



SuSE Linux Enterprise Server Benchmark v1.0

(SuSE Linux Enterprise Server 9.0)

March, 2006

Copyright 2001-2005, The Center for Internet Security

<http://www.CISecurity.org/>

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, .mew, 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

CIS SuSE Linux Benchmark

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

CIS SuSE Linux Benchmark

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

Table of Contents

CIS SuSE Linux Enterprise Server Benchmark.....	9
Applicability	9
Conventions	9
Root Shell Environment Assumed	9
Executing Actions.....	9
Reboot Required.....	9
Vulnerabilities.....	10
Backup Key Files.....	10
Build Considerations	10
Software Package Removal.....	11
Software Package Installation.....	11
Notes About Bastille.....	11
1.1 Apply Latest OS Patches	13
1.2 Validate Your System Before Making Changes	14
1.3 Configure SSH	14
1.4 Enable System Accounting.....	15
1.5 Install and Run Bastille	16
2.1 Disable Standard Services.....	17
2.2 Configure TCP Wrappers and Firewall to Limit Access	18
2.3 Only Enable telnet If Absolutely Necessary	21
2.4 Only Enable FTP If Absolutely Necessary	22
2.5 Only Enable rlogin/rcp If Absolutely Necessary	23
2.6 Only Enable TFTP Server if Absolutely Necessary	23
2.7 Only Enable IMAP If Absolutely Necessary	24
2.8 Only Enable POP If Absolutely Necessary	24
3.1 Set Daemon umask.....	25
3.2 Disable xinetd, If Possible	25
3.3 Disable postfix Server, If Possible	26
3.4 Disable GUI Login If Possible	26
3.5 Disable X Font Server If Possible	27
3.6 Disable Standard Boot Services.....	27
3.7 Only Enable SMB (Windows File Sharing) Processes If Absolutely Necessary	28
3.8 Only Enable NFS Server Processes If Absolutely Necessary	29
3.9 Only Enable NFS Client Processes If Absolutely Necessary	29
3.10 Only Enable NIS Client Processes If Absolutely Necessary	30
3.11 Only Enable NIS Server Processes If Absolutely Necessary	30
3.12 Only Enable RPC Portmap Process If Absolutely Necessary	30
3.13 Only Enable netfs Script If Absolutely Necessary	31
3.14 Only Enable Printer Daemon Processes If Absolutely Necessary	31
3.15 Only Enable Web Server Processes If Absolutely Necessary	32

CIS SuSE Linux Benchmark

3.16 Only Enable SNMP Processes If Absolutely Necessary	32
3.17 Only Enable DNS Server Process If Absolutely Necessary	33
3.18 Only Enable SQL Server Processes If Absolutely Necessary	34
3.19 Only Enable Webmin Processes If Absolutely Necessary	34
3.20 Only Enable Squid Cache Server If Absolutely Necessary	34
3.21 Only Enable Kudzu Hardware Detection If Absolutely Necessary	35
4.1 Network Parameter Modifications.....	35
4.2 Additional Network Parameter Modifications.....	36
5.1 Capture Messages Sent To Syslog AUTHPRIV Facility	37
5.2 Turn On Additional Logging For FTP Daemon.....	38
5.3 Confirm Permissions On System Log Files	38
5.4 Configure syslogd to Send Logs to a Remote LogHost.....	39
6.1 Add 'nodelv' Option To Appropriate Partitions In /etc/fstab	40
6.2 Add 'nosuid' and 'nodelv' Option For Removable Media In /etc/fstab.....	41
6.3 Disable User-Mounted Removable File Systems	41
6.4 Verify passwd, shadow, and group File Permissions	42
6.5 World-Writable Directories Should Have Their Sticky Bit Set.....	43
6.6 Find Unauthorized World-Writable Files.....	43
6.7 Find Unauthorized SUID/SGID System Executables	44
6.8 Find All Unowned Files	44
6.9 Disable USB Devices (AKA Hotplugger).....	45
7.1 Remove .rhosts Support In PAM Configuration Files	45
7.2 Create ftpusers Files	46
7.3 Prevent X Server From Listening On Port 6000/tcp.....	46
7.4 Restrict at/cron To Authorized Users.....	47
7.5 Restrict Permissions On crontab Files	48
7.6 Configure xinetd Access Control.....	48
7.7 Restrict Root Logins To System Console.....	49
7.8 Set LILO/GRUB Password.....	50
7.9 Require Authentication For Single-User Mode.....	51
7.10 Restrict NFS Client Requests To Privileged Ports	51
7.11 Only Enable syslog To Accept Messages If Absolutely Necessary	52
8.1 Block System Accounts	53
8.2 Verify That There Are No Accounts With Empty Password Fields	54
8.3 Set Account Expiration Parameters On Active Accounts.....	54
8.4 Verify No Legacy '+' Entries Exist In passwd, shadow, And group Files	55
8.5 Verify That No UID 0 Accounts Exist Other Than Root	55
8.6 No '.' or Group/World-Writable Directory In Root's \$PATH	56
8.7 User Home Directories Should Be Mode 750 or More Restrictive	56
8.8 No User Dot-Files Should Be World-Writable	57
8.9 Remove User .netrc Files	57
8.10 Set Default umask For Users	58

CIS SuSE Linux Benchmark

8.11 Disable Core Dumps	59
8.13 Limit Access To The Root Account From su.....	59
8.14 Reboot	60
9 Warning Banners	60
9.1 Create Warnings For Network And Physical Access Services	61
9.2 Create Warnings For GUI-Based Logins	62
9.3 Create	63
10 Anti-Virus Consideration.....	64
11 Remove Backup Files.....	64
Appendix A Additional Security Notes.....	65
SN.1 Create Symlinks For Dangerous Files	65
SN.2 Change Default Greeting String For sendmail	65
SN.3 Enable TCP SYN Cookie Protection.....	65
SN.4 Additional LILO Security	66
SN.5 Evaluate Packages Associated With Startup Scripts	66
SN.6 Evaluate Every Installed Package.....	67
SN.7 Install and Configure sudo.....	68
SN.8 Additional Kernel Tunings	68
SN.9 Remove All Compilers and Assemblers.....	69
Appendix B File Backup Script.....	70
Appendix C Bastille Configuration.....	73
Appendix D Change History	78
References	79

CIS SuSE Linux Enterprise Server Benchmark

Applicability

This benchmark was developed and tested on SuSE Linux Enterprise Server (SLES) 9.0. It is likely to work for other versions of SuSE Linux as well (such as SuSE Linux Professional). The scoring tool may yield inaccurate results on non-SuSE systems.

Conventions

The following typographical conventions are used in this document:

Roman font	normal text
<code>Courier</code>	used to indicate either a command or a standard Unix parameter or a file
<i>Italics</i>	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. You may find that many of the "chkconfig" actions, which activate or deactivate services, produce the message "<service name>: unknown service" These messages are quite normal and should not cause alarm – they simply indicate that the program being referenced was not installed on your machine. As SuSE Linux installs allow a great deal of flexibility in what software you choose to install, these messages are unavoidable.

