which is dynamically generated based on the results of the `do-backup.sh` script. To roll back the changes performed by this benchmark, first run `RevertBastille` followed by `do-restore.sh`, and all changes will be backed out. Since not all Linux installations are identical, the `do-restore.sh` script is created based on the files that actually existed at the time `do-backup.sh` was run.

Note: If you make any 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 may be prudent to delete the do-restore.sh script once you have validated the changes to prevent inadvertently undoing the changes.

Build Considerations

If you have not done so already, plan out a partitioned hard drive. By creating a robust partition scheme an administrator can mitigate the threat of common local attacks, such as those based on hard links and consuming available partition space. The first step in achieving this is to place user-writable directory structures on a separate partition. This includes `/home, /tmp,` and `/var/tmp`. Additionally, any directory structure that may variably consume large quantities of disk space should also be placed on separate partitions. This includes `/var/log` and `/var/spool/mail`, where applicable. Note: Debian will download and store packages at `/var/cache/apt/archives`. Some administrators may find it easier to create a separate partition for the entire `/var` directory structure. To limit the inconveniences caused by filling up `/home`, consider implementing user and group quotas on the `/home` file system. Quotas will limit how much a single user (or single group) can store on a given file system. More information is available at http://www.debian-administration.org/articles/47.

Software Package Removal

There is considerable debate over the maintenance 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 makes no recommendation for the removal of unused software. If 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 risks thereof.

Software Package Installation

Throughout this Benchmark, you may be directed to enable software package init scripts using the `update-rc.d` command. This assumes you already installed said package(s). If the `update-rc.d` command fails, verify you actually installed the software required.

1 Pre-Installation and Installation Recommendations

1.1 Subscribe to Debian Security Lists

Debian maintains the `debian-security-annouce` mailing list for the purpose of providing timely information on security problems discovered within the Debian packages. It is recommended that Debian administrators subscribe to this list to keep abreast of security issues that may impact their environment. To subscribe to this list, visit http://lists.debian.org/debian-security-announce/. Administrators should also consider subscribing to the `debian-security` mailing list to discuss general security issues in Debian. To subscribe to this list, visit http://lists.debian.org/debian-security/.

1.2 Establish a BIOS Password

Before installing Debian, your organization may choose to establish a strong BIOS password. Establishing a strong BIOS password will reduce the exposure of a system compromise via physical access. However, establishing a BIOS password has the potentially negative effect of limiting the ability to remotely reboot the server. Some BIOS' may be configured to require a password upon modifying the BIOS but not upon boot; this is the preferred settings.

1.3 Configure BIOS Boot Devices

An additional countermeasure to slightly mitigate the threat of a physical attack is configuring the BIOS boot sequence. One can accomplish this by disabling the server's ability to boot off all non-harddisk devices, including floppy, CD-ROM, and USB.

1.4 Create a Robust Partition Scheme

By creating a robust partition scheme an administrator can mitigate the threat of common local attacks, such as those based on hardlinks and consuming available partition space. The first step in achieving this is to place user-writable directory structures on a seperate partition. This includes `/home`, `/tmp`, and `/var/tmp`. Additionally, any directory structure that may variabley consume large quantities of disk space should also be placed on seperate partitions. This includes `/var/log` and `/var/spool/mail`, where applicable. Note: Debian will download and store packages at `/var/cache/apt/archives`.

Minimally, the following conditions should must exist:

- user writable directories (i.e /tmp) should have their own partitions to prevent hardlink attacks
- /var and /opt should should not share a partition with the system root '/'
- /var and /opt should should not share a partition with the system root '/'

To limit the inconveniences caused by filling up /home, consider implementing user and group quotas on the /home file system. Quotas will limit how much a single user (or single group) can store on a given file system

1.5 File System Considerations

Depending on the role of the server, the file system may have a significant impact on performance and availability. By default, the Debian installer will select a journalling file system, `ext3`. This file system is generally recommended in most scenarios as it increases system availability and data integrity in the event of a system crash by requiring less time to perform file system checks and by ensuring that file data updates are flushed to disk before any transactions commit. A potential downfall to the `ext3` file system is a reduced ability to recover deleted files via `undelete` or `debugfs`.

1.6 Set a Secure Root Password

After the base installion is complete, the Debian installer will prompt for a root password. It is essential to the integrity of the system that a complex and nondeterministic root password is selected. Consult your organization's password policy requirements for additional requirements or follow these guidelines:

* Passwords must be eight or more characters long
* Passwords must contain at least three character classes (upper, lower, numeric, etc)
* Passwords must not be simple variations of dictionary words or proper names i.e Password1

1.7 Package Selection

The Debian installer provides templates for common roles such as Web Server, DNS Server, FTP Server, Workstation, etc. It is recommended that administrators manually configure package selections to ensure that only required packages are installed.

2 Patches, Packages and Initial Lockdown

2.1 Apply Latest OS Patches

Action:

Update system per your enterprise update procedures. For non-enterprise environments, and or environments without a formal update procedure use either aptitude or one of the other packages management tools offered by Debian. Debian recommends the use of aptitude as it is the most sophisticated package management tool offered by this distribution.

```
aptitude update
aptitude dist-upgrade
```

Discussion

Debian maintains the debian-security-announce mailing list for the purpose of providing timely information on security problems discovered within the Debian packages. It is recommended that Debian administrators subscribe to this list to keep abreast of security issues that may impact their environment. To subscribe to this list, visit http://lists.debian.org/debian-security-announce/. Administrators should also consider subscribing to the debian-security mailing list to discuss general security issues in Debian. To subscribe to this list, visit http://lists.debian.org/debian-security/.

Developing a 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 Debian publishes an update, they include the procedures with it for updating the package. This usually entails downloading the new packages (.deb) from Debian, and making them available to the individual servers. Some enterprises make these packages available over an NFS share or an internal anonymous FTP/HTTP server - your enterprise may follow this practice or do something different.

It is also important to observe that your applications work properly after patching. Though problems in patches are quite rare in Debian Linux 3.1, it is generally recommended that any patch be deployed to a non-production system first for testing.

Finally, there is some risk to using a non-patched, non-hardened machine to download the patches, as this involves connecting a system with security vulnerabilities on a network, which is not an industry best practice. Please consider these issues carefully.

Debian offers at least partially automated patch download and installation, via `apt-get` and `aptitude`. Consider using `apt-get` or `aptitude` whenever Debian announces a vulnerability. If your enterprise has several servers, consider installing an update server that can be used in place of Debian's package servers - the updates will go much faster, you will use much less bandwidth from your ISP, and you will reduce the load on Debian's servers. This can be accomplished via `apt-proxy`, `apt-mirror`, or `apt-move`. It is recommended that patches be validated and functionality regressed in a lab environment before applying to live/production systems.

2.2 Validate Your System Before Making Changes

Action:

Ensuring your system is functioning properly before you make a change is a prudent system administration best practice and will save you hours of aggravation. Applying this Benchmark to a system that already has issues makes troubleshooting very difficult and may lead you to believe the Benchmark is at fault.

Examine the system and application logs (`/var/log`). Key words to look for include, but are not limited to, "error", "warning", "critical", and "alert".

Resolve all issues before continuing

2.3 Configure SSH

Action:

```
unalias cp rm mv
cd /etc/ssh
cp ssh_config ssh_config.tmp
cat /etc/ssh/ssh_config.tmp | grep -v Protocol | sed '$a\\nProtocol 2'
> /etc/ssh/ssh_config
rm ssh_config.tmp
diff ssh_config-preCIS ssh_config
cp sshd_config sshd_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
/^#? *X11Forwarding/ \
{ print "X11Forwarding yes"; next };
/^#? *IgnoreRhosts/ \
{ print "IgnoreRhosts yes"; next };
/^#? *RhostsAuthentication/ \
{ print " RhostsAuthentication no"; next };
/^#? *RhostsRSAAuthentication/ \
{ print "RhostsRSAAuthentication no"; next };
/^#? *HostbasedAuthentication/ \
{ print "HostbasedAuthentication no"; next };
/^#? *PermitRootLogin/ \
{ print "PermitRootLogin no"; next };
/^#? *PermitEmptyPasswords/ \
{ print "PermitEmptyPasswords no"; next };
/^#? *Banner/ \
{ print "Banner /etc/issue.net"; next };
{print}' sshd_config.tmp > sshd_config
rm sshd_config.tmp
diff sshd_config-preCIS sshd_config
```

Discussion

OpenSSH is a popular free distribution of the standards-track SSH protocols which has become the standard implementation on Linux distributions. For more information on OpenSSH, see http://www.openssh.org.

The settings in this section attempt to ensure safe defaults for both the client and the server. Specifically, both the ssh client and the sshd server are configured to use only SSH protocol 2, as 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.

