the CENTER for
INTERNET SECURITY

Slackware Linux Benchmark v1.1

(for Slackware 10.2)

Slackware Linux Benchmark v1.0
October 24, 2005

TERMS OF USE AGREEMENT

Background.

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

No Representations, Warranties, or Covenants.

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

User Agreements.

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

1.No network, system, device, hardware, software, or component can be made fully secure;
2.We are using the Products and the Recommendations solely at our own risk;
3.We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4.We have the sole responsibility to evaluate the risks and benefits of the Products and

Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5.Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and

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

Grant of Limited Rights.

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

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

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

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

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

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

Special Rules.

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

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

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

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

Table of Contents

Applicability

This benchmark was developed and tested on Slackware Linux version 10.2. It is likely to work for older versions of Slackware and other Linux distributions as well.

Conventions

The following typographical conventions are used in this document:

Arial font	normal text
`Courier New font`	used to indicate either a command or a standard Unix parameter or a file
Italics	used for a question that you must evaluate before continuing

Root Shell Environment Assumed

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

```
/bin:/sbin:/usr/bin:/usr/sbin
```

Executing Actions

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

Reboot Required

Rebooting the system is required after completing all of the actions below in order to complete the re-configuration of the system. In many cases, the changes made in the steps below will not take effect until this reboot is performed. If substantial operating system updates are performed after the initial OS load, you may have to reboot more than once.

Vulnerabilities

In addition to any specific issues presented by a particular service or protocol, ***every*** service has the potential of being an entry point into a system if 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 run `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 System Administrator needs to understand what the system will be used for before installing Slackware, because Slackware does not have a default partitioning. It is up to the administrator to setup the system according to his needs.

Some general rules of thumb are:

/home could need to be large to support a large number of users with accounts on the server
/var could need to be larger for mail, databases, logs / could need to be bigger for KDE (installs under /opt)

However, Slackware does have some certain minimums, so please consult the Slackware documentation and the links on partitioning listed at the end of this document:

<u>General Server</u>

SWAP	- double RAM (but generally not more than 1 GB)
/	- [1 G]
/home	- [100 M - remainder of disk]
/usr	- [3 G]
/var	- [2 G]
/opt	- [1 G]

Desktop (Single User)

SWAP	- double RAM (but generally not more than 1 GB)
/	- [2 G]
/home	- [1 G - remainder of disk]
/usr	- [3 - 4 G]
/var	- [1 G]
/opt	- [1 G]

Slackware Default Full Installation (without Open Office)

/bin	- 5.6 M
/boot	- 3.3 M
/dev	- 348 K
/etc	- 9.8 M
/lib	- 24 M
/lost + found	- 16 K
/mnt	- 16 K
/opt	- 600 M
/proc	- 3 K
/root	- 1.5 M
/sbin	- 11 M
/sys	- 4 K
/tmp	- 64 K
/usr	- 2.2 G
/var	- 21 M

It is important to keep /var and /home (and possible /opt) on their own partitions. Some applications have a tendency to crash when the / or /usr file system 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.

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

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 and security patching efforts for the administrators. This Benchmark makes no recommendation for the removal of unused software (other than compilers and debuggers in section 8.12). 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.

1 Patches, Packages and Initial Lockdown

1.1 Apply Latest OS Patches

Action:

Update system using Slackware package update procedures.

Discussion:

Developing a procedure for keeping up-to-date with package updates 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.

You can receive notice of security updates by joining the Slackware security mailing list on http://www.slackware.com/lists/. Security advisories are published at: http://www.slackware.com/security/.

When Slackware publishes an update, they include the procedures with it for updating the package. This usually entails downloading the new packages from the Slackware ftp site. The location is: ftp://ftp.slackware.com/pub/slackware/slackware-10.2/patches/

There will be two directories, packages and source, either compile the source or use `pkgtool` to install the patched software. All the applications listed in those directories, have been patched for security vulnerabilities since the distribution release, so make sure you update your system.

Some companies make these packages available over an NFS share or an internal anonymous FTP/HTTP server – your company may follow this practice or do something different.

It is also important to observe that your applications work properly after updating. Though problems in updated packages are quite rare in Slackware, it is generally recommended that updated packages be deployed to a non-production system first for testing.

Some packages may need to be installed before others. The instructions on the Slackware web site will document these needs. 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-updated, non-hardened machine to download the updates, as this involves connecting a system with security vulnerabilities on a network, which is not an Industry Best Practice. Please consider these issues carefully.

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`".