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 un-needed service, you could have a problem if a hole is found.

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. The default partitioning for Suse Linux Enterprise Server is similar to this:

/	1 GB
swap	1xRAM
/var	1 GB
/usr	4 GB
/opt	4 GB
/home	remaining disk space

It is important to keep `/var` and `/home` on their own partitions. Some applications have a tendency to crash when the `/` or `/usr` filesystem reaches 100%. This could happen if users were to store considerable amounts of data (developers storing jar files or copies of application logs, for example) or logs were to fill up their partition. Some Enterprises define a `/logs` partition and store application logs there.

For additional security, an additional and separate partition may be created for `/boot` which creates the kernel binaries and boot loader configuration. A `/boot` partition may be mounted read-only to avoid accidental damage and to make malicious changes a little bit more difficult (e.g. less space for backdoors in malicious kernel patches). A read-only `/boot` partition however will require special procedures for a valid kernel patch (or update).

To limit the inconveniences caused by filling up `/home`, consider implementing user and group quotas on the `/home` filesystem. Quotas will limit how much a single user (or single group) can store on a given filesystem. More information is available in the Suse Linux manuals (see the installation CDs).

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.

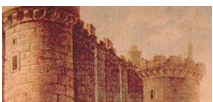
Software Package Installation

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

Notes About Bastille

Throughout this Benchmark, you will see the Bastille castle in the left margin. This indicates a section that is addressed by Bastille. If you installed Bastille and ran it with the configuration file provided, this area will already be taken care of for you.

It is still worth walking through that section to ensure your system is configured properly. In some cases where the logo appears, that section is addressed by Bastille, but it is the script provided does not address it as manual intervention is required. Setting a LILO/GRUB password is an example of this case. Bastille addresses setting the password, however, that must be set per system. In those cases, a note will appear in



CIS SuSE Linux Benchmark

bold italics regarding Bastille.

1 Patches, Packages and Initial Lockdown

1.1 Apply Latest OS Patches

Action:

Update system per your Enterprise Update procedures.

Discussion:

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 Novell publishes an update for SuSE Linux, they include the procedures with it for updating the package. This usually entails downloading the new RPMs from Novell, 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 SuSE Linux, it is generally recommended that any patch be deployed to a non-production system first for testing.

Some RPMs may need to be installed before others. For the most part, RPM understands and solves dependencies. Novell creates separate instructions for special cases, like the replacement of the kernel or the general C library glibc. You may need to examine the list of updates that you have downloaded to check for any of these cases.

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. One approach is to use a stateful hardware firewall to separate and protect the unpatched system from all other systems. For the purpose of update and installation the hardware firewall should be configured to prevent all inbound connections; as well as packets that aren't part of an established session.

Novell offers at least partially automated patch download and installation via YaST Online Update. In lieu of an existing Enterprise Standard, consider using YaST Online Update whenever Novell announces vulnerabilities. If your Enterprise has several servers, consider installing an update server that can be used in place of the update servers at Novell– the updates will go much faster, you will use much less bandwidth from your

ISP, and you will reduce the load on Novell's servers.

If YaST Online Update is used, it should be used on a lab server and the patches validated and the system regression tested before going to live/production systems.

1.2 Validate Your System Before Making Changes

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".

Performing a scan for rootkits is a prudent measure. Some enterprises may also wish to perform further validation on the integrity of the operating system: anti-virus scanning and checking the integrity of system files against a trusted database of file hashes. While this standard does not endorse specific tools, the following are examples of tools used.

Rootkit detection: Chkrootkit, Rootkit Hunter or kstat (for advanced users).

Anti-virus: clamav (freeware) or commercial anti-virus products from Computer Associates, F-Secure, Kaspersky, Sophos, Symantec or Trend Micro.

Trusted hash databases: The NSRL hash database, a database of file hashes from this server, stored on a separate system (e.g. hashes from AIDE, Tripwire, Trusted Computing Base, etc).

Resolve all issues before continuing.

1.3 Configure SSH

Action:

```
unalias cp rm mv
cd /etc/ssh
cp ssh_config ssh_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
    { print }' ssh_config.tmp > ssh_config
if [ "`egrep -l ^Protocol ssh_config`" == "" ]; then
    echo 'Protocol 2' >> ssh_config
fi
rm ssh_config.tmp
diff ssh_config-preCIS ssh_config
```

Look at `/etc/ssh/ssh_config` to and verify "Protocol 2" is under the "Host

*

 entry. If it is not there, edit the file and put "Protocol 2" under the "Host * entry.

```
cp sshd_config sshd_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
/^#? *X11Forwarding/ \
    { print "X11Forwarding yes"; next };
/^#? *IgnoreRhosts/ \
    { print "IgnoreRhosts yes"; 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.

1.4 Enable System Accounting

Action:

Install package `sysstat`.

Discussion:

Note: SLES does not include `sysstat` by default (unless the full installation is chosen).

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/sa/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/sa/` directory on a regular basis to preserve this data for longer periods.

1.5 Install and Run Bastille

Action:

Bastille is included in the SLES installation media. If you did a full installation or chose Bastille specifically, then it will be installed on your system. To check for Bastille and its version, use the following command:

```
rpm -qa | grep -i bastille
```

If it is installed, the response will be similar to the following:

```
bastille-2.1.1-32.9
```

Download and install the latest Bastille RPM from <http://www.bastille-linux.org/#get>. As of this writing, the current version is 3.0.7-1.0 – install it like so:

```
rpm -ivh Bastille-3.0.7-1.0.noarch.rpm
```

Note: Bastille is under constant revision. As of August 11, 2005, the current version of Bastille is 3.0.7-1.0. Download and install the current version listed on the site above.

If you are only performing an Assessment with Bastille then you won't need the perl modules indicated at <http://www.bastille-linux.org/perl-rpm-chart.html>. If you are running Bastille in hardening mode, however, then you will need the perl modules. The chart indicates that you should use the updated version of the perl modules that come with the Suse distribution. Check for the installed modules as follows:

```
rpm -qa | egrep -i "perl-tk|perl-curses"
```

If it is installed, the response will be similar to the following:

```
perl-Tk-800.024-429.1
```

```
perl-Curses-1.06-470.1
```

Before running Bastille, please review Appendix C and understand the changes that it will

make.

After Bastille is installed, copy the `bastille.CIS.conf` file provided in the archive containing this document to `/etc/Bastille/config`. The configuration file is also provided in Appendix C. Run Bastille in batch mode as shown:

```
cd /etc/Bastille
cp /path/to/bastille.CIS.conf config
bastille -b
```

At this point, Bastille commits the changes.

Reboot now: `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.

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.

Reboot now. Then proceed with the Benchmark. Rebooting is required as many services are disabled by Bastille and the remainder of the Benchmark is based on this environment.

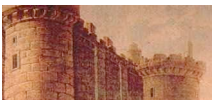
2 Minimize xinetd network services

You will need to unalias the `mv` and `cp` commands as some commands overwrite files and you may be prompted numerous times about overwriting these files:

```
unalias mv cp
```

2.1 Disable Standard Services

Note: *Bastille configuration does not cover all of these services*



Action:

```
cd /etc/xinetd.d
for FILE in atftp chargen chargen-udp cups-lpd cyrus \
daytime daytime-udp echo echo-udp fam finger imap \
pure-ftpd qpopper rexec rlogin rsh rsync rsyncd servers \
services systat talk telnet tftp time time-udp vnc \
vsftpd; do
    chkconfig ${FILE} off
done
```

Discussion:

On Linux, `xinetd` has outpaced `inetd` as the default network superserver. SuSE Linux uses `xinetd`.

After enabling SSH, it is possible to nearly do away with all `xinetd`-based services, since SSH provides both a secure login mechanism and a means of transferring files to and from the system. The actions above will disable all standard services normally enabled in the `xinetd` configuration.

When running the above commands, you may receive one or more errors like this:

```
unknown service
```

This is perfectly acceptable as all it means is the software for that service was not installed.

The rest of the actions in this section give the administrator the option of re-enabling certain services. Rather than disabling and then re-enabling these services, experienced administrators may wish to simply disable only those services that they know are unnecessary for their systems. If there is any doubt, it is better to disable everything, then re-enable the necessary services based on the function of the server.

Note: If you attempt to re-enable a service and get a message like this:

```
unknown service
```

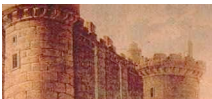
it means that you have not installed the software for that service yet. Install the software package then proceed with the Benchmark.

2.2 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 action below.



Action:

Note: Bastille configuration set to 'No'

Note: Do not deny access to your system without allowing access. Complete both parts of this section.

TCP Wrappers

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.

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

You may wish to further customize your configuration. For example, if you would like to ensure that only one ip address, 192.168.50.4, can access SSH on your server at 192.168.50.2, then follow the example below.

Change `/etc/hosts.allow` from:

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

to:

```
sshd : 192.168.50.4/255.255.255.255 : ALLOW
ALL EXCEPT sshd: localhost, 192.168.50.2/255.255.255.0
```

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

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. There are options during installation that allow you to minimally configure the iptables firewall (to be confirmed and examined in greater detail). There are also sample files.

The default configuration of iptables should not be considered secure without specific configuration. The Center for Internet Security recommends using a tool (graphical- or

CIS SuSE Linux Benchmark

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 a less secure system.

See the following iptables resources:

Web-Based

Easy Firewall Generator for IPTables - <http://easyfwgen.morizot.net/>

Package-Based

FireHOL - <http://firehol.sourceforge.net/>

Firestarter - <http://www.fs-security.com/>

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.

2.3 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:

```
chkconfig telnet on
```

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 SuSE 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.

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

2.4 Only Enable FTP If Absolutely Necessary

Question:

Is this machine an (anonymous) FTP server, or is there a mission-critical reason why data must be transferred to and from this system via an ftp server, rather than sftp or scp?

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

Action:

```
chkconfig vsftpd on
```

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. SSH provides two different encrypted file transfer mechanisms – scp and sftp – and should be used instead. Even if FTP is required because the local system is an anonymous FTP server, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols. For further information on restricting FTP access to the system, see section 7.2 below.

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

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

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

2.5 Only Enable `rlogin/rcp` If Absolutely Necessary

Action:

```
chkconfig rsh on
chkconfig rlogin on
```

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 7.1 for additional security-related configuration settings.

2.6 Only Enable TFTP Server 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?

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

Action:

```
chkconfig tftp on
if [ ! -d "/tftpboot" ] ; then
    mkdir -m 0755 /tftpboot && \
    chown root:root /tftpboot
fi
```

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 SuSE Linux. You will have to install it if you need to use it. After installing it, perform the actions above.

2.7 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:

```
chkconfig cyrus on
```

or

```
chkconfig imap on
```

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 then either `cyrus` or `imap` may be activated. Note: `cyrus` and `imap` both provide IMAP **and** POP services.

2.8 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:

```
chkconfig qpopper on
```

or

```
chkconfig cyrus on
```

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 then either `qpopper` or `cyrus` may be activated.

3 Minimize boot services

3.1 Set Daemon umask

Action:

```
cd /etc
awk '($1=="umask") { if ($2 < "027") { $2="027";} }; \
    { print }' rc.status-preCIS > rc.status
if [ `grep -c umask rc.status` -eq 0 ]; then
    echo "umask 027" >> rc.status
fi
diff rc.status-preCIS rc.status
```

Discussion:

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

3.2 Disable *xinetd*, If Possible

Action:

```
cd /etc/xinetd.d
if [ `find . -type f | \
    xargs awk '($1=="disable" && $3=="no") {print}' \
    | wc -l` -eq 0 ]; then
    chkconfig xinetd off
fi
```

Discussion:

If the actions in Section 2 of this benchmark resulted in no services being enabled in the inet super daemon `/etc/xinetd.d`, then the `xinetd` service may be disabled completely on this system.

Experienced SysAdmins 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.

3.3 Disable *postfix* 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.

Action:

```
if [ -f "/etc/postfix/master.cf" ]; then
    cd /etc/postfix
    awk '$1 ~ /^smtp$/ { print "#" $0; next };
        { print }' master.cf.preCIS > master.cf
    diff master.cf.preCIS master.cf
fi
```

Discussion:

It is possible to run a Unix system with the postfix daemon disabled and still allow users on that system to send email out from that machine. Running postfix in "*daemon mode*" 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 postfix security issues.

Experienced administrators will understand that a *chroot*-jailed user or program can still interact with a postfix process listening on the *loopback* interface.

3.4 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
printf "/etc/inittab\troot.root\t600\n" >> \
/etc/permissions.local
```

Discussion:

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. In SuSE Linux, there are two main runlevels that the system runs in. Runlevel 5 boots directly into X Windows, so as to allow graphical login or easy use of specialized X terminals. Otherwise, for normal text-based console login, runlevel 3 is desirable. 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.

3.5 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:

```
chkconfig xfs off
```

Discussion:

If you won't be using an X server on this machine, this action will deactivate the font server.