Note that a banner is added in the sshd_config file – we will create this banner later and it is discussed in detail in section 9. If you choose not to implement a banner, you will have to remove the reference to /etc/issue from sshd_config manually. Please read the section on the legal use of banners before deciding to remove it.

2.4 Enable System Accounting

Action:

```
aptitude install sysstat
cd /etc/default
cp sysstat sysstat.tmp
awk '/^ENABLED/ { print "ENABLED=true"; next }; { print }' sysstat.tmp
> sysstat
rm sysstat.tmp
```

Discussion

System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 10 minutes. The data may be accessed with the `sar` command, or by reviewing the nightly report files named `/var/log/sysstat/sar*`. Once a normal baseline for the system has been established, 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. Note that this data is only archived for one week before being automatically removed by the regular nightly cron job. Administrators may wish to archive the `/var/log/sysstat/` directory on a regular basis to preserve this data for longer periods.

2.5 Install and Run Bastille

Action:

```
aptitude install bastille
cd /etc/Bastille
cp /path/to/bastille.CIS.conf config
bastille -b
init 6
```

Discussion

Bastille is a series of perl scripts that ask you questions and hardens your machine based on the answers. The Benchmark will then walk you through opening up your system for the services that have a legitimate business need.

In this benchmark, it was decided it is better to direct you to use Bastille rather than incorporate their procedures into this document. This provides fair credit to an excellent resource, and reduces the maintenance effort involved to keep this Benchmark up to date. Appendix C discusses the rationale behind all of the answers used in the configuration file.

After Bastille is installed, copy the bastille.CIS.conf file provided in the archive containing the PDF version of this document (and in Appendix C) to /etc/Bastille/config.

Note Regarding SUID Programs:

Bastille will remove the SUID bit from several utilities like `ping`, `mount` and `traceroute`. If your enterprise has a business need to allow unprivileged users access to these commands, then you will have to restore the SUID bit (`chmod 4755`) after running Bastille. A complete list of files changed is in Appendix B. Before running Bastille, please review Appendix C and understand the changes that it will make. The following commands will install Bastille, copy the CIS configuration file to the appropriate location, execute Bastille, which will commit changes to your system, and finally reboot. Rebooting is required as many services are disabled by Bastille and the remainder of the Benchmark is based on this environment.

2.6 Ensure sources.list Sanity

Action:

```
cat /etc/apt/sources.list
```

Discussion

Debian manages software packages via the Advanced Package Tool (APT). An administrator may interact with the APT library via many utilities including `dselect(8)`, `aptitude(8)`, and `apt-get(8)`. All of which obtain instruction on where to locate packages from `/etc/apt/sources.list`. Ensuring that this file contains sane values is essential. Administrators should validate that each entry in this file points to a trusted and secure location. Additionally, to obtain latest security updates, this file should contain an entry akin to:

```
deb http://security.debian.org/ stable/updates main contrib non-free
```

For further information on the `/etc/apt/sources.list` file, run `man sources.list` from the shell.

3 Minimize inetd network services

You may need to unalias `mv` and `cp` commands as some commands to avoid being prompted numerous times while configuring this section.

Action:

```
unalias mv cp
```

3.1 Disable Standard Services

Note: Bastille configuration may not cover all these services

Action:

```
cp /etc/inetd.conf /etc/inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^\([[:alpha:]]\)/#\1/' > inetd.conf
rm /etc/inetd.conf.tmp
```

Discussion

Debian utilizes `inetd` as the default network superserver.

Debian, by default, has only `ident` enabled within `inetd.conf`. However, servers may have had various inetd-aware services installed. The actions in this group will disable all standard services commonly enabled in a `inetd` configuration.

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. If there is any doubt, it is better to disable everything, then re-enable the necessary services based on the function of the server.

3.2 Configure TCP Wrappers and Firewall to Limit Access

Question:
Is there a reason to allow unlimited network access to this server?
If the answer to this question is no, then perform the following action below.

Note: Bastille configuration set to 'No'
Note: Do not deny access to your system without allows access. Complete both parts of this section.

TCP Wrappers

By limiting access to the server, you reduce your exposure to threats from attackers on remote systems. 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. Many daemons (SSH for example) are compiled with TCP Wrapper support, so you can use `/etc/hosts.allow` and `/etc/hosts.deny` to limit SSH access to your systems. It is important to note that TCP wrappers looks at `hosts.allow` first, then `hosts.deny`, and controls access based on the first match. If you omit entries in `hosts.allow` and deny access to ALL in `hosts.deny`, you will block network access to all network clients.

Deny access to this server from all networks:

```
echo "ALL: ALL" > /etc/hosts.deny
diff /etc/hosts.deny-preCIS /etc/hosts.deny
```

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, you need to allow localhost traffic. The following script will create a sample `hosts.allow` file that will allow access to the locally connected networks:

```
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 printf ", $I." >> /etc/hosts.allow
done
echo >> /etc/hosts.allow
diff /etc/hosts.allow-preCIS /etc/hosts.allow
```

Note: The above script intentionally ignores IPv6 networks
Note: The above script assumes a netmark of 255.255.255.0. if yours is different, you will have to adjust `/etc/hosts.allow` for your environment.

You should review the resulting `/etc/hosts.allow` to ensure it meets your needs. Test your configuration now by logging in remotely.

Firewall
See discussion.

Discussion

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, you reduce your exposure to threats from attackers on remote systems. 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.

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

It is important to note that TCP wrappers looks at `hosts.allow` first, then hosts.deny, and controls access based on the first match. If you omit entries in `hosts.allow` and deny access to ALL in hosts.deny, you will block network access 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 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 commercial offerings. The Center for Internet Security makes no recommendations for a vendor or even a specific firewall configuration as firewalls are very complex systems. Entire books have been written on iptables and are outside the scope of this benchmark. The default Bastille Linux 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 firewall as manual rule configuration is extremely error-prone and you may end up with a false sense of security and have less secure system.

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.

3.3 Only Enable telnet If Absolutely Necessary

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, proceed with the actions below.

Action:

```
cd /etc
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#telnet/telnet/' > inetd.conf
rm inetd.conf.tmp
```

Discussion:
`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 Debian 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/). There are numerous commercially supported SSH clients as well – check to see if your 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.

Note: `telnet` is not enabled by default on Debian.

3.4 Only Enable FTP If Absolutely Necessary

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 service, rather than `sftp` or `scp`?
If the answer to this question is yes, proceed with the action that corresponds with the FTP services you have installed.

Action:

```
update-rc.d vsftpd defaults
update-rc.d wu-ftpd dafaults
cd /etc/
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#ftp/ftp/' > inetd.conf
rm inetd.conf.tmp
```

Discussion:

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 are 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 – which should be used instead. Even if FTP is required, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols.

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.

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.

Note: Debian does not install a default FTP daemon.

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

Note: `ftp` services are not enabled by default on Debian.

3.5 Only Enable rlogin/rsh/rcp If Absolutely Necessary

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, proceed with the actions below.

Action:

```
cd /etc
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#l\(shell\|login\)/\1/' > inetd.conf
rm inetd.conf.tmp
```

Discussion:

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 X.X for additional security-related configuration settings.

Note: `r-services` are not enabled by default on Debian.

3.6 Only Enable TFTP If Absolutely Necessary

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?

Action:

```
cd /etc
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#tftp/tftp/' > inetd.conf
rm inetd.conf.tmp
```

Discussion:

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 Debian Linux.

3.7 Only Enable IMAP If Absolutely Necessary

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.

Action:

```
cd /etc
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#imaps/imaps/' > inetd.conf
rm inetd.conf.tmp
```

Discussion:

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, `uw-imap-ssl` may be activated. `uw-imap-ssl` activates an SSL-encrypted, and thus much safer, version of IMAP. Standard IMAP is not encrypted and allows an attacker to eavesdrop on 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. IMAP-SSL suffers none of these problems.

Note: The `uw-imapd-ssl` package is not installed by default on Debian Linux.

3.8 Only Enable POP If Absolutely Necessary

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.

Action:

```
update-rc.d popa3d defaults
```

Discussion:

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, `popa3d` may be activated. Note: The `popa3d` package is not installed by default on Debian Linux. You will have to install it if you need to use it. After installing it, perform the following actions to ensure it's enabled.

Note: The `popa3d` package is not installed by default on Debian Linux.

3.9 Only Enable Ident If Absolutely Necessary

Only Enable Ident If Absolutely Necessary
Does this machine interact with a service that requires Ident? If the answer to this question is yes, proceed with the actions below
Some services, like SMTP, may be configured to perform an Ident request prior to further processing of the request. If this system participates with a service that requires Ident responses, pidentd" may be installed.

```
cd /etc
cp inetd.conf inetd.conf.tmp
cat inetd.conf.tmp | sed 's/^#ident/ident/' >inetd.conf
rm inetd.conf.tmp
```

4 Minimize boot services

4.1 Disable inetd, If Possible

Action:

```
if [ `egrep -v '^(#|[[:space:]]|$)' /etc/inetd.conf | wc -l` -eq 0 ]
then echo "Disabling inetd"; update-rc.d -f inetd remove;
fi
```

If the actions in Section X of this benchmark resulted in no services being enabled in the inet super daemon `/etc/inetd.conf`, then the `inetd` service may be disabled completely on this system.