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

cp sshd_config sshd_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
    /^#? *X11Forwarding/ \
        { print "X11Forwarding yes"; next };
    /^#? *IgnoreRhosts/ \
        { print "IgnoreRhosts yes"; next };
    /^#? *RhostsAuthentication/ \
        { print " RhostsAuthentication no"; next };
    /^#? *RhostsRSAAuthentication/ \
        { print "RhostsRSAAuthentication no"; next };
    /^#? *HostbasedAuthentication/ \
        { print "HostbasedAuthentication no"; next };
    /^#? *PermitRootLogin/ \
        { print "PermitRootLogin no"; next };
    /^#? *PermitEmptyPasswords/ \
        { print "PermitEmptyPasswords no"; next };
    /^#? *Banner/ \
        { print "Banner /etc/issue.net"; next };
    {print}' sshd_config.tmp > sshd_config
rm sshd_config.tmp
diff sshd_config-preCIS sshd_config
```

Discussion:

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

The settings in this section attempt to ensure safe defaults for both the client and the server. Specifically, both the ssh client and the sshd server are configured to use only SSH protocol 2, as security vulnerabilities have been found in the first SSH protocol. This may cause compatibility issues at sites still using the vulnerable SSH protocol 1   these sites should endeavor to configure all systems to use only SSH protocol 2.

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

1.4 Enable System Accounting

Action:

Install package `sysstat`.

```
cd /usr/src
tar xvzf sysstat-6.0.1.tgz
cd sysstat-6.0.1
make config – the defaults are okay to use
make
make install
```

`systat` provides a file named `crontab` which is then added to root's cron jobs.

```
crontab -l > cron.temp
cat crontab >> cron.temp
crontab cron.temp
```

Note: You may want to edit the cron jobs and fine tune the way sysstat works, and change the reporting, use `man sar` for more information.

Discussion:

Note: Slackware does not include `sysstat`. It is not available on the Slackware packages web site www.linuxpackages.net. You will need to get it from the sysstat home page (http://perso.wanadoo.fr/sebastien.godard/) , compile and install it manually.

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.

2 Minimize `inetd` 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

Action:

```
cp /etc/inetd.conf /etc/inetd.conf.original
sed \
   -e 's/^\(echo\)/\#\1/' \
   -e 's/^\(discard\)/\#\1/' \
   -e 's/^\(daytime\)/\#\1/' \
   -e 's/^\(chargen\)/\#\1/' \
   -e 's/^\(time\)/\#\1/' \
   -e 's/^\(ftp\)/\#\1/' \
   -e 's/^\(telnet\)/\#\1/' \
   -e 's/^\(comsat\)/\#\1/' \
   -e 's/^\(shell\)/\#\1/' \
   -e 's/^\(login\)/\#\1/' \
   -e 's/^\(exec\)/\#\1/' \
   -e 's/^\(talk\)/\#\1/' \
   -e 's/^\(ntalk\)/\#\1/' \
   -e 's/^\(klogin\)/\#\1/' \
   -e 's/^\(eklogin\)/\#\1/' \
   -e 's/^\(kshell\)/\#\1/' \
   -e 's/^\(krbupdate\)/\#\1/' \
   -e 's/^\(kpasswd\)/\#\1/' \
   -e 's/^\(pop\)/\#\1/' \
   -e 's/^\(imap\)/\#\1/' \
   -e 's/^\(uucp\)/\#\1/' \
   -e 's/^\(tftp\)/\#\1/' \
   -e 's/^\(bootps\)/\#\1/' \
   -e 's/^\(finger\)/\#\1/' \
   -e 's/^\(systat\)/\#\1/' \
   -e 's/^\(netstat\)/\#\1/' \
   -e 's/^\(auth\)/\#\1/' \
   -e 's/^\(netbios\)/\#\1/' \
   -e 's/^\(swat\)/\#\1/' \
   -e 's/^\(rstatd\)/\#\1/' \
   -e 's/^\(rusersd\)/\#\1/' \
   -e 's/^\(walld\)/\#\1/' \
/etc/inetd.conf > /etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
diff /etc/inetd.conf-preCIS /etc/inetd.conf
```

For these changes to take effect, you should either reboot, or