3.6 Disable Standard Boot Services

Action:

```
for FILE in apache2 apache apmd autofs fbset gpm hotplug \  
hwscan joystick lpd mars-new named nfs portmap smb snmpd \  
ypbind ypserv yppasswdd; do  
    /etc/init.d/$FILE stop  
    chkconfig $FILE off  
done  
for USERID in lp apache named mysql; do  
    usermod -L -s /bin/false $USERID  
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.

SuSE Linux uses a facility called `chkconfig` to manage all the SysV rc-scripts. `chkconfig` adds or deletes links in each of the appropriate runlevel directories

(`/etc/rc.d/rc*.d`) to activate or deactivate each of the rc-scripts.

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

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

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

The third loop in the "Action" section locks daemon-user accounts related to servers that we examine by setting a lockout password. This will not prevent a given daemon from running as these users – it simply confirms that these users are not available for human login. It also changes the shell to `/bin/false` for an additional layer of security as long as shell access is not necessary. Bear in mind that some packages (`findutils` up to version 4.1.20, for example) do not work properly without a shell for the `nobody` account – be sure you test this thoroughly if you choose to invalidate the daemon shells.

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

3.7 Only Enable SMB (Windows File Sharing) Processes 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:

```
chkconfig smb on
```

Discussion:

SuSE Linux includes the popular Open Source Samba server for providing file and print services to Windows-based systems. This allows a Unix system to act as a file or print server in on a Windows network, and even act as a Domain Controller (authentication server) to older Windows operating systems. However, if this functionality is not required by the site, the service should be disabled.

3.8 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:

```
chkconfig nfs on
```

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.

3.9 Only Enable NFS Client Processes 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:

```
chkconfig autofs on
```

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.

3.10 Only Enable NIS Client Processes 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:

```
chkconfig ypbind on
```

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.

3.11 Only Enable NIS Server Processes 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:

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

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.

3.12 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:

```
chkconfig portmap on
```

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.

3.13 Only Enable ncpfs Script If Absolutely Necessary

Question:

Is this machine sharing files via the NFS, Novell Netware or Windows file sharing protocols?

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

Action:

```
chkconfig ncpfs on
```

Discussion:

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

3.14 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:

```
chkconfig lpd on
```

```
# Following added to undo Bastille change:
```

CIS SuSE Linux Benchmark

```
# SuSE Linux uses cups and symlinks to lpr
# if symlink exists, this is a cups system
if [ -L /usr/bin/lpr ]; then
    chmod 0755 /usr/bin/lpr* /usr/bin/lprm*
    chmod 0755 /usr/bin/lpq* /usr/bin/lpstat*
else
    chmod 0755 /usr/bin/lpr /usr/bin/lprm /usr/bin/lpq
fi
```

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

3.15 Only Enable Web Server Processes If Absolutely Necessary

Question:

Is there a mission-critical reason why this system must run a Web 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.

```
chkconfig apache2 on
```

Discussion:

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

3.16 Only Enable SNMP Processes 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:

```
chkconfig snmpd on
```

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. On SuSE Linux systems, this parameter has already been changed to a reasonably secure setting in the file `/etc/snmpd.conf`.

No further action is required.

Note: In a large Enterprise that relied heavily on SNMP, it was discovered during the Linux rollout that SNMP was not a critical service, and not having it enabled increased the security posture of the servers.

3.17 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:

```
chkconfig named on
```

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 consider tightening the configuration. One highly suggested configuration is to bind the DNS server program in a chroot environment. 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. The BIND name server that most machines run has had major security problems recently.

Additionally, consider using the use of Access Control Lists (ACL's) in `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 internal and external name servers and should consider this precaution.

3.18 Only Enable SQL Server Processes 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.

```
chkconfig postgresql on  
chkconfig mysql on
```

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.

3.19 Only Enable Webmin Processes If Absolutely Necessary

Not Applicable to SuSE, This section is retained for consistency with the other Linux Benchmarks.

3.20 Only Enable Squid Cache Server If Absolutely Necessary

Question:

Do you use the squid web cache to speed up web transactions?

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

Action:

```
chkconfig squid on
```

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 does use Squid, do 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).

3.21 Only Enable hwscan Hardware Detection If Absolutely Necessary

Question:

Does the site absolutely need to allow users at the console to add hardware to the system?

If the answer to this question is yes, then perform the action below.

Action:

```
chkconfig hwscan on
```

Discussion:

Hwscan is SuSE Linux's hardware detection program, which is normally set to run during system startup. It detects changes in hardware and, without demanding authentication of any sort, allows the user at the console to configure that hardware. This lack of authentication presents the primary danger – any user sitting at the console during a reboot can configure any new devices added to the system.

This configuration is an unnecessary risk for most sites, with the exception of those that need to allow users to easily make hardware changes without having a root password. Sites in the exception class might need to allow students to connect external hard drives, backup drives or other potentially common external devices.

If you deactivate this rc-script, hwscan is still accessible. To run hwscan after installing new hardware, run `/etc/init.d/hwscan start` at the shell prompt while logged in as root.

4 Kernel Tuning

4.1 Network Parameter Modifications

Action:

```
cat <<END_SCRIPT >> /etc/sysctl.conf  
# Following 11 lines added by CISecurity Benchmark sec 4.1
```

CIS SuSE Linux Benchmark

```
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
chmod 0600 /etc/sysctl.conf
    printf "/etc/sysctl.conf\troot.root\t600\n" >> \
        /etc/permissions.local
diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Discussion:

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

See also SN.9 for additional security-related tunings that you may want to consider.

4.2 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 4.2
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
```

```
printf "/etc/sysctl.conf\troot.root\t600\n" >> \  
    /etc/permissions.local  
diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Discussion:

For an explanation of some of these parameters, read the latest from the cross-referencing Linux site: <http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt>.

5 Logging

The items in this section cover enabling various different forms of system logging in order to keep track of activity on the system. Because it is often necessary to correlate log information from many different systems (particularly after a security incident) experts recommend establishing some form of time synchronization among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. 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.

5.1 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\t/var/log/secure" \  
        >> /etc/syslog.conf  
fi  
touch /var/log/secure  
chown root:root /var/log/secure  
chmod 600 /var/log/secure  
printf "/var/log/secure\troot.root\t600\n" >> \  
    /etc/permissions.local  
diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Discussion:

The default installation of SuSE Linux captures authpriv.none but it doesn't capture all possible authpriv log messages. Therefore, it should be added. Information that is sent to

the LOG_AUTHPRIV facilities contain a great deal of important security-related events (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc). The above action causes this information to be captured in the /var/log/secure file (which is only readable by the superuser). This file should be reviewed and archived on a regular basis.

5.2 Turn On Additional Logging For FTP Daemon

Action:

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

Discussion:

The above script ensures that all connections are logged and the log format is the vsftpd default.