Experienced SysAdmins will note that the inet super daemon is usually 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.

4.2 Disable sendmail Server, If Possible

Question:

Is this system a mail server – that is, does this machine receive and process email from other hosts? Note: The email server need not be running to send outgoing mail.

Proceed with the appropriate actions below.

Action - Yes - sendmail is required:

```
cd /etc/mail
cp -pf sendmail.conf-preCIS sendmail.conf
chown root:root sendmail.conf
chmod 644 sendmail.conf
/usr/sbin/sendmailconfig
```

Action - No - sendmail is not required:

```
cd /etc/mail
cp sendmail.conf sendmail.conf.tmp
awk '/^DAEMON_MODE/ { print "DAEMON_MODE=\"none\";"; next }; { print }'
sendmail.conf.tmp > sendmail.conf
/usr/sbin/sendmailconfig
rm sendmail.conf.tmp
```

Discussion:

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. Running Sendmail in "daemon mode" (with the -bd command-line option) is only required on machines that act as mail servers, receiving and processing email from other hosts on the network. Note that if the system is an email server, the administrator is encouraged to search the Web for additional documentation on Sendmail security issues. Some information is available at http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf and at http://www.sendmail.org.

Although Sendmail may be configured to listen only to the loopback network interface, this document still deactivates "daemon mode." Listening on the loopback interface still presents a slightly higher level of exposure to attack than not listening at all. Experienced administrators will understand that a chroot-jailed user or program can still interact with a Sendmail process listening on the loopback interface.

4.3 Disable GUI Login If Possible

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.

Action:

```
sed -e 's/id:5:initdefault:/id:3:initdefault:/' \
> /etc/inittab-preCIS > /etc/inittab
chown root:root /etc/inittab
chmod 0600 /etc/inittab
diff /etc/inittab-preCIS /etc/inittab
```

Discussion:

There is usually no reason to run X Windows on a dedicated server machine, like a dedicated web server. This action disables the graphical login, if present, leaving the user to login via SSH or a normal text-based console. If you elect to deactivate the GUI login screen, users can still run X Windows by typing startx at the shell prompt. GUI login is activated or deactivated by changing this runlevel in /etc/inittab. Again, note that runlevel 3 still allows the user to run X Windows by typing startx at the shell prompt.

4.4 Disable X Font Server If Possible

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.

Action:

```
update-rc.d -f xfs remove
```

Discussion:
There's usually no reason to run X Windows on a dedicated server machine, like a dedicated web server. If you won't be using an X server on this machine, this action will deactivate the font server.

4.5 Disable Standard Boot Services

Action:

```
for FILE in nfs-common nis \
portmap samba nfs-user-server nfs-kernel-server lpd apache apache2
snmpd \
bind postgresql mysql webmin squid nis wu-ftpd vsftpd hpoj cupsys \
exim4 hotplug popa3d sendmail nmbd pcmcia bluez-utilz;
do
/etc/init.d/$FILE stop
update-rc.d -f $FILE remove
done
```

Discussion

Every system daemon that does not have a clear and necessary purpose on the host should be deactivated. This greatly reduces the chances that the machine will be running a vulnerable daemon when the next vulnerability is discovered in its operating system.

Debian Linux uses a facility called `update-rc.d` to manage init scripts.

This process "`update-rc.d`'s" all of the init scripts off so that the 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 `update-rc.d <daemon> defaults`.

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.

Note: Not all of the scripts listed above will exist on all systems, as this is a superset of the available init scripts that may be running on your system. The benchmark's recommended action will register some trivial errors - these are not cause for alarm.

4.6 Only Enable SMB (Windows File Sharing) Process If Absolutely Necessary

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.

Action:

```
update-rc.d nmbd defaults
update-rc.d smbd defaults
```

Discussion:
Debian Linux offers 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 some business reason to mount Windows Shares, do not remove the packages: `samba-client` and `samba-common`.

Note: Debian, by default, does not come installed with SMB services

4.7 Only Enable NFS Server Processes If Absolutely Necessary

Question:
Is this machine an NFS file server?
If the answer to this question is yes, proceed with the actions below.

Action: `update-rc.d nfs-user-server defaults`

Discussion:
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. 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" where appropriate. For more information, consult the exports manual page.

Note: Debian, by default, does not come installed with NFS services

4.8 Only Enable NFS Client If Absolutely Necessary

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.

Action:

```
update-rc.d nfs-common defaults
```

Discussion:

Again, unless there is a significant need for this system to acquire data via NFS, administrators should disable NFS-related services. Note that other file transfer schemes (such as rdist via SSH) can often be preferable to NFS for certain applications.

Note: Debian, by default, does not come installed with NFS client packages

4.9 Only Enable NIS Client If Absolutely Necessary

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.

Action:

```
cd /etc/default/
cp nis nis.tmp
awk '/^[[:space:]]*NISCLIENT/ { print "NISCLIENT=true"; next }; { print
}' nis.tmp > nis
update-rc.d nis defaults
```

Discussion:

Unless this site must use NIS, it should really be avoided. While it can be very useful for transparently scaling the number of workstations, it's not well designed for security. Sun Microsystems is now phasing out NIS+ in favor of LDAP for naming services – NIS and NIS+ are now reaching end of life.
Debian utilizes the same init script, `/etc/init.d/nis`, to control both NIS client and NIS server processes. However, which processes are invoked is determine by values articulated in `/etc/default/nis`.

Note: Debian, by default, does not come installed with NIS packages

4.10 Only Enable NIS Server If Absolutely Necessary

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.

Action:

If the server participates as a NIS slave server, execute the following:

```
cd /etc/default/
cp nis nis.tmp
awk '/^[[:space:]]*NISSERVER/ { print "NISSERVER=slave"; next }; {
print }' nis.tmp > nis
```

```
rm nis.tmp
update-rc.d nis defaults
```

If the server participates as a NIS master server, execute the following:

```
cd /etc/default/
cp nis nis.tmp
awk '/^[[:space:]]*NISSERVER/ { print "NISSERVER=master"; next }; {
print }' nis.tmp > nis
rm nis.tmp
update-rc.d nis defaults
```

Discussion:
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.

Note: Debian, by default, does not come installed with NIS packages

4.11 Only Enable RPC Portmap Process If Absolutely Necessary

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 this question is yes, proceed with the actions below.

Action:

```
update-rc.d portmap defaults
```

Discussion:

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.

Note: Debian, by default, does not come installed with portmap.

4.12 Only Enable Printer Daemon Processes If Absolutely Necessary

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.

Action:

```
if [ -e /etc/init.d/cups ]; then
update-rc.d cupsys defaults
sed -e 's/^\#User lp/User lp/' /etc/cups/cupsd.conf \
-e 's/^\#Group lpadmin/Group lpadmin/' \
/etc/cups/cupsd.conf-preCIS >/etc/cups/cupsd.conf
chown lp:lpadmin /etc/cups/cupsd.conf
chmod 600 /etc/cups/cupsd.conf
fi
update-rc.d hpoj defaults
update-rc.d lpd defaults
diff /etc/cups/cupsd.conf-preCIS /etc/cups/cupsd.conf
chmod 0755 /usr/bin/lpr /usr/bin/lprm /usr/bin/lpq
```

Discussion:
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`. The Unix print servers have generally had a poor security record – be sure to keep up-to-date on vendor patches.

Note that this item also sets `cupsd`, when present, to run as a non-root user and group, namely user `lp` and group `lpadmin`.

Note: Debian, by default, does not come installed with printer services

4.13 Only Enable Web Server Process If Absolutely Necessary

Question:
Is there a mission-critical reason why this system must run a Web server? 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 is required, review and apply the CIS Apache benchmark available at http://www.cisecurity.org/bench_apache.html. If this is not a web server, and you are not using piranha, the answer is no.
If the answer to this question is yes, proceed with the actions below.

Action:
If Apache is used, download and apply appropriate recommendations from the CIS Apache Benchmark.

Please read the discussion before executing these commands and select the appropriate command.

```
update-rc.d apache defaults
update-rc.d apache2 defaults
```

Discussion:

Utilize one of the above commands to enable the corresponding version of apache that is installed on your server.

Note: Debian, by default, does not come installed with a web server.

4.14 Only Enable SNMP Process If Absolutely Necessary

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 actions below.

Action:

```
update-rc.d snmpd defaults
```

Discussion:

If SNMP is used to monitor the hosts on this network, experts recommend changing the default community string used to access data via SNMP.

Note: Debian, by default, does not come installed with a SNMP services.