```
killall -s HUP inetd
```

Discussion:

Although other distributions have moved to using `xinetd` as the default network supervisor, Slackware Linux continues to use `inetd`.

The stock `inetd` configuration has improved considerably. However many services which were either rarely-used or for which there were more secure alternatives. After enabling SSH, it is possible to nearly do away with all `inetd`-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 Slackware configuration file `/etc/inetd.conf`.

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.

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: 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.

Note: The above script assumes a netmask of 255.255.255.0. If yours is different, you will have to adjust `/etc/hosts.allow` for your environment.

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

Firewall

See discussion.

Discussion:

TCP Wrappers (`tcpd`) and Host-Based Firewalls (`iptables`) 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.

The TCP Wrapper tools included in Slackware are:

`tcpd` - access control facility for internet services (the TCP Wrapper daemon)
`tcpdchk` - tcp wrapper configuration checker
`tcpdmatch` - predicts how the tcp wrapper would handle a specific request for service.

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, but not activated) or via commercial offerings. The Center for Internet Security makes no recommendations for a vendor or even a specific firewall configuration as firewalls are very complex systems. Entire books have been written on `iptables` and are outside the scope of this benchmark.

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

See the following `iptables` resources to learn how to activate and build the rules for the firewall:

Web-Based

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

Package-Based

- FireHOL - http://firehol.sourceforge.net/
- Firewall Builder - http://sourceforge.net/projects/fwbuilder/
- GuardDog - http://www.simonzone.com/software/guarddog/
- Firestarter - http://www.fs-security.com/

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:

```
sed -e 's/^\#[ \t]*\(telnet\)/\1/' /etc/inetd.conf >
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

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 Slackware 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/). Note that PuTTY does not use the OpenSSL cryptographic library. Other SSH implementations for Windows can be found here: http://www.openssh.com/windows.html 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, run:

```
sed -e 's/^\(telnet\)/\#\1/' /etc/inetd.conf > \
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

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

To use PROFTP (Professional File Transfer), run:

```
sed -e '/proftpd/s/^\#[ \t]*\(ftp\)/\1/' /etc/inetd.conf >\
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

or

To use VSFTP (Very Secure File Transfer), run:

```
sed -e '/vsftpd/s/^\#[ \t]*\(ftp\)/\1/' /etc/inetd.conf >
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
```

```
killall -s HUP inetd
```

Discussion:

Slackware comes with two ftp servers – `vsftpd` (Very Secure File Transfer Protocol) and `proftpd` (Professional File Transfer Protocol).

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/rsh/rcp` If Absolutely Necessary

Question:

Is there a mission-critical reason why rlogin/rsh/rcp must be used instead of the more secure ssh/scp?

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

Action:

```
sed -e 's/\#[ \t]*\(shell\)/\1/' \
-e 's/\#[ \t]*\(login\)/\1/' /etc/inetd.conf > \
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
```

```
killall -s HUP inetd
```

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:

```
sed -e 's/\#[ \t]*\(tftp\)/\1/' /etc/inetd.conf > \
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

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 Slackware 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:

```
sed -e 's/\#[ \t]*\(imap\)/\1/' /etc/inetd.conf > \
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

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, IMAP may be activated.

Slackware provides standard IMAP, which is not encrypted and allows an attacker to eavesdrop on e-mails being transferred or to take over the connection. It may, based on which authentication method is used, allow an attacker to steal user passwords as well.

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:

```
sed -e 's/\#[ \t]*\(pop\)/\1/' /etc/inetd.conf > \
/etc/inetd.conf.temp
mv -f /etc/inetd.conf.temp /etc/inetd.conf
killall -s HUP inetd
```

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, pop3s may be activated.

Slackware provides a standard POP3 server, which is not encrypted and thus allows an attacker to eavesdrop on e-mails being transferred or to take over the connection. It may – based on which authentication method is used – allow an attacker to steal user passwords as well.

3 Minimize boot services

3.1 Disable `inetd`, If Possible

Action:

```
/etc/rc.d/rc.inetd stop
chmod ugo-x /etc/rc.d/rc.inetd
```

Discussion:

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

3.2 Disable `sendmail` Server, If Possible

Question:

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

Proceed with the appropriate actions below.

Action – Yes – `sendmail` is required:

```
chmod ugo+x /etc/rc.d/rc.sendmail
```

Action – No – `sendmail` is not required:

```
chmod ugo-x /etc/rc.d/rc.sendmail
```

Discussion:

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

3.3 Disable GUI Login If Possible

Question:

Is there a mission-critical reason to run a GUI login program on this system?

If the answer to this question is no, proceed with the actions below.

Action:

```
sed -e 's/id:4:initdefault:/id:3:initdefault:/' \
< /etc/inittab-preCIS > /etc/inittab
chown root:root /etc/inittab
chmod 0600 /etc/inittab
```

Discussion:

There is usually no reason to run X Windows on a dedicated server machine, like a dedicated web server. This action disables the graphical login, if present, leaving the user to login via SSH or a normal text-based console. If you elect to deactivate the GUI login screen, users can still run X Windows by typing `startx` at the shell prompt. In Slackware, there are two main runlevels that the system runs in. Runlevel 4 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.