5.3 Confirm Permissions On System Log Files

Action:

```
cd /var/log

for FILE in /var/log/boot.log* /var/log/messages*
/var/log/news/* /var/log/pgsql /var/log/samba/*
/var/log/sa/*; do
    [ -e $FILE ] && chmod o-rwx $FILE
    printf "$FILE\troot.root\t600\n" >> \
```

CIS SuSE Linux Benchmark

```
        /etc/permissions.local
done
printf "/var/log/pgsql \tpostgres.postgres\t600\n" >> \
    /etc/permissions.local
for FILE in /var/log/news/* ; do
    printf "$FILE\tnews.news\t640\n" >> \
        /etc/permissions.local
done

chown -R root:root .
chgrp /var/run/utmp wtmp
printf "/var/run/utmp \troot.wtmp\t640\n" >> \
    /etc/permissions.local
[ -e news ] && chown -R news:news news
[ -e pgsql ] && chown postgres:postgres pgsql
[ -e squid ] && chown -R squid:squid squid
for FILE in /var/log/squid/* ; do
    printf "$FILE \tsquid.squid\t640\n" >> \
        /etc/permissions.local
done
```

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.

5.4 Configure syslog 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 \
SuSE Benchmark Section 5.4\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.

6 File/Directory Permissions/Access

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

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($3 ~ /^ext[23]$\|^reiserfs$/ && $2 != "/") \
    { $4 = $4 ",nodev" }; \
    { print }' /etc/fstab.tmp > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
printf "/etc/fstab \troot.root\t644\n" >> \
    /etc/permissions.local
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.

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

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($2 ~ /^\/m.*\/(floppy|cdrom)$/) \
    { $4 = $4 ",nosuid,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:

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 filesystems to mount with the nodev option, as explained in item 6.1.

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.

6.3 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:

```
cp -p /etc/fstab /etc/fstab.tmp
cat /etc/fstab.tmp | \
sed 's|\( /media/[fc].* *subfs .*[ ,]\)\|\
'user\([ ,]\)\|\1nouser\2|'| \
sed 's|\( /media/[fc].* *subfs .*[ ,]\)\|\
'users\([ ,]\)\|\1nouser\2|'| > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
rm -f /etc/fstab.tmp
```

```
diff /etc/fstab-preCIS /etc/fstab
```

Discussion:

In SLES, only the root user can mount removable media such as a floppy or cdrom for use, by default. However if /etc/fstab has been changed to allow user mounting, then this item will remove the risk posed by user mounting.

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 examines the floppy and cdrom media entries in /etc/fstab and changes the user or users option to nouser (thereby preventing user mounting).

6.4 Verify passwd, shadow, and group File Permissions

Action:

```
cd /etc
chown root:root passwd shadow group
chmod 644 passwd group
chmod 600 shadow
printf "/etc/passwd \troot.root\t644\n" >> \
    /etc/permissions.local
printf "/etc/group \troot.root\t644\n" >> \
    /etc/permissions.local
printf "/etc/shadow \troot.root\t600\n" >> \
    /etc/permissions.local
```

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>) – the successor to Tripwire – are excellent products for alerting you to changes in these files. Whereas AIDE is an improvement to the non-commercial version of Tripwire, it is still listed as Beta software, and may not be suitable for Enterprise Production systems.

6.5 World-Writable Directories Should Have Their Sticky Bit Set

Action:

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

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

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

There should be no entries returned.

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.

6.6 Find Unauthorized World-Writable Files

Action:

The automated testing tool supplied with this benchmark will flag unexpected world-writable files on the system.

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

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

There should be no entries returned. If `grub.conf` shows up, its permissions will be adjusted in step 7.8.

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

6.7 Find Unauthorized SUID/SGID System Executables

Action:

The automated testing tool supplied with this benchmark will flag unexpected set-UID and set-GID applications on the system.

Administrators who wish to obtain a list of the set-UID and set-GID programs currently installed on the system may run the following commands:

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

6.8 Find All Unowned Files

Action:

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

There should be no entries returned.

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.

6.9 Disable USB Devices (AKA Hotplugger)

Hotplugger cannot be removed without removing xfree86. Removing the X server is beyond the scope of this Benchmark. This section is retained for consistency with the other Linux Benchmarks.

7 System Access, Authentication, and Authorization

7.1 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 $FILE
    printf "$FILE \troot.root\t644\n" >> \
        /etc/permissions.local
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).

7.2 Create *ftusers* Files

Action:

```
for NAME in `cut -d: -f1 /etc/passwd`; do
    if [ `id -u $NAME` -lt 500 ]; then
        echo $NAME >> /etc/ftusers
    fi
done
chown root:root /etc/ftusers
chmod 600 /etc/ftusers
printf "/etc/ftusers \troot.root\t644\n" >> \
    /etc/permissions.local
diff /etc/ftusers-preCIS /etc/ftusers
```

Discussion:

`/etc/ftusers` contains a list of users who *are not* allowed to access the system via `vsftpd` and `lukem-ftpd`. 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.

7.3 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" \
        && $0 !~ /-nolisten tcp/) \
        { $3 = $3 " -nolisten tcp" }; { print }' \
        Xservers-preCIS > Xservers
    chown root:root Xservers
    chmod 444 Xservers
    printf "/etc/X11/xdm/Xservers \troot.root\t444\n" >> \
        /etc/permissions.local
    diff Xservers-preCIS Xservers
fi
```

CIS SuSE Linux Benchmark

```
if [ -e /etc/sysconfig/displaymanager ]; then
    cd /etc/sysconfig/
    cat displaymanager-preCIS |
        sed 's|\(DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN\)'\
'.*.yes.|\1="no"|' > displaymanager
    chown root:root displaymanager
    chmod 644 displaymanager
    printf "/etc/sysconfig/displaymanager
\troot.root\t644\n" >> \
        /etc/permissions.local
    diff displaymanager-preCIS displaymanager
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.

7.4 Restrict *at/cron* To Authorized Users

Action:

```
cd /var/spool/cron/
rm -f deny
echo root > allow
diff allow-preCIS allow
chown root:root cron.allow
chmod 400 cron.allow
printf "/var/spool/cron/allow \troot.root\t400\n" >> \
    /etc/permissions.local
cd /etc
rm -f at.deny
echo root > at.allow
diff at.allow-preCIS at.allow
chown root:root at.allow
chmod 400 at.allow
printf "/etc/at.allow \troot.root\t400\n" >> \
    /etc/permissions.local
```

Discussion:

The `crontab.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 `crontab.allow`, cron jobs can still be run as that user. `crontab.allow` only controls administrative access to the `crontab` command for scheduling and modifying cron jobs.

7.5 Restrict Permissions On `crontab` Files

Action:

```
chown root:root /etc/crontab
chmod 400 /etc/crontab
printf "/etc/crontab \troot.root\t400\n" >> \
    /etc/permissions.local
chown -R root:root /var/spool/cron
chmod -R go-rwx /var/spool/cron
for FILE in /var/spool/cron/*; do
    printf "$FILE \troot.root\t400\n" >> \
        /etc/permissions.local
done
ls | grep cron | grep -v preCIS | xargs chown -R root:root
ls | grep cron | grep -v preCIS | xargs chmod -R go-rwx
for FILE in `ls /etc/* | grep cron | grep -v preCIS`; do
    printf "$FILE \troot.root\t400\n" >> \
        /etc/permissions.local
done
```

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.