4.15 Only Enable DNS Server Process If Absolutely Necessary

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.

Action:
Download and follow the appropriate configurations from the CIS BIND benchmark, then enable BIND as follows.

```
update-rc.d bind defaults
```

Discussion:

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/bind/named.conf` to limit who can query your 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

Note: Debian, by default, does not come installed with a DNS services.

4.16 Only Enable SQL Server Process If Absolutely Necessary

Question:
Is this machine an SQL (database) server?
If the answer to this question is yes, proceed with the actions below.

Action:
Please read the discussion before executing these commands and select the appropriate command.

```
update-rc.d mysql defaults
update-rc.d postgresql defaults
```

Discussion:

If this machine does not need to run the mainstream database (SQL) servers Postgres or MySQL, it is safe to deactivate them. If you need to enable them, issue the command (above) for the database that you installed.

Note: Debian, by default, does not come installed with a database service.

4.17 Only Enable Webmin Processes If Absolutely Necessary

Question:
Does the site absolutely need to administer the system through the remote webmin tool? Proceed with the actions below.

Action - Yes, webmin is necessary:
```
update-rc.d webmin defaults
```

Action - No, webmin is not necessary:
```
aptitude remove webmin
```

Discussion:

One can remotely administer a system through the relatively safe SSH remote shell system. Webmin, and other tools like it, can be dangerous as they have a history of poor authentication or session management.

Note: Debian, by default, does not come installed with webmin services.

4.18 Only Enable Squid Services If Absolutely Necessary

Question:
Does this machine use squid to proxy web transactions?
If the answer to this question is yes, proceed with the actions below.

Action:
```
update-rc.d squid defaults
```

Discussion:

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, if your site 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 you are using it for a reverse web proxy, which is a very specific installation, and beyond the scope of this benchmark).

Note: Debian, by default, does not come installed with squid services.

5 Kernel Tuning

5.1 Network Parameter Modifications

Question:
Does this machine connect to a network?
If the answer to this question is yes, proceed with the actions below.

Action:

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 11 lines added by CISecurity Benchmark sec 5.1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_syncookies=1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
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
net.ipv4.icmp_echo_ignore_broadcasts = 1
END_SCRIPT chown root:root /etc/sysctl.conf
```

Discussion:

For an explanation of some of these parameters, see
http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt

5.2 Additional Network Parameter Modifications

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.

Action:

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 3 lines added by CISecurity Benchmark sec 5.2
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
END_SCRIPT
chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf diff
```

```
/etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Discussion:

For an explanation of some of these parameters, see
http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt

6 Logging

The items in this section cover enabling various 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. 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.

6.1 Capture Messages Sent To Syslog AUTHPRIV Facility

Action:

```
if [ `grep -v '^#' /etc/syslog.conf | \
grep -c 'authpriv'` -eq 0 ];
then echo -e "authpriv.*\t\t\t\t/var/log/auth.log" \
>> /etc/syslog.conf
fi
touch /var/log/auth.log
chown root:root /var/log/auth.log
chmod 600 /var/log/auth.log
diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Discussion:

The default installation of Debian Linux already has this enabled. It is included in case it had been previously disabled.

Not all Linux distributions, especially the older ones, capture logging information which is sent to the LOG_AUTHPRIV facilities. This is unfortunate, since a great deal of important security-related information is sent via these channels (e.g., network service startups, commands like usermod and chage, etc). The above action causes this information to be captured in the /var/log/auth.log file (which is only readable by the superuser). This file should be reviewed and archived on a regular basis.

6.2 Turn On Additional Logging For FTP Daemon

Action:

```
if [ -f /etc/wu-ftpd/ftpaccess ]; then
cd /etc/default
echo 'WU_OPTIONS="-l -a -d"' >> wu-ftpd
```

```
chown root:root wu-ftpd
chmod 644 wu-ftpd
cd /etc/
cp inetd.conf inetd.conf.tmp
sed 's/^\(ftp.*\/usr\/sbin\/wu\-ftpd\).*$/\1 -l -a -d/' inetd.conf.tmp>
inetd.conf
rm inetd.conf.tmp
fi
if [ -f /etc/vsftpd.conf ]; then
FILE = "/etc/vsftpd.conf"
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
chmod 0600 $FILE
chown root:root $FILE
diff ${FILE}-preCIS $FILE
fi
```

Discussion:

Some installations might prefer vsftpd over WU-FTPd, and the above script reflects that preference.

The modifications above ensure that all commands sent to the server are logged. In WUFTPd, the action above also requires the server to log all security violations or policy boundary conditions and to ensure that file transfers are logged to syslog, in addition to the default `/var/log/xferlog`.

6.3 Confirm Permissions On System Log Files

Action:

```
cd /var/log
chmod o-rwx boot.log* cron* dmesg ksyms* httpd/* \
maillog* messages* news/* pgsql rpmpkgs* samba/* sa/* \
scrollkeeper.log secure* spooler* squid/* vbox/* wtmp
chmod o-rx boot.log* cron* maillog* messages* pgsql \
secure* spooler* squid/* sa/*
chmod g-w boot.log* cron* dmesg httpd/* ksyms* \
maillog* messages* pgsql rpmpkgs* samba/* sa/* \
scrollkeeper.log secure* spooler*
chmod g-rx boot.log* cron* maillog* messages* pgsql \
secure* spooler*
chmod o-w gdm/ httpd/ news/ samba/ squid/ sa/ vbox/
chmod o-rx httpd/ samba/ squid/ sa/
chmod g-w gdm/ httpd/ news/ samba/ squid/ sa/ vbox/
chmod g-rx httpd/ samba/ sa/
chmod u-x kernel syslog loginlog
```

```
chown -R root:root .
chgrp utmp wtmp
[ -e news ] && chown -R news:news news
[ -e pgsql ] && chown postgres:postgres pgsql
chown -R squid:squid squid
```

Discussion:

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 you should add any of the services that affect the above logs, please revisit this section to ensure the logs have the correct/secure permissions.

Note: You may get some errors from `chmod` if the file does not exit.

6.4 Configure syslogd to Send Logs to a Remote LogHost

Note: Bastille configuration set to 'No' as this is system/site specific

Action:

In the script below, replace `loghost` with the proper name (FQDN, if necessary) of your loghost.

```
printf "### Following lines added by CISecurity \
Debian Benchmark Section 6.4\n\
kern.warning;*.err;authpriv.none\t@loghost\n\
*.info;mail.none;authpriv.none;cron.none\t@loghost\n\
*.emerg\t@loghost\n\
local7.*\t@loghost\n" >> /etc/syslog.conf
diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Discussion:

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.

7 File/Directory Permissions/Access

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

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($3 ~ /^ext[23]$/ && $2 != "/") \
{ $4 = $4 ",nodev" }; \
{ print }' /etc/fstab.tmp > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
rm -f /etc/fstab.tmp
diff /etc/fstab-preCIS /etc/fstab
```

Discussion:

Placing "nodev" on these partitions prevents users from mounting unauthorized devices on any partitions that we know should not contain devices. There should be little need to mount devices on any partitions other than `/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 you are using chroot jails on your machines, you should be careful with the nodev option.

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

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($2 ~ /^\/m.*\/(floppy|cdrom)$/) && \
($4 !~ /,nodev,nosuid/) \
{ $4 = $4, "nodev,nosuid" }; \
{ print }' /etc/fstab.tmp > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
rm -f /etc/fstab.tmp
diff /etc/fstab-preCIS /etc/fstab
```

Discussion:

Removable media is one vector by which malicious software can be introduced onto the system. By forcing these file systems to be mounted with the nosuid option, the administrator prevents users from bringing set-UID programs onto the system via CDROMs and floppy disks. We also force these file systems to mount with the nodev option, as explained in item 2.1.7.1.

If this machine has multiple CD-ROM or floppy drives, additional action must be taken. Simply add `nosuid` to the fourth field for the `/etc/fstab` lines that reference those drives.

7.3 Disable User-Mounted Removable File Systems

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.

Action:

```
cd /etc
cp fstab fstab.tmp
awk '/media/ { sub(/(users|user)/, "", $4); \
sub(/^,|,$/,"",$4); sub(/,,/,",",$4); \
printf("%s\t%s\t%s\t%s\t%s\t%s\n", $1, $2, $3, $4, $5, $6); next} \
{ print }' fstab.tmp > fstab
rm fstab.tmp
```

Discussion:

By default, Debian allows unprivileged users to mount cdrom and floppy devices. 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. This item removes the `user` and `users` options from these devices. Therefor only allowing `root` to mount these devices.

Note: By default, Debian mounts removable media beneath `/media`. The above script only modifies entries within the `fstab` that are mounted to this location. As such, administrators should review the fstab to ensure all removeable media devices lack the `user` or `users` option.

7.4 Verify passwd, shadow, and group File Permissions

Action:

```
cd /etc
chown root:root passwd shadow group
```

```
chmod 644 passwd group
chmod 400 shadow
```

Discussion:

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 644. Tripwire (http://www.tripwire.org/downloads/index.php) and AIDE (http://sourceforge.net/projects/aide) are excellent products for alerting you to changes in these files.

7.5 World-Writable Directories Should Have Their Sticky Bit Set

Action:

```
for PART in `awk '($3 == "ext2" || $3 == "ext3") \
{ print $2 }' /etc/fstab`; do
find $PART -xdev -type d \
\( -perm -0002 -a ! -perm -1000 \) -print
done
```

Discussion:

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.

7.6 Find Unauthorized World-Writable Files

Action:

```
for PART in $(grep -v '^#' /etc/fstab |
awk '($6 != "0") { print $2 }' ); do
find $PART -xdev -type f \
\( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned.