3.4 Disable Standard Boot Services

Action:

```
for FILE in acpid alsa atalk bind cups dnsmasq font.new \
    gpm hotplug httpd mysqld nfsd pcmcia portmap \
    samba saslauthd sendmail serial sysvinit \
    udev wireless yp; do
    /etc/rc.d/rc.$FILE stop
    chmod ugo-x /etc/rc.$FILE
done
for USERID in lp sync mail news uucp games ftp smmsp \
    mysql rpc sshd gdm operator pop nobody bin daemon \
    adm; do
    usermod -L -s /dev/null $USERID
done
```

Discussion:

Note: sshd was not included in the above script because it is considered an essential service, if you do not need it for your environment because you always use console access, just add sshd in one of the for loops in the action above – however, you will not be able to log in remotely with ssh if you do this.

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.

Slackware has a simple approach to startup scripts. There are a number of rc.* scripts in /etc/rc.d. These can be deactivated individually by removing the execute permission with chmod ugo-x /etc/rc.d/rc.script, and reactivated by setting the execute permission with chmod ugo+x /etc/rc.d/rc.script.

This process deactivates most of the rc-scripts, 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 chmod ugo+x /etc/rc.d/rc.daemon.

Note that security upgrades and updates may restore some of the original entries in the startup script directories /etc/rc.d/rc.* – it is always a good idea to check /etc/rc.d and remove any scripts that may have been added by upgrades or patches.

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.

The second 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 /dev/null for an additional layer of security as long as shell access is not necessary. Bear in mind that some packages (find-utils 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. The benchmark's recommended action will register some trivial errors on each distribution version as a result – these are not cause for alarm.

3.5 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:

```
chmod ugo+x /etc/rc.d/rc.samba
/etc/rc.d/rc.samba start
```

Discussion:

Slackware 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.

The SysAdmin may also wish to remove the packages from the system:

```
cd /var/log/packages
removepkg samba
```

3.6 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:

```
chmod ugo+x /etc/rc.d/rc.portmap
/etc/rc.d/rc.portmap start
```

Discussion:

Note: This section needs to precede the next two sections (3.7 and 3.8).

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.

3.7 Only Enable NFS Server Processes If Absolutely Necessary

Question:

Is this machine an NFS file server?

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

Action:

```
chmod ugo+x /etc/rc.d/rc.nfsd
/etc/rc.d/rc.nfsd start
```

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 (`man exports`).

3.8 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:

```
chmod ugo-x /usr/sbin/ypbind
```

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.

3.9 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:

```
chmod ugo+x /etc/rc.d/rc.yp
/etc/rc.d/rc.yp start
```

Discussion:

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

Note: Slackware has every line in `/etc/rc.d/rc.yp` commented out by default. A SysAdmin would have to modify that file, plus the other NIS configuration files to get NIS working. If your NIS server is also a NIS client, you will need to skip section 3.10.

3.10 Only Enable Printer Daemon Processes If Absolutely Necessary

Question:

Is this system a print server, or is there a mission-critical reason why users must submit print jobs from this system?
If the answer to this question is yes, proceed with the actions below.

Action:

```
if [ -e /etc/rc.d/rc.cups ]; then
    chmod ugo+x /etc/rc.d/rc.cups
    /etc/rc.d/rc.cups start
    sed -e 's/^\#User lp/User lp/' /etc/cups/cupsd.conf \
        -e 's/^\#Group sys/Group sys/' \
        /etc/cups/cupsd.conf-preCIS >/etc/cups/cupsd.conf
    chown root:root /etc/cups/cupsd.conf
    chmod 600 /etc/cups/cupsd.conf
fi
diff /etc/cups/cupsd.conf-preCIS /etc/cups/cupsd.conf
```

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

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

3.11 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:

```
chmod ugo+x /etc/rc.d/rc.httpd
/etc/rc.d/rc.httpd start
```

Discussion:

If you are running a web server, make sure you check for security advisories. For suggestions on how to configure Apache, check out the guide from the Center for Internet Security: http://www.cisecurity.org/bench_apache.html

3.12 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:

```
chmod ugo+x /etc/rc.d/rc.bind
/etc/rc.d/rc.bind start
```

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.

Additionally, consider the use of Access Control Lists (ACL's) in `/etc/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.

3.13 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 the action.

```
chmod ugo+x /etc/rc.d/rc.mysqld
/etc/rc.d/rc.mysqld start
```

Discussion:

If this machine does not need to run the mainstream database (SQL) server MySQL, it is safe to deactivate it. If you need to enable it, issue the command (above).

There is another SQL database called PostgreSQL, it is available from: http://www.linuxpackages.net/

Before running the above action, MySQL must be configured. By default, there are 4 configuration files provided in /etc:

```
my-huge.cnf
my-large.cnf
my-medium.cnf
my-small.cnf
```

Choose one of these and copy it to /etc/my.cnf – edit the file to suit your needs.