7.6 Configure `xinetd` Access Control

Action:

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

CIS SuSE Linux Benchmark

```
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/port Sentry.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.

7.7 Restrict Root Logins To System Console

Action:

```
echo console >> /etc/securetty
chown root:root /etc/securetty
chmod 400 /etc/securetty
printf "/etc/securetty \troot.root\t400\n" >> \
    /etc/permissions.local
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.

7.8 Set LILO/GRUB Password

Note: Bastille configuration set to 'No'

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

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

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

Replace `<password>` with an appropriate password for your organization.
2. Execute the following commands as root:

```
chown root:root /etc/lilo.conf
chmod 600 /etc/lilo.conf
printf "/etc/lilo.conf \troot.root\t600\n" >> \
    /etc/permissions.local
lilo
```

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

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

```
password <password>
```

Replace `<password>` with an appropriate password for your organization.
2. Execute the following commands as root:

```
chown root:root /etc/grub.conf
chmod 600 /etc/grub.conf
```

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.

7.9 *Require Authentication For Single-User Mode*

Action:

```
cd /etc
if [ "`grep -l sologin inittab`" = "" ]; then
    awk '{ print }; /^id:[0123456sS]:initdefault:/ \
        { print "~:S:respawn:/sbin/sologin" }' \
        inittab > inittab.tmp
    mv -f inittab.tmp inittab
    chown root:root inittab
    chmod 644 inittab
    printf "/etc/inittab \troot.root\t644\n" >> \
        /etc/permissions.local
fi
diff inittab-preCIS inittab
```

Discussion:

On some Linux systems you can enter single user mode simply by typing "linux single" at the LILO prompt or in the GRUB boot-editing menu. This 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.

SuSE Linux prevents this risk, by default, however this item checks for the proper setting and puts it back in place if it is missing.

The 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.

7.10 *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.

7.11 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.

Action:

Read `syslog` manpage for the `-l`, `-r` and `-s` options.

Edit `/etc/sysconfig/syslog` and look for the line that says:

```
SYSLOGD_PARAMS=""
```

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

```
SYSLOGD_PARAMS="-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.

8 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/>.

8.1 Block System Accounts

Action:

```
for NAME in `cut -d: -f1 /etc/passwd`; do
    MyUID=`id -u $NAME`
    if [ $MyUID -lt 500 -a $NAME != 'root' ]; then
        usermod -L -s /bin/false $NAME
    fi
done
```

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 machine 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. `/bin/false` is a good choice—it is a valid executable that is not a valid login shell. `/bin/false` is the choice used by Novell for SuSE Linux instead of `/dev/null` or `/bin/nologin`.

This section expands upon section 3.6 for locking out users.

8.2 Verify That There Are No Accounts With Empty Password Fields

Action:

The command:

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

should return no lines of output.

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 "NP" or "*LOCKED*".

8.3 Set Account Expiration and Password Parameters On Active Accounts

Action:



```
cd /etc
cp login.defs login.defs.tmp
if [ `grep -c "^PASS_MIN_LEN" login.defs` -eq 0 ]; then
    echo "PASS_MIN_LEN 6" > login.defs.tmp
fi
awk '($1 ~ /^PASS_MAX_DAYS/) { $2="90" }
    ($1 ~ /^PASS_MIN_DAYS/) { $2="7" }
    ($1 ~ /^PASS_WARN_AGE/) { $2="28" }
    ($1 ~ /^PASS_MIN_LEN/) { $2="6" }
    ($1 ~ /^LOGIN_RETRIES/) { $2="3" }
    { print } ' login.defs.tmp > login.defs
chown root:root login.defs
chmod 640 login.defs
printf "/etc/login.defs \troot.root\t640\n" >> \
    /etc/permissions.local
rm login.defs.tmp
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
```

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 6 characters.

These are recommended starting values. Some regulated industries require more restrictive values – ensure they comply with your Enterprise security policy.

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

Action:

The command:

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

should return no lines of output.

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.

8.5 Verify That No UID 0 Accounts Exist Other Than Root

Action:

The command:

```
awk -F: '($3 == 0) { print $1 }' /etc/passwd
```

should return only the word "root".

Discussion:

Any account with UID 0 has superuser privileges on the system. The only superuser account on the machine should be the root account, and it should be accessed by logging in as an unprivileged user and using the su command (or equivalent) to gain additional

privilege.

Finer granularity access control for administrative access can be obtained by using the – freely-available `sudo` program (<http://www.courtesan.com/sudo/>).

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

Action:

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

To find '.' in \$PATH:

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

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

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

These commands should produce no output.

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 horse program.

8.7 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.

8.8 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.

8.9 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.

8.10 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 $FILE
    printf "/etc/$FILE \troot.root\t444\n" >> \
        /etc/permissions.local
    diff ${FILE}-preCIS $FILE
done

cd /root
for FILE in .bash_profile .bashrc .cshrc .tcshrc; do
    if ! egrep -q 'umask.*77' $FILE ; then
        echo "umask 077" >> $FILE # See description
    fi
    chown root:root $FILE
    printf "/root/$FILE \troot.root\t600\n" >> \
        /etc/permissions.local
    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.

8.11 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 9 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.

8.12 Limit Access To The Root Account From su

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/
if [ `grep -c "^auth *required *pam_wheel.so" su` -eq 0 ]
then
    printf "auth        required        pam_wheel.so
use_uid\n" \
    >> su
```

```
fi
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 ensure the following line exists in `/etc/pam.d/su`:

```
auth required pam_wheel.so
```

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.

8.14 Reboot

Action:

```
init 6
```

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.

9 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>.

9.1 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.
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 issue.net motd; do
    cp -f ${FILE} ${FILE}.tmp
    egrep -vi "SUSE|kernel" ${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

if [ "`grep -i authorized /etc/issue`" == "" ]; then
    echo "Authorized uses only. All activity may be \
monitored and reported." >> /etc/issue
fi
```

CIS SuSE Linux Benchmark

```
if [ "`grep -i authorized /etc/motd`" == "" ]; then
    echo "Authorized uses only. All activity may be \
monitored and reported." >> /etc/motd
fi
diff issue.net-preCIS issue.net
```

3. Create banners for network access:

```
cp -fp /etc/issue /etc/issue.net
if [ "`grep -i authorized /etc/issue.net`" == "" ]; then
    echo "Authorized uses only. All activity may be \
monitored and reported." >> /etc/issue.net
fi
```

4. Protect banner:

```
chown root:root /etc/motd /etc/issue /etc/issue.net
chmod 644 /etc/motd /etc/issue /etc/issue.net
for FILE in motd issue issue.net; do
    printf "/etc/$FILE \troot.root\t644\n" >> \
/etc/permissions.local
done
```

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.