Discussion:

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.

7.7 Find Unauthorized SUID/SGID System Executables

Action:

```
for PART in $(grep -v '^#' /etc/fstab | awk '($6 != "0") {
print $2 }' ); do
find $PART -xdev \( -perm -04000 -o -perm -02000 \) \
-type f -print
done
```

Discussion:

The administrator should take care to ensure that no rogue set-UID programs have been introduced into the system. In addition, if possible, the administrator should attempt a Set-UID audit and reduction.

7.8 Find All Unowned Files

Action:

```
for PART in $(grep -v '^#' /etc/fstab | awk '($6 != "0") {
print $2 }'); do
find $PART -xdev -nouser -o -nogroup -print
done
```

Discussion:

Do not allow any unowned files on your system. Unowned files may be an indication an intruder has accessed your system or improper package maintenance/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. Another common cause is the installation of software that does not properly set file ownerships.

Files in any NFS mounts may be ignored as the user ID mapping between systems may be out of sync. If your enterprise uses a central user management system (NIS or LDAP), the presence of unowned files may indicate another problem and should be investigated.

7.9 Disable USB Devices

Question:

Is there a mission-critical reason to allow use of PCMCIA or USB-based devices on this system?

If the answer to this question is no, then perform the action below.

Action:

```
K=$(uname -a | awk '{print $3}')
aptitude remove pcmcia-cs
aptitude remove kernel-pcmcia-modules-$K
aptitude remove pcmcia-modules-$K
aptitude remove hotplug
```

Discussion:

PCMCIA cards, USB drives and memory devices represent another attack vector against your systems. The prices for a 512MB or even 1GB USB memory device have become very affordable, and is enough storage to transport vast quantities of data off a system. Few servers have any need for PCMCIA or 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 you are setting up. See the discussion regarding floppy and CD-ROM drives in section 7.2.

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

8 System Access, Authentication, and Authorization

8.1 Remove .rhosts Support In PAM Configuration Files

Action:

```
for FILE in /etc/pam.d/*; do
grep -v rhosts_auth $FILE > ${FILE}.tmp
mv -f ${FILE}.tmp $FILE
chown root:root $FILE
chmod 644 $FILE done
```

Discussion:

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.

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 600).

8.2 Create ftpusers file

Action:

```
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 600 /etc/ftpusers
[ -e /etc/ftpusers-preCIS ] && \
diff /etc/ftpusers-preCIS /etc/ftpusers

VSFTP_CONF="/etc/vsftpd.conf"
ALT_CONF="/etc/vsftpd.conf"
test -f $ALT_CONF && VSFTP_CONF=$ALT_CONF
if [ -e $VSFTP_CONF ] &&
! grep -q "^userlist_deny=NO" $VSFTP_CONF; then
cp -fp /etc/ftpusers /etc/vsftpd.ftpusers
[ -e /etc/vsftpd.ftpusers-preCIS ] &&
diff /etc/vsftpd.ftpusers-preCIS /etc/vsftpd.ftpusers
fi
```

Discussion:

`/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 above 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 your configuration after these changes to be sure that only the expected users are allowed to login via ftp.

8.3 Prevent X Server From Listening On Port 6000/tcp

Action:

```
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 444 Xservers
diff Xservers-preCIS Xservers
fi

if [ -e /etc/X11/gdm/gdm.conf ]; then
cd /etc/X11/gdm
awk -F= '($2 ~ /\/X$/) \
{ printf("%s -nolisten tcp\n", $0); next };
{ print }' gdm.conf-preCIS > gdm.conf
```

```
diff gdm.conf-preCIS gdm.conf
chown root:root gdm.conf
chmod 644 gdm.conf
fi

if [ -d /etc/X11/xinit ]; then
cd /etc/X11/xinit
if [ -e xserverrc ]; then awk '/X/ && !/^#/ \
{ print $0 " :0 -nolisten tcp \$@"; next }; \
{ print }' xserverrc-preCIS > xserverrc
else
cat <<END & xserverrc
#!/bin/bash exec X :0 -nolisten tcp \$@ END
fi
chown root:root xserverrc
chmod 755 xserverrc
[ -e xserverrc-preCIS ] && \
diff xserverrc-preCIS xserverrc
fi
```

Discussion:

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.

8.4 Restrict at/cron To Authorized Users

Action:

```
cd /etc/
rm -f cron.deny at.deny
echo root > cron.allow
[ -e cron.allow-preCIS ] && \
diff cron.allow-preCIS cron.allow
echo root > at.allow
[ -e at.allow-preCIS ] && \
diff at.allow-preCIS at.allow
chown root:root cron.allow at.allow
chmod 400 cron.allow at.allow
```

Discussion:

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 system administrator needs the ability to schedule jobs. Note that 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`.

8.5 Restrict Permissions on crontab files

Action:

```
chown root:root /etc/crontab
chmod 400 /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
```

Discussion:

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.

8.6 Configure xinetd Access Control

Action:

Insert the following line into the "defaults" block in `/etc/xinetd.conf`:

```
only_from = <net>/<num_bits> <net>/<num_bits>
```

where each <net>/<num_bits> combination represents one network block in use by your organization. For example:

```
only_from = 192.168.1.0/24
```

would restrict connections to only the 192.168.1.0/24 network, with the netmask 255.255.255.0.

Note: There are two <TAB>'s between the only_from and the = in the above lines.

Discussion:

This item configures `xinetd` to use simple IP-based access control and log connections. Just as `xinetd`'s access control mechanisms are used to monitor illicit connection attempts, the popular PortSentry tool (http://www.psionic.com/products/portsentry.html) can be used to monitor access attempts on unused ports. Note that running PortSentry may result in the CIS testing tools reporting "false positives" for "active" ports that are actually being held by the PortSentry daemon. Consider replacing the PortSentry daemon with PSAD, short for Port Scan Attack Detector, available from http://www.cipherdyne.com/psad/. Unlike PortSentry, PSAD doesn't have to hold open ports -- instead, it communicates directly with the kernel.

8.7 Restrict Root Logins To System Console

Action:

```
rm -f /etc/securetty
echo console >> /etc/securetty
for i in `seq 1 11`; do
echo vc/$i >> /etc/securetty
done
for i in `seq 1 6`; do
echo tty$i >> /etc/securetty
done
chown root:root /etc/securetty
chmod 400 /etc/securetty
diff /etc/securetty-preCIS /etc/securetty
```

Discussion:

Anonymous root logins should never be allowed, except on the system console in emergency situations. At all other times, the 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 at least some audit trail in the event of problems.

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 protected as well. If this applies to your organization, you may execute these lines:

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

Be advised that doing so will reduce your CIS Scoring Tool score and reduce your security posture.

8.8 Set LILO/GRUB Password

Note: Bastille configuration set to 'No'

Action (if you have an /etc/lilo.conf file):

Add the following lines to the beginning of /etc/lilo.conf

```
restricted
password=<password>
```

Action (if you have an /boot/grub/menu.lst file):

Begin by executing `grub-md5-crypt` to generate the value provided to the `password` parameter within menu.lst.

Copy the value provded by `grub-md5-crypt` and place the following before the first uncommented line within menu.lst

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

Discussion:

By default on most Linux systems, the boot loader prompt allows an attacker to subvert the normal boot process very easily. The action above will allow the system to boot normally, only requiring a password when the user attempts to modify the boot process by passing commands to LILO or GRUB. Make sure to replace <password> in the actions above with a good password.

8.9 Require Authentication For Single-User Mode

Action:

```
cd /etc
if [ "`grep -l sulogin inittab`" = "" ]; then
awk '{ print }; /^id:[0123456sS]:initdefault:/ \
{ print "~~:S:wait:/sbin/sulogin" }' \ inittab > inittab.tmp
mv -f inittab.tmp inittab
chown root:root inittab
chmod 644 inittab
fi
diff inittab-preCIS inittab
```

Discussion:

By default on Debian Linux, you can enter single user mode simply by typing "linux single" at the LILO prompt or in 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 simply 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.

Note: Even though this topic is addressed by Bastille, it performs a step not executed by Bastille and should be completed even if Bastille was used.