In sections, 3.6 and 8.1 the mysql user was "locked down." Before starting the MySQL daemon, we must unlock the mysql user:

```
     usermod -U -s /bin/bash mysql
```

Also, the database needs to be initialized before starting the daemon. This is done by logging in as the mysql user and initializing the database with these commands:

```
     su - mysql
     mysql_install_db
     exit
```

Then run above action to start the mysql daemon.

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
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
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 Security Note 8, 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
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.

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/var/log/secure" \
        >> /etc/syslog.conf
fi
touch /var/log/secure
chown root:root /var/log/secure
chmod 600 /var/log/secure
diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Discussion:

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

Not all Linux distributions, especially the older ones, capture logging information which is sent to the `LOG_AUTHPRIV` facilities. This is unfortunate, since a great deal of important security-related information is sent via these channels (e.g., 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
    awk '/^#?xferlog_std_format/ \
        { print "xferlog_std_format=NO"; next };
    /^#?log_ftp_protocol/ \
        { print "log_ftp_protocol=YES"; next };
    { print }' /etc/vsftpd.conf-preCIS > /etc/vsftpd.conf
    if [ `egrep -c log_ftp_protocol /etc/vsftpd.conf` == 0 ]; then
        echo "log_ftp_protocol=YES" >> /etc/vsftpd.conf
    fi
    chmod 0600 /etc/vsftpd.conf
    chown root:root /etc/vsftpd.conf
    diff /etc/vsftpd.conf-preCIS /etc/vsftpd.conf
fi
```

Discussion:

Slackware already logs connections and all files transferred in both vsftpd and proftpd. The above script will change the vsftpd configuration file to allow more detailed logs to be kept if vsftpd is used. The proftpd does not provide this level of granularity.

The list of files transferred can be found at `/var/log/xferlog` and the list of ftp connections can be found at `/var/log/secure` for both proftpd and vsftpd.

5.3 Confirm Permissions On System Log Files

Action:

```
cd /var/log
# Permissions for other
#   log files in /var/log
chmod o-rwx btmp cron* debug* dmesg faillog lastlog maillog* \
messages* secure* spooler* syslog* wtmp xferlog
#   directories in /var/log
chmod o-w apache cups iptraf nfsd samba sa uucp
#   contents of directories in /var/log
chmod o-rwx apache/* cups/* iptraf/* nfsd/* samba/* sa/* uucp/*
#   Slackware package management
chmod o-w packages removed_packages removed_scripts \
scripts setup
chmod o-rwx packages/* removed_packages/* removed_scripts/* \
scripts/* setup/*
```

```
# Permissions for group
#   log files in /var/log
chmod g-wx btmp cron* debug* dmesg faillog lastlog maillog* \
messages* secure* spooler* syslog* wtmp xferlog
#   directories in /var/log
chmod g-w apache cups iptraf nfsd samba sa uucp
#   contents of directories in /var/log
chmod g-wx apache/* cups/* iptraf/* nfsd/* samba/* sa/* uucp/*
#   Slackware package management
chmod g-w packages removed_packages removed_scripts \
scripts setup
chmod g-wx packages/* removed_packages/* removed_scripts/* \
scripts/* setup/*

# Permissions for owner
#   log files in /var/log
chmod u-x btmp cron* debug* dmesg faillog lastlog maillog* \
messages* secure* spooler* syslog* wtmp xferlog
#   contents of directories in /var/log
chmod u-x apache/* cups/* iptraf/* nfsd/* samba/* sa/* uucp/*
#   Slackware package management
chmod u-x packages/* removed_packages/* removed_scripts/* \
scripts/* setup/*

# Change ownership
chown -R root:root .
chown uucp uucp
chgrp uucp uucp/*
chgrp utmp wtmpq
```

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 `syslogd` to Send Logs to a Remote LogHost

Action:

In the script below, replace loghost with the proper name (Full Quallified Domain Name

(FQDN), if necessary) of your loghost.

```
printf "### Following lines added by CISecurity \
Slackware 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.

For more information or remote logging use: `man syslogd`.

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
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 Verify `passwd`, `shadow`, and `group` File Permissions

Action:

```
cd /etc
chown root:root passwd shadow group
chmod 644 passwd group
chmod 400 shadow
```

Discussion:

These are the default owners and access permissions for these files. It is worthwhile to periodically check these file permissions as there have been package defects that changed `/etc/shadow` permissions to 644.

Tripwire (http://www.tripwire.org/downloads/index.php) and AIDE (http://sourceforge.net/projects/aide) – the successor to Tripwire – are excellent products for alerting you to changes in these files. Whereas AIDE is an improvement to Tripwire, it is still listed as Beta software, and may not be suitable for enterprise production systems.