9.2 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
```

CIS SuSE Linux Benchmark

```
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
    printf "/etc/X11/xdm/kdmrc \troot.root\t644\n" >> \
        /etc/permissions.local
    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
    printf "/etc/X11/gdm/gdm.conf \troot.root\t644\n" >> \
        /etc/permissions.local
    diff gdm.conf-preCIS gdm.conf
fi
```

Discussion:

The commands above set the warning message on xdm, kdm and gdm – that is, all of the X display managers.

9.3 Create "authorized only" Banners For vsftpd, 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
fi
```

Discussion:

This item configure's vsftpd "authorized users only" banner messages.

10 Anti-Virus Consideration

Anti-Virus Products

Certain systems – such as mail servers and file servers – should have anti-virus 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 Computer Associates InoculateIT http://www.cai.com/	Commercial Commercial

11 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.

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.

SN.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).

*SN.2 Change Default Greeting String For **sendmail***

Not applicable to SuSE as SuSE does not ship with sendmail.

SN.3 Enable TCP SYN Cookie Protection

Action:

```
echo "echo 1 > /proc/sys/net/ipv4/tcp_syncookies" \  
>> /etc/init.d/boot.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.

SN.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`.

SN.5 Evaluate Packages Associated With Startup Scripts

Question:

How many of the startup script do you really need?

Perform the action below.

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

In some cases, you will not be able to remove a script/package – `kdcrotate` is a good

example: it belongs to package `krb5-libs`, which is required by several packages, including `sendmail` and `nss_ldap`. In cases like this, you may just want to use `chkconfig <sccriptname> off` to keep it from running.

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

SN.6 Evaluate Every Installed Package

Question:

How much unused software was installed on your system?

Perform the action below.

Action:

See Discussion

Discussion:

SuSE Linux installation includes many packages that are usually not necessary in an Enterprise server environment (`dosfstools`, for example). 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

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

in one shell, and then using the other shell to remove the packages. You will find some packages are dependent upon others and you will have to remove several packages at once. In some cases, an unused package will be required by another useful package, and it will have to remain installed – for example, `dateconfig` may rely upon `audiofile`. If the features of `dateconfig` are required, then `audiofile` will have to remain. One may think that the functionality of `dateconfig` is not necessary, however, this tool is used to adjust the date, timezone and NTP settings of the server, and some Enterprises

will have problems making system changes to servers without using the vendor-recommended tools.

Also note that if the service is disabled, the relevant software should be removed for the following reasons:

1. Less software to maintain and monitor for security issues.
2. The service cannot be inadvertently enabled by an errant administrator.
3. Minimize damage in an attack should the attacker gain (or already have) access to the server.

Removed software can always be reinstalled using the Enterprise procedures.

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

SN.7 Install and Configure `sudo`

Action:

Using your Enterprise process, 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.

SN.8 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
printf "/etc/sysctl.conf \troot.root\t600\n" >> \
    /etc/permissions.local
```

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.

SN.9 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:

Remove the following packages if they exist on your system:

```
gcc gcc3 gcc3-c++ gcc3-g77 gcc3-java gcc3-objc
gcc-c++ gcc-chill gcc-g77 gcc-java gcc-objc bin86
dev86 nasm.
```

Discussion:

C compilers pose a credible threat to production systems and should not be installed. Compilers should be installed on select development systems – those systems that have a Business need for a compiler – and the resulting output binaries deployed onto other development and production systems using the existing Enterprise change processes.

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
```

CIS SuSE Linux Benchmark

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/ssh_config /etc/ssh/sshd_config /etc/hosts.deny \  
/etc/hosts.allow /etc/rc.status \  
/etc/inittab /etc/sysctl.conf /etc/syslog.conf /etc/ftpaccess \  
/etc/vsftpd.conf /etc/vsftpd/vsftpd.conf /etc/syslog.conf /etc/fstab \  
/etc/security/console.perms /etc/passwd /etc/shadow /etc/ftpusers \  
/etc/vsftpd.ftpusers /etc/X11/xdm/Xservers /etc/X11/gdm/gdm.conf \  
/etc/X11/xinit/xserverrc /etc/cron.deny /etc/at.deny /etc/crontab \  
/etc/securetty /etc/lilo.conf /etc/grub.conf /etc/exports \  
/etc/init.d/syslog /etc/profile /etc/csh.login /etc/csh.cshrc \  
/etc/bashrc /root/.bash_profile /root/.bashrc /root/.cshrc \  
/root/.tcshrc /etc/security/limits.conf /etc/issue /etc/motd \  
/etc/issue.net /etc/X11/xdm/Xresources /etc/X11/xdm/kdmrc \  
/etc/sysctl.conf /var/spool/cron/allow /var/spool/cron/deny \  
/etc/login.defs /etc/bash.bashrc /etc/default/useradd /etc/pam.d/su \  
/at.allow /etc/permissions.local /etc/postfix/master.cf; 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
```

CIS SuSE Linux Benchmark

```
echo "Completed file backups - backing up directories"

for DIR in \
    /etc/xinetd.d    /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."
```


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 7.8 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**

See the `umask` discussion in sections 3.1 and 8.10. Do not just blindly change the `umask` without fully understanding the ramifications of doing so. Read the `umask` discussion in sections 3.1 and 8.10.

Q: Would you like to disable the `gcc` compiler? **Yes**

Removing compilers unless absolutely necessary is a long-standing industry best practice.

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

Allowing `sendmail` to process the mail queue is a good idea as important alerts may have been generated and will be sitting in the queue, waiting to be processed.

Q: Would you like to deactivate the Apache web server? **Yes**

Note: All answers regarding Apache configuration are non-intrusive answers as configuring Apache is outside of the scope of a Level 1 Operating System Benchmark.

Q: Would you like to bind the web server to listen only to the localhost? **No**

Q: Would you like to bind the web server to a particular interface? **No**

Q: Would you like to deactivate the following of symbolic links? **No**

Q: Would you like to deactivate server-side includes? **No**

Q: Would you like to disable CGI scripts, at least for now? **No**

Q: Would you like to disable indexes? **No**

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

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

Note: This question is asked twice to account for both types of printing systems – BSD `lpr` and `cups`. Most servers will not need to print. If they do need to print, the printing functionality will be restored in section 3.14.

Q: Would you like to disable user privileges on the FTP daemon? **No**

Note: All answers regarding FTP configuration are non-intrusive answers as configuring the FTP daemon is outside of the scope of a Level 1 Operating System Benchmark.