8.10 Restrict NFS Client Requests To Privileged Ports

Action:

Add the secure option to all entries in the /etc/exports file. The following Perl code will perform this action automatically.

```
if [ -s /etc/exports ]; then
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
diff /etc/exports-preCIS /etc/exports
```

Discussion:

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). This should not hinder normal NFS operations but may block some automated NFS attacks that are run by unprivileged users.

8.11 Only Enable Syslog To Accept Messages If Absolutely Necessary

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.

Read syslog manpage for the `-l`, `-r` and `-s` options.
Edit `/etc/init.d/sysklogd` and look for the line that says:

```
SYSLOGD=""
```

and add the entries that are appropriate for your site. An example entry would look like this:

```
SYSLOGD="-m 0 -l loghost -r -s mydomain.com"
```

Discussion:

By default the system logging daemon, syslogd, does not listen for log messages from other systems on network port 514/udp (Solaris, by contrast, does listen by default).

It is considered good 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.

9 User Accounts and Environment

Note that 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 System Accounts

Action:

```
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
diff passwd-preCIS passwd
diff shadow-preCIS shadow
```

Discussion:

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.

9.2 Verify That There Are No Accounts With Empty Password Fields

Action:

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

The above command should return no values

Discussion:

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 you if you try to unlock an account with an empty password.

9.3 Set Account Expiration Parameters On Active Accounts

Action:

```
cd /etc
awk '($1 ~ /^PASS_MAX_DAYS/) { $2="90" }
($1 ~ /^PASS_MIN_DAYS/) { $2="7" }
($1 ~ /^PASS_WARN_AGE/) { $2="28" }
($1 ~ /^PASS_MIN_LEN/) { $2="8" }
{ print } ' login.defs-preCIS > login.defs
chown root:root login.defs
chmod 640 login.defs
diff login.defs-preCIS login.defs

useradd -D -f 7
diff /etc/default/useradd-preCIS /etc/default/useradd
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 28 -I 7 $NAME
fi
done
diff shadow-preCIS shadow
```

The above command should return no values

Discussion:

It is a good idea to force users to change passwords on a regular basis. The commands above 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 28 days (-W 28) before their password expires. Once the password expired, the account will be locked out after 7 days (-I 7). Finally, the instructions above set a minimum password length of 8 characters.
These are recommended starting values. Some regulated industries require more restrictive values – ensure they comply with your enterprise security policy.

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

Action:
The command:

```
grep ^+: /etc/passwd /etc/shadow /etc/group
```

The above command should return no values

Discussion:

'+' 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 for attackers to gain privileged access on the system, and should be deleted if they exist.

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

Action:
To find '.' in $PATH:

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

To find group- or world-writable directories in $PATH:

```
find `echo $PATH | tr ':' ' '` -type d \
\( -perm -002 -o -perm -020 \) -ls
```

The above command should return no values

Discussion:

'Including the current working directory ('.') or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan program.

9.6 User Home Directories Should Be Mode 750 or More Restrictive

Action:

```
for DIR in \
`awk -F: '($3 >= 500) { print $6 }' /etc/passwd`; do
chmod g-w $DIR chmod o-rwx $DIR
done
```

Discussion:

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 above 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 document for the web server.

9.7 No User Dot-Files Should Be World-Writable

Action:

```
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
```

Discussion:

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 above modifications are relatively benign, making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users.

9.8 Remove User .netrc Files

Action:

```
find / -name .netrc
```

Stop!!! Read the discussion before proceeding.

```
for DIR in `cut -f6 -d: /etc/passwd`; do
if [ -e $DIR/.netrc ]; then
echo "Removing $DIR/.netrc"
rm -f $DIR/.netrc
fi
done
```

Discussion:

`.netrc` files may contain unencrypted passwords which may be used to attack other systems. While the above modifications are relatively benign, making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. If the first command returns any results, carefully evaluate the ramifications of removing those files before executing the remaining commands as you may end up impacting an application that has not had time to revise its architecture to a more secure design.

9.9 Set Default umask For Users

Action:

```
cd /etc
for FILE in profile csh.login csh.cshrc bash.bashrc; do
if ! egrep -q 'umask.*77' $FILE ; then
echo "umask 077" >> $FILE
fi
chown root:root $FILE
chmod 444 $FILE
diff ${FILE}-preCIS $FILE
done
cd /root
for FILE in .profile .bash_profile .bashrc .cshrc .tcshrc; do
if ! egrep -q 'umask.*77' $FILE ; then
echo "umask 077" >> $FILE # See description
fi
chown root:root $FILE
diff ${FILE}-preCIS $FILE done
```

Discussion:

With a default umask setting of 077 – a setting agreed to as part of the consensus process with DISA and NSA – files and directories created by users will not be readable by any other 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.

We 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.

Note: This is been shown to cause problems with the installation of software packages where the installation script uses the default umask – the directories are owned by root with 700 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. Typically 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 sftplogging patch http://sftplogging.sourceforge.net/

9.10 Disable Core Dumps

Question:

Do you have developers who 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.

Action:

```
cd /etc/security
cat <<END_ENTRIES >> limits.conf
# Following 2 lines added by CISecurity Benchmark sec 8.11
* soft core 0
* hard core 0
END_ENTRIES
diff limits.conf-preCIS limits.conf
```

Discussion:

Core dumps can consume large amounts 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.

9.11 Limit Access To The Root Account From su

Question:

Do you have developers who 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.

Action:
WARNING: If you do not have immediate physical access to the server, ensure you have a user in the wheel group before running the below script. Failure to do so will prevent you from using `su` to become 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-preCIS/su > su
diff /etc/pam.d-preCIS/su su
```

Discussion:

The `su` command allows you to become other users on the system. This is commonly used to become “root” and execute commands as the super-user. If you do not want certain users to `su` to root then uncomment the following line in `/etc/pam.d/su`:

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

Uncommenting this line allows only the users in the wheel group to become root by using the su command and entering the root password. All other users will receive a message stating the password is incorrect.

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.

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 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 this information). Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. 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

Action:

1. Edit the banner currently in /etc/issue – this was created by Bastille and may need to be changed for your enterprise. Leave the words “its owner” as this will be replaced in the next step with the name of your organization.

2. Create banners for console access:

Important: You need to change “The Company” in the text below to an appropriate value for your organization

```
unalias cp mv
cd /etc # Remove OS indicators from banners
for FILE in issue motd; do
cp -f ${FILE} ${FILE}.tmp
egrep -vi "debian" ${FILE}.tmp > ${FILE}
rm -f ${FILE}.tmp done
# Change name of owner
# Remember to enter name of your company here:
COMPANYNAME="The Company"
cp -f issue issue.tmp
sed -e "s/its owner/${COMPANYNAME}/g" issue.tmp > issue
rm -f issue.tmp
diff issue-preCIS issue
```

Discussion:

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.

10.2 Create Warnings For GUI-Based Logins

Action:

```
if [ -e /etc/X11/xdm/Xresources ]; then
cd /etc/X11/xdm
awk '/xlogin\*greeting:/ \
{ print "xlogin\*greeting: Authorized uses only!"; next };
{ print }' Xresources-preCIS > Xresources
chown root:root Xresources
chmod 644 Xresources
diff Xresources-preCIS Xresources fi
if [ -e /etc/X11/xdm/kdmrc ]; then
cd /etc/X11/xdm
awk '/GreetString=/ \ { print "GreetString=Authorized uses only!"; next
};
{ print }' kdmrc-preCIS > kdmrc
chown root:root kdmrc
chmod 644 kdmrc
diff kdmrc-preCIS kdmrc
fi
if [ -e /etc/X11/gdm/gdm.conf ]; then
cd /etc/X11/gdm
cp -pf gdm.conf gdm.conf.tmp
awk '/^Greeter=/ && /gdmgreeter/ \
{ printf("#%s\n", $0); next }; /^#Greeter=/ && /gdmlogin/ \
{ $1 = "Greeter=gdmlogin" }; /Welcome=/ \
{ print "Welcome=Authorized uses only!"; next };
{ print }' gdm.conf.tmp > gdm.conf
rm -f gdm.conf.tmp
chown root:root gdm.conf
chmod 644 gdm.conf
diff gdm.conf-preCIS gdm.conf
fi
```

Discussion:

The commands above set the warning message on xdm, kdm and gdm – in case something other than the default X login GUI was installed.

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

Action:

```
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
diff vsftpd.conf-preCIS vsftpd.conf
fi
if [ -e proftpd.conf ]; then
echo -e "DisplayConnect\t\t/etc/issue.net" >> proftpd.conf
echo -e "DisplayLogin\t\t/etc/motd" >> proftpd.conf
diff proftpd.conf-preCIS proftpd.conf
fi
```

Discussion:

Whenever you make substantial changes to a system, reboot. Some System Administrators believe any change to the init scripts warrant a reboot to ensure the system 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 was an init problem that would have been detected had the reboot taken place.

10.4 Reboot

Action:

```
init 6
```

Reboot:

Whenever you make substantial changes to a system, reboot. Some System Administrators believe any change to the init scripts warrant a reboot to ensure the system 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 was an init problem that would have been detected had the reboot taken place.

11 Anti-Virus Consideration

Anti-Virus Products

Certain systems – such as mail servers and file servers – should have anti0virus software installed to protect the Windows clients that use the server. The following table summarizes the popular anti-virus offerings for the Linux platform. The Center for Internet security makes no endorsement for any product.

Vendor	Product
Sophos http://www.sophos.com/	Commercial
NAI Virus Scan	Commercial
ClamAV http://www.clamav.net/	Open Source
McAfee http://www.mcafee.com/	Commercial
CyberSoft Vfind http://www.cyber.com/products/masterprice.html	
H+B edv (hbedv)	
f-prot Antivirus http://www.f-prot.com/products/corporate_users/unix/	Commercial
Trend Micro	Commercial
Computer Associates InoculateIT http://www.cai.com/	Commercial

12 Remove Backup Files

Action:
Warning: Read discussion before performing this action.