6.4 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" || $3 == "ext3" || \
     $3 == "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 (`chmod +t <filename>`) to any world writable directories found in order to avoid breaking any application dependencies on a given directory.

6.5 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 '($3 == "ext2" || $3 == "ext3" || \
     $3 == "reiserfs") \
     { print $2 }' /etc/fstab`; do
     find $PART -xdev -type f \
     \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned.

Discussion:

Data in world-writable files can be modified and compromised by any user on the system. World-writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. 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.

6.6 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 '($3 == "ext2" || $3 == "ext3" || \
     $3 == "reiserfs") \
     { 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 either by removing files or changing the permissions (`chmod -s <filename>`), but always consult relevant vendor documentation in order to avoid breaking any applications.

6.7 Find All Unowned Files

Action:

```
for PART in `awk '($3 == "ext2" || $3 == "ext3" || \
     $3 == "reiserfs") \
     { 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.

6.8 Disable USB Devices (AKA Hotplugger)

Question:

Is there a mission-critical reason to allow use of PCMCIA or USB-based devices on this system?
If the answer to this question is no, then perform the action below.

Action:

To stop the packages from running and prevent them from running at boot:

```
cd /etc/rc.d
/etc/rc.d/rc.pcmcia stop
chmod ugo-x rc.pcmcia
/etc/rc.d/rc.hotplug stop
chmod ugo-x rc.hotplug
```

Once the packages have been stopped, to completely remove the packages from the system (no reboot required):

```
cd /var/log/packages
removepkg pcmcia*
removepkg hotplug*
```

Discussion:

PCMCIA cards, USB drives and memory devices represent another attack vector against your systems. The prices for a 512MB or even 1GB USB memory device have become very affordable, and is enough storage to transport vast quantities of data off a system. Few servers have any need for PCMCIA or USB devices and this whole avenue should be disabled.

Another possible attack would be to have a bootable Linux system installed on the USB device. Most modern BIOS' allow booting from USB devices, so this would let a person with physical access to a server an extremely easy way take over a system and bypass some of the security you are setting up. See the discussion regarding floppy and CD-ROM drives in section 6.2.

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

7 System Access, Authentication, and Authorization

7.1 Disable rhosts Support

Is there a mission-critical reason to allow the use of the BSD-style “r-commands”on this system?
If the answer to this question is no, then perform the action below.

Action:

```
chmod ugo-x /usr/bin/rlogin
chmod ugo-x /usr/bin/rsh
chmod ugo-x /usr/bin/rcp
```

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.

To permanently disable `.rhosts` support, the administrator can remove the following files:

```
    /usr/bin/rlogin
    /usr/bin/rsh
    /usr/bin/rcp
```

7.2 All `.rhosts` Files Should Be Readable Only By Their Owner

Action:

```
find / -type f -name '.rhosts' | xargs chmod 600
```

Discussion:

Ensure that .rhosts files are only readable by the owner of the file (i.e., these files should be mode 600).

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.

7.3 Create ftpusers Files

Action:

```
for NAME in `cut -d: -f1 /etc/passwd`; do
    if [ `id -u $NAME` -lt 500 ]; then
        echo $NAME >> /etc/ftpusers
    fi
done
chown root:root /etc/ftpusers
chmod 600 /etc/ftpusers
diff /etc/ftpusers-preCIS /etc/ftpusers

if [ -e /etc/vsftpd.conf ]; then
    rm -f /etc/vsftpd.ftpusers
    cp -fp /etc/ftpusers /etc/vsftpd.ftpusers
    diff /etc/vsftpd.ftpusers-preCIS /etc/vsftpd.ftpusers
fi
```

Discussion:

/etc/ftpusers and /etc/vsftp.ftpusers contain a list of users who are not allowed to access the system via proftpd and vsftpd, respectively.

Generally, only normal users should ever access the system via FTP – there should be no reason for "system" type accounts to be transferring information via this mechanism. Certainly the root account should never be allowed to transfer files directly via FTP.

7.4 Prevent X Server From Listening On Port 6000/tcp

Action:

```
if [ -e /etc/X11/xdm/Xservers ]; then
    cd /etc/X11/xdm
    awk '($1 !~ /^#/ && $3 == "/usr/X11R6/bin/X") \
        { $3 = $3 " -nolisten tcp" };
    { print }' Xservers-preCIS > Xservers
    chown root:root Xservers
    chmod 444 Xservers
    diff Xservers-preCIS Xservers
fi
if [ -d /etc/X11/xinit ]; then
    cd /etc/X11/xinit
    if [ -e xserverrc ]; then
        awk '/X/ && !/^#/ \
        { print $0 " :0 -nolisten tcp \$@"; next }; \
        { print }' xserverrc-preCIS > xserverrc
    else
        cat <<END > xserverrc
#!/bin/bash
exec X :0 -nolisten tcp \$@
END
    fi
    chown root:root xserverrc
    chmod 755 xserverrc
    diff xserverrc-preCIS xserverrc
fi
FILE=/opt/kde/share/config/kdm/kdmrc
if [ -e $FILE ]; then
    sed -e 's/^#ServerArgsLocal/ServerArgsLocal/' $FILE-preCIS >
$FILE
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.