CIS SuSE Linux Benchmark

Q: Would you like to disable anonymous download? No

Q: Would you like to install TMPDIR/TMP scripts? No

Q: Would you like to run the packet filtering script? No

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 set more restrictive permissions on the
administration utilities? [N]
FilePermissions.generalperms_1_1="N"
# Q: Would you like to disable SUID status for mount/umount?
FilePermissions.suidmount="Y"
# Q: Would you like to disable SUID status for ping? [Y]
FilePermissions.suidping="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 cardctl? [Y]
FilePermissions.suidcard="Y"
# Q: Would you like to disable SUID status for at? [Y]
FilePermissions.suidat="Y"
# Q: Would you like to disable SUID status for DOSEMU? [Y]
FilePermissions.suiddos="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 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 usernetctl? [Y]
FilePermissions.suidusernetctl="Y"
# Q: Would you like to disable SUID status for traceroute? [Y]
FilePermissions.suidtrace="Y"
# Q: Would you like to disable SUID status for Xwrapper? [N]
FilePermissions.suidXwrapper="N"
# Q: Would you like to disable SUID status for XFree86? [N]
FilePermissions.suidXFree86="N"
# Q: Should Bastille disable clear-text r-protocols that use IP-based
authentication? [Y]
AccountSecurity.protectrhost="Y"
# Q: Would you like to enforce password aging? [Y]
AccountSecurity.passwdage="Y"
# Q: Would you like to restrict the use of cron to administrative
accounts? [Y]
```

CIS SuSE Linux Benchmark

```
AccountSecurity.cronuser="Y"
# Q: Do you want to set the default umask? [Y]
AccountSecurity.umaskyn="Y"
# Q: What umask would you like to set for users on the system? [077]
AccountSecurity.umask="027"
# Q: Should we disallow root login on tty's 1-6? [N]
AccountSecurity.rootttylogins="N"
# 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 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 disable CTRL-ALT-DELETE rebooting? [N]
BootSecurity.secureinittab="N"
# Q: Would you like to password protect single-user mode? [Y]
BootSecurity.passsum="Y"
# Q: Would you like to set a default-deny on TCP Wrappers and xinetd?
[N]
SecureInetd.tcpd_default_deny="N"
# Q: Should Bastille ensure the telnet service does not run on this
system? [Y]
SecureInetd.deactivate_telnet="Y"
# Q: Should Bastille ensure inetd's FTP service does not run on this
system? [Y]
SecureInetd.deactivate_ftp="Y"
# Q: Would you like to display "Authorized Use" messages at log-in
time? [Y]
SecureInetd.banners="Y"
# Q: Who is responsible for granting authorization to use this machine?
SecureInetd.owner="its owner"
# Q: Would you like to disable the gcc compiler? [N]
DisableUserTools.compiler="Y"
# Q: Would you like to put limits on system resource usage? [N]
ConfigureMiscPAM.limitsconf="N"
# Q: Should we restrict console access to a small group of user
accounts? [N]
ConfigureMiscPAM.consolelogin="N"
# Q: Would you like to add additional logging? [Y]
Logging.morelogging="Y"
# Q: Do you have a remote logging host? [N]
Logging.remotelog="N"
# Q: Would you like to set up process accounting? [N]
Logging.pacct="N"
# Q: Would you like to disable apmd? [Y]
MiscellaneousDaemons.apmd="Y"
# Q: Would you like to deactivate NFS and Samba? [Y]
MiscellaneousDaemons.remotefs="Y"
# Q: Would you like to disable PCMCIA services? [Y]
```

CIS SuSE Linux Benchmark

```
MiscellaneousDaemons.pcmcia="Y"
# Q: Would you like to disable the DHCP daemon? [Y]
MiscellaneousDaemons.dhcpd="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 routed? [Y]
MiscellaneousDaemons.disable_routed="Y"
# Q: Would you like to deactivate gated? [Y]
MiscellaneousDaemons.disable_gated="Y"
# Q: Would you like to deactivate NIS server programs? [Y]
MiscellaneousDaemons.nis_server="Y"
# Q: Would you like to deactivate NIS client programs? [Y]
MiscellaneousDaemons.nis_client="Y"
# Q: Would you like to disable SNMPD? [Y]
MiscellaneousDaemons.snmpd="Y"
# Q: Do you want to stop sendmail from running in daemon mode? [Y]
Sendmail.sendmaildaemon="Y"
# Q: Would you like to run sendmail via cron to process the queue? [N]
Sendmail.sendmailcron="Y"
# Q: Would you like to disable the VRFY and EXPN sendmail commands? [Y]
Sendmail.vrfyexpn="Y"
# 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 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 deactivate the following of symbolic links? [Y]
Apache.symmlink="N"
# Q: Would you like to deactivate server-side includes? [Y]
Apache.ssi="N"
# Q: Would you like to disable CGI scripts, at least for now? [Y]
Apache.cgi="N"
# Q: Would you like to disable indexes? [N]
Apache.apacheindex="N"
# Q: Would you like to disable printing? [N]
Printing.printing="Y"
# Q: Would you like to disable printing? [N]
Printing.printing_cups="Y"
# Q: Would you like to disable user privileges on the FTP daemon? [N]
FTP.userftp="N"
# Q: Would you like to disable anonymous download? [N]
FTP.anonftp="N"
# Q: Would you like to install TMPDIR/TMP scripts? [N]
```

CIS SuSE Linux Benchmark

```
TMPDIR.tmpdir="N"  
# Q: Would you like to run the packet filtering script? [N]  
Firewall.ip_intro="N"
```

Appendix D Change History

January 3, 2006 – Version 1.0

- Original conversion from the Red Hat Linux Benchmark. This Benchmark is a fork of the RHEL Benchmark, version 1.0.3, and updated concurrently with version 1.0.4 of the RHEL Benchmark.

References

The Center for Internet Security

Free benchmark documents and security tools for various OS platforms and applications:

<http://www.cisecurity.org/>

SuSE Linux Enterprise Server Administration Guide

SuSE Linux Enterprise Server User Guide

Other Misc Documentation

Various documentation on Linux security issues:

Primary source for information on NTP

<http://www.ntp.org/>

Information on MIT Kerberos:

<http://web.mit.edu/kerberos/www/>

Apache "Security Tips" document:

http://httpd.apache.org/docs-2.0/misc/security_tips.html

Information on Sendmail and DNS:

<http://www.sendmail.org/>

<http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf>

OpenSSH (secure encrypted network logins):

<http://www.openssh.org>

TCP Wrappers source distribution:

<ftp://porcupine.org>

PortSentry and Logcheck (port and log monitoring tools):

<http://sourceforge.net/projects/sentrytools/>

Swatch (log monitoring tool):

<http://www.oit.ucsb.edu/~eta/swatch/>

Open Source Sendmail (email server) distributions:

<ftp://ftp.sendmail.org/>

CIS SuSE Linux Benchmark

LPRng (Open Source replacement printing system for Unix):

<http://www.lprng.org/>

sudo (provides fine-grained access controls for superuser activity):

<http://www.courtesan.com/sudo/>

Tripwire – file modification utility

<http://www.tripwire.org>