```
find / -xdev | grep preCIS | xargs rm -rf
```

Discussion:

When you are certain your changes are successful, remove the backup files as they will have insecure contents and/or permissions/ownerships. By leaving these files on your system, an attacker can use the backup files as if they were the originals thereby defeating much of your efforts.

13 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.

13.1 Create Symlinks For Dangerous Files

Action:

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

Discussion:

The `/root/.rhosts`, `/root/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control (see the discussion of .rhosts files above). 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).

13.2 Change Default Greeting String For sendmail

Action:

```
cd /etc/mail
awk '/O SmtpGreetingMessage=/ \
{ print "O SmtpGreetingMessage=mailer ready"; next}
{ print }' sendmail.cf > sendmail.cf.new
mv -f sendmail.cf.new sendmail.cf
chown root:bin sendmail.cf
chmod 444 sendmail.cf
/usr/sbin/sendmailconfig
```

Discussion:

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.

13.3 Enable TCP SYN Cookie Protection

Action:

```
echo "echo 1 > /proc/sys/net/ipv4/tcp_syncookies" \
>> /etc/rc.local
```

Discussion:
A "SYN Attack" is a denial of service (DoS) attack that consumes resources on your system forcing you to 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 your system with several (hundreds or thousands) of half-open connections. This is a fairly simple attack and should be blocked.

13.4 Additional LILO/GRUB Security

Action:

```
chattr +i /etc/lilo.conf
chattr +i /boot/grub/menu.lst
```

Discussion:
Setting the immutable flag on the LILO and GRUB config files will prevent any changes (accidental or otherwise) to the lilo.conf or menu.lst files. If you wish to modify either file you will need to unset the immutable flag using the chattr command with -i instead of +i.

13.5 Evaluate Packages Associated With Startup Scripts

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

Action:

```
cd /etc/init.d
ls
```

Discussion:
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 `dpkg --search /etc/init.d/<scriptname>` to determine the package it belongs to, use `aptitude show <packagename>` to read about it, then use `aptitude remove <packagename>` to remove it.

13.6 Evaluate Every Installed Package

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

Action:
See Discussion

Discussion:
Computer Security Industry Best Practices recommend removing unused services and software to minimize attack vectors on a system. The following references suggest 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 and running `aptitude` in GUI mode,selecting `Installed Packages`, and pressing "-" on each package that is determined unneeded.

13.7 Install and Configure sudo

Action:
Install `sudo` via your enterprise process, if applicable. Otherwise, run `aptitude install sudo`.

Discussion:
sudo is a package that allows the System Administrator 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 you have 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 using 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. Experience has shown that if `/etc/sudoers` gets botched (from using vi without visudo's error checking feature), recovery may become very difficult.

13.8 Lockout Accounts After 3 Failures

Action:

```
printf \
"auth required \
/lib/security/pam_tally.so onerr=fail no_magic_root\n\
account required \
/lib/security/pam_tally.so deny=3 no_magic_root reset" \
>> /etc/pam.d/common-auth
```

Discussion:

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 above 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 – you are free to increase it if desired.

Note: The above command assumes account lockouts are not already implemented on the system. If they are already implemented, you will have to edit `/etc/pam.d/common-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

13.9 Additional Kernel Tunings

Action:

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 2 lines added by CISecurity Benchmark sec SN.9
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
```

Discussion:

Before implementing these changes, please review them with your environment in mind. The above 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 martians may generate an excessive amount of logs, especially on multi-homed servers with at least one network interface on a hostile network (i.e, your border firewalls). You should ensure you have plenty of log space available as well as sending your logs to a remote logging host.

13.10 Remove All Compilers and Assemblers

Note: Bastille configuration set to remove c compiler only.
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.

Action:
See Discussion

Discussion:
The following command will help identify such packages:

```
dpkg -l | egrep "cpp|dev|java|asm|gcc|bin86|dev86"
```

13.11 Verify That No Unauthorized UID 0 Accounts Exists

Action:

```
getent passwd | awk -F: '$3 == "0" { print $1 }'
```

Discussion:
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.

14 Appendix B: File Backup Script

```
#!/bin/bash
# Create /root/do-restore.sh
cat <<EOF > /root/do-restore.sh
#!/bin/bash
# This script restores the files changed by the CISecurity
# Linux Benchmark do-backup.sh script.
unalias rm mv cp
sed -n "31,9999p" /root/do-restore.sh | while read LINE; do
FILE=\`echo \$LINE | awk '{print \$1}'\`
PERMS=\`echo \$LINE | awk '{print \$2}'\`
echo "Restoring \$FILE with \$PERMS permissions"
[ -f \${FILE}-preCIS ] && /bin/cp -p \${FILE}-preCIS \${FILE}
/bin/chmod \${PERMS} \${FILE}
[ -f \${FILE}-preCIS ] && /bin/rm \${FILE}-preCIS
done

echo "Completed file restoration - restoring directories"
for DIR in \
/etc/xinetd.d /etc/rc.d \
/var/spool/cron /etc/cron.* \
/etc/pam.d /etc/skel
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."
exit 0
### END OF SCRIPT. DYNAMIC DATA FOLLOWS. ###
EOF
/bin/chmod 700 /root/do-restore.sh
echo "Backing up individual files"
for FILE in \
/etc/ssh/sshd_config /etc/ssh/ssh_config /etc/default/sysstat\
/etc/inetd.conf /etc/hosts.deny /etc/hosts.allow\
/etc/mail/sendmail.conf /etc/inittab\
/etc/bind/named.conf /etc/sysctl.conf /etc/syslog.conf \
/etc/wu-ftpd/ftpaccess /etc/vsftpd.conf /etc/fstab \
/etc/vsftpd.ftpusers /etc/X11/xdm/Xservers\
/etc/X11/gdm/gdm.conf /etc/X11/xinit/xserverrc\
/etc/cron.allow /etc/at.allow /etc/cron.deny\
/etc/at.deny /etc/crontab \
/etc/securetty /etc/inittab /etc/exports \
/etc/shadow /etc/passwd /etc/login.defs\
/etc/default/useradd /etc/profile /etc/csh.login\
/etc/csh.cshrc /etc/bash.bashrc /etc/security/limits.conf\
/etc/issue /etc/motd /etc/X11/xdm/kdmrc\
/etc/X11/xdm/Xresources \
/etc/proftpd.conf /etc/ftpusers \
/boot/grub/menu.lst /etc/issue.net\
/root/.tcshrc /etc/security/limits.conf \
/root/.bash_profile /root/.bashrc /root/.cshrc; do
if [ -f ${FILE} ]; then
# Backup file
/bin/cp -p ${FILE} ${FILE}-preCIS
# Add it to the do-restore script
echo ${FILE} `find ${FILE} -printf "%m"` >> /root/do-restore.sh
fi
done
echo "Completed file backups - backing up directories"
for DIR in \
/etc/init.d \
/var/spool/cron /etc/cron.* \
/etc/pam.d /etc/skel
do
echo ${DIR}
[ -d ${DIR} ] && /bin/cp -pr ${DIR} ${DIR}-preCIS
done
echo "Recording log permissions"
find /var/log -printf "%h/%f %m\n" >> /root/do-restore.sh
echo "Backup complete."
```

15 Appendix C: Bastille Configuration

Here is the recommended Bastille configuration.

Note: Bastille has the ability to set the GRUB/LILO boot passwords but it is not used here to ensure the password is unique to the enterprise implementing this benchmark. Setting this password is covered in section X.X of the Benchmark.