Note: gdm is not supplied, as Gnome is not supplied with Slackware.

7.5 Restrict `at/cron` To Authorized Users

Action:

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

Discussion:
The `cron.allow` and `at.allow` files are a list of users who are allowed to run the `crontab` and at commands to submit jobs to be run at scheduled intervals. On many systems, only the system administrator needs the ability to schedule jobs. Note that even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user. `cron.allow` only controls administrative access to the `crontab` command for scheduling and modifying `cron` jobs.

7.6 Restrict Permissions On `crontab` Files

Action:

```
chown root:root /etc/crontab
chmod 400 /etc/crontab
chown -R root:root /var/spool/cron
chmod -R go-rwx /var/spool/cron
ls | grep cron | grep -v preCIS | xargs chown -R root:root
ls | grep cron | grep -v preCIS | xargs chmod -R go-rwx
```

Discussion:

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

7.7 Configure `inetd` Access Control

Action:

See discussion below.

Discussion:

To enhance access control further (from section 2.2) to to daemons spawned from inetd or that run all the time, consider the following applications: PortSentry or PSAD. These programs provide an additional layer of access control protection at the application layer.

The PortSentry tool (http://sourceforge.net/projects/sentrytools/) 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. Also, note that PortSentry does not seem to be actively supported, since its last update was in May 2003.

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 and is currently maintained.

7.8 Restrict Root Logins To System Console

Action:

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

Discussion:

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

Many Enterprises – who use serial port concentrators to connect to a server in a data center without physically having to use the keyboard – consider the serial port a console. This is in keeping with the Unix server tradition of controlling headless Unix machines using a serial port console. Just like the virtual consoles, this one needs protected as well. If this applies to your organization, you may execute these lines:

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

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

7.9 Set `LILO` Password

Action:

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
lilo
```

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. Make sure to replace `<password>` in the actions above with a good password.

7.10 Require Authentication For Single-User Mode

Action:

See discussion below.

Discussion:

By default on Slackware, if you attempt to enter single user mode by typing "linux single" at the LILO prompt, you are then required to login as root and enter the root password.

If an attacker has access to the physical machine, there are a range of attacks that can be made, including booting from the Slackware installation cdrom, booting a Knoppix cdrom, or using LILO attacks that allow brief root access enough to change the root password.

To help prevent these sorts of attacks, you should consider setting the BIOS to boot only from the main hard disk and locking this setting with a BIOS password. Even these measures can be defeated on some servers by opening the box and resetting BIOS to its defaults. Physical security of the hardware is important. 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, and Bastille does not support Slackware, the system administrator may want to apply the precautions in the article.

7.11 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.

7.12 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/rc.d/rc.syslog` and look for the line that says:

```
/usr/sbin/syslogd
```

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

```
/usr/sbin/syslogd -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 /dev/null $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 machines does not use the daemon/service that each is responsible for, though it is safest to simply deactivate them as is done here. To deactivate them, lock the password and set the login shell to an invalid shell. `/dev/null` is a good choice because it is not a valid login shell, and should an attacker attempt to replace it with a copy of a valid shell the system will not operate properly. Note, if the administrator is using the MySQL service, they will need to change the shell back to bash. The command to do this is:

```
     usermod -L -s /bin/bash mysql
```

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*`".

The default Slackware indicator for a locked system account is “`!*`”. Optionally, the administrator may want to run the following script, that will change empty password fields and the default Slackware locked password indicator “`!*`” to “`*LOCKED*`”.

```
awk 'BEGIN { OFS=":"; FS=":"} ($2 == "" || $2 == "!*") \
     { $2 = "*LOCKED*" }; \
     { print } ' /etc/shadow > /etc/shadow.tmp
mv -f /etc/shadow.tmp /etc/shadow
chmod 400 /etc/shadow
```

Note: even if an account has no password, the second field will still show a hashed value.