Points to note where the CISecurity Benchmark differ from Bastille'e defaults:

Q: What umask would you like to set for users on the system? **027**

Q: Would you like to disable indexes? **Yes**

Q: Would you like to disable the gcc and/or g++ compiler? **Yes**

Q: May we activate LauS? **No** (Note: There is no default answer for this question)

Q: Would you like to deactivate the HP OfficeJet (hpoj) script on this machine? **Yes** (Note: There is no default answer for this question)

Q: Would you like to deactivate the ISDN script on this machine? **Yes** (Note: There is no default answer for this question)

Q: Would you like to deactivate kudzu's run at boot? **Yes** (Note: There is no default answer for this question)

Q: Would you like to run sendmail via cron to process the queue? **Yes**

Note that use of host-based firewalls may interfere with existing enterprise practices and the Level 1 benchmark makes no recommendation for enabling or disabling the host-based packet filter.

CIS Bastille Configuration File

Note that this configuration file is also provided in the archive containing the PDF version of this document and the CIS scoring tool.

file: bastille.CIS.conf

```
# Q: Would you like to restrict the use of cron to administrative accounts? [Y]
AccountSecurity.cronuser="Y"
# Q: Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"
# Q: Should Bastille disable clear-text r-protocols that use IP-based authentication? [Y]
AccountSecurity.protectrhost="Y"
# Q: Should Bastille ask you for extraneous accounts to delete?
AccountSecurity.removeaccounts="Y"
# Q: Which extraneous accounts should Bastille delete (space-separated) ?
AccountSecurity.removeaccounts_list="games gopher"
# Q: Should Bastille ask you for extraneous groups to delete?
AccountSecurity.removegroups="N"
# Q: Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="N"
# Q: What umask would you like to set for users on the system? [077]
AccountSecurity.umask="027"
```

```
# Q: Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"
# Q: Would you like to disable indexes? [N]
Apache.apacheindex="Y"
# Q: Would you like to deactivate the Apache web server? [Y]
Apache.apacheoff="Y"
# Q: Would you like to bind the Web server to listen only to the localhost? [N]
Apache.bindapachelocal="N"
# Q: Would you like to bind the web server to a particular interface? [N]
Apache.bindapachenic="N"
# Q: Would you like to disable CGI scripts, at least for now? [Y]
Apache.cgi="Y"
# Q: Would you like to deactivate server-side includes? [Y]
Apache.ssi="Y"
# Q: Would you like to deactivate the following of symbolic links? [Y]
Apache.symlink="Y"
# Q: Would you like to reduce the LILO delay time to zero? [N]
BootSecurity.lilodelay="N"
# Q: Do you ever boot Linux from the hard drive? [Y]
BootSecurity.lilosub_drive="Y"
# Q: Would you like to write the LILO changes to a boot floppy? [N]
BootSecurity.lilosub_floppy="N"
# Q: Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
# Q: Would you like to password-protect the GRUB prompt? [N]
BootSecurity.protectgrub="N"
# Q: Would you like to password-protect the LILO prompt? [N]
BootSecurity.protectlilo="N"
# Q: Would you like to disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="N"
# Q: Should we restrict console access to a small group of user accounts? [N]
ConfigureMiscPAM.consolelogin="N"
# Q: Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="N"
# Q: Would you like to chroot named and set it to run as a non-root user? [N]
DNS.chrootbind="N"
# Q: Would you like to deactivate named, at least for now? [Y]
DNS.namedoff="Y"
# Q: Would you like to disable the gcc and/or g++ compiler? [N]
DisableUserTools.compiler="Y"
# Q: Would you like to disable anonymous download? [N]
FTP.anonftp="N"
# Q: Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="N"
# Q: Would you like to set more restrictive permissions on the administration utilities? [N]
```

```
FilePermissions.generalperms_1_1="N"
# Q: Would you like to disable SUID status for XFree86? [N]
FilePermissions.suidXFree86="N"
# Q: Would you like to disable SUID status for Xwrapper? [N]
FilePermissions.suidXwrapper="N"
# Q: Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"
# Q: Would you like to disable SUID status for cardctl? [Y]
FilePermissions.suidcard="Y"
# Q: Would you like to disable SUID status for DOSEMU? [Y]
FilePermissions.suiddos="Y"
# Q: Would you like to disable SUID status for dump and restore? [Y]
FilePermissions.suiddump="Y"
# Q: Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"
# Q: Would you like to disable SUID status for news server tools? [Y]
FilePermissions.suidnews="Y"
# Q: Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="N"
# Q: Would you like to disable SUID status for printing utilities? [N]
FilePermissions.suidprint="N"
# Q: Would you like to disable the r-tools? [Y]
FilePermissions.suidrtool="Y"
# Q: Would you like to disable SUID status for traceroute? [Y]
FilePermissions.suidtrace="Y"
# Q: Would you like to disable SUID status for usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
# Q: Would you like to run the packet filtering script? [N]
Firewall.ip_intro="N"
# Q: May we activate LAuS?
Logging.laus="N"
# Q: Would you like to add additional logging? [Y]
Logging.morelogging="Y"
# Q: Would you like to set up process accounting? [N]
Logging.pacct="N"
# Q: Do you have a remote logging host? [N]
Logging.remotelog="N"
# Q: Would you like to disable acpid and/or apmd? [Y]
MiscellaneousDaemons.apmd="Y"
# Q: Would you like to disable the DHCP daemon? [Y]
MiscellaneousDaemons.dhcpd="Y"
# Q: Would you like to deactivate gated? [Y]
MiscellaneousDaemons.disable_gated="Y"
# Q: Would you like to deactivate the HP OfficeJet (hpoj) script on this machine?
MiscellaneousDaemons.disable_hpoj="Y"
# Q: Would you like to deactivate the ISDN script on this machine?
```

```
MiscellaneousDaemons.disable_isdn="Y"
# Q: Would you like to deactivate kudzu's run at boot?
MiscellaneousDaemons.disable_kudzu="Y"
# Q: Would you like to deactivate routed? [Y]
MiscellaneousDaemons.disable_routed="Y"
# Q: Would you like to disable GPM? [Y]
MiscellaneousDaemons.gpm="Y"
# Q: Would you like to disable the news server daemon? [Y]
MiscellaneousDaemons.innd="Y"
# Q: Would you like to deactivate NIS client programs? [Y]
MiscellaneousDaemons.nis_client="Y"
# Q: Would you like to deactivate NIS server programs? [Y]
MiscellaneousDaemons.nis_server="Y"
# Q: Would you like to disable PCMCIA services? [Y]
MiscellaneousDaemons.pcmcia="Y"
# Q: Would you like to deactivate NFS and Samba? [Y]
MiscellaneousDaemons.remotefs="Y"
# Q: Would you like to disable SNMPD? [Y]
MiscellaneousDaemons.snmpd="Y"
# Q: Would you like to disable printing? [N]
Printing.printing="N"
# Q: Would you like to disable printing? [N]
Printing.printing_cups="N"
# Q: Would you like to disable CUPS' legacy LPD support? [N]
Printing.printing_cups_lpd_legacy="N"
# Q: Would you like to display "Authorized Use" messages at log-in time? [Y]
SecureInetd.banners="Y"
# Q: Should Bastille ensure inetd's FTP service does not run on this system? [y]
SecureInetd.deactivate_ftp="Y"
# Q: Should Bastille ensure the telnet service does not run on this system? [y]
SecureInetd.deactivate_telnet="Y"
# Q: Who is responsible for granting authorization to use this machine?
SecureInetd.owner="its owner"
# Q: Would you like to set a default-deny on TCP Wrappers and xinetd? [N]
SecureInetd.tcpd_default_deny="N"
# Q: Would you like to run sendmail via cron to process the queue? [N]
Sendmail.sendmailcron="Y"
# Q: Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
# Q: Would you like to disable the VRFY and EXPN sendmail commands? [Y]
Sendmail.vrfyexpn="Y"
# Q: Would you like to install TMPDIR/TMP scripts? [N]
TMPDIR.tmpdir="N"
```

16 Change History

Date	Revision	Change
2/26/2007	0.0.1	Fixed typos in sections 3.5, 4.18, 4.5, 5.1, 5.2, 6.4, and 7.9.
2/26/2007	0.0.1	In dobackup.sh, removed references to /etc/xinetd.conf, /etc/xinetd.d, and /etc/rc.d. Added /etc/init.d.
2/26/2007	0.0.1	Replaced 'question' portion in section 5.1 with "Does this machine connect to a network?"
2/26/2007	0.0.1	In section 2.5 added "After Bastille is installed, copy the bastille.CIS.conf file provided in the archive containing the PDF version of this document (and in Appendix C) to /etc/Bastille/config."
3/05/2007	0.0.1	Updated BIOS password rule to reflect preference of requiring a BIOS password for modifying the BIOS but not for boot.
4/05/2007	0.0.1	Normalized password recommendations - eight or more characters in length
4/05/2007	0.0.1	Updated partitioning guidance
4/05/2007	0.0.1	Added XCCDF platform and front matter