8.3 Set Account Expiration Parameters On Active Accounts

Action:

```
cd /etc
awk '($1 ~ /^PASS_MAX_DAYS/) { $2="90" }
    ($1 ~ /^PASS_MIN_DAYS/) { $2="7" }
    ($1 ~ /^PASS_WARN_AGE/) { $2="28" }
    ($1 ~ /^PASS_MIN_LEN/) { $2="6" }
    { print } ' login.defs-preCIS > login.defs
chown root:root login.defs
chmod 640 login.defs
diff login.defs-preCIS login.defs
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 $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 the root account) to force password changes every

90 days, and then prevent password changes for seven days thereafter. Users will begin receiving warnings 28 days before their password expires. Slackware also has the option of expiring idle accounts after a certain number of days (see the on-line manual page for the `usermod` command, particularly the -f option). 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 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 achieved by using `sudo` and `visudo`. Administrators can find more information by checking the man pages.

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. If output is produced, the administrator should audit the scripts in `/etc/profile` and `/etc/profile.d`.

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

Action:

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 (used by ftp) 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, such as using sftp.

8.10 Set Default umask For Users

Action:

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

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

Discussion:

With a default umask setting of 077 – a setting agreed to as part of the consensus process with DISA and NSA – files and directories created by users will not be readable by any other user on the system. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile, .cshrc, etc.) in their home directories. A umask of 027 would make files and directories readable by users in the same Unix group, while a `umask` of 022 would make files readable by every user on the system.

We adjust root's `umask` setting separately in this item, as root shells don't necessarily read the system-wide configuration files. For example, root sessions using bash doesn't get `umask` settings from `/etc/profile`.

Note: This is been shown to cause problems with the installation of software packages where the installation script uses the default `umask` – the directories are owned by root with 700 permissions, and then the application and/or daemon cannot read its files. A simple fix to this problem is to manually issue a less restrictive `umask` (such as `umask` 022) for the shell session doing the installation, or place such a `umask` command in the beginning to a less restrictive value before the installation, or in the beginning of the installation script.

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:

```
echo "ulimit -Hc 0" >> /etc/profile
diff /etc/profile /etc/profile.preCIS
echo "limit -h coredumpsize 0" >> /etc/csh.login
diff /etc/profile /etc/csh.login.preCIS
```

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 default Slackware installation has core dumps turned off. However, users can easily over-ride this with the `limit` and `ulimit` commands.

The action above will set hard limits for core dumps so that "average" users will be prevented from turning core dumps on. Determined users can still turn core dumps on by starting a shell with command line parameters to prevent starting with `/etc/profile` or `/etc/csh.login` and activating the hard limits. System administrators should regularly review core dump usage on the system, use cron to report on core dumps, and possibly remove core dumps.

8.12 Remove All Compilers and Assemblers

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:

```
cd /var/log/packages
removepkg gcc
removepkg gcc-g++
removepkg gcc-g77
removepkg gcc-gnat
removepkg gcc-java
removepkg gcc-objc
removepkg bin86
removepkg nasm
removepkg gdb
```

Discussion:

Compilers pose a credible threat to production systems and should not be installed. Compilers and debuggers 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.

8.13 Limit Access To The Root Account From `su`

Action:

```
echo "root:ALL:DENY" >> /etc/suauth
chown root:root /etc/suauth
chmod 400 /etc/suauth
diff /etc/suauth-preCIS /etc/suauth
```

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. The script in the action section stops all users from becoming root with the su command. All users that attempt to become root using su, will be rejected.

If the administrator wants to allow certain users (especially the administrators non-root account) change the text in quotes from the first line of the script to something similar to the following example:

```
root:ALL EXCEPT username1, username2, usernameN:DENY
```

If the administrator needs all users belonging to an entire group to be able to use the su command to become root, then change the text in quotes from the first line of the script to something similar to the following example:

```
root:ALL EXCEPT GROUP somegroup:DENY
```

For more information see the suauth man pages.

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:

```
shutdown -r now
```

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. Turn off the automatic creation of the default /etc/motd.

```
FILE=/etc/rc.d/rc.S
sed -e '/> \/etc\/motd/s/^/#/' $FILE > $FILE.temp
mv -f $FILE.temp $FILE
```

2. Create a warning banner before login.

```
cat <<END_ISSUE > /etc/issue
************************************************
NOTICE TO USERS
This is a private system and is the property of
[insert company name here]. It is for authorized
use only. Users (authorized or unauthorized) have
no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on
this system may be intercepted, monitored,
recorded, copied, audited, inspected, and disclosed
to authorized site, and law enforcement
personnel, as well as authorized officials of
other agencies, both domestic and foreign. By
using this system, the user consents to such
```

```
interception, monitoring, recording, copying,
auditing, inspection, and disclosure at the
discretion of the authorized site.

Unauthorized or improper use of this system may
result in administrative disciplinary action and
civil and criminal penalties. By continuing to use
this system you indicate your awareness of and
consent to these terms and conditions of use. DO
NOT LOGIN if you do not agree to the conditions
stated in this warning.
**************************************************
END_ISSUE
```

3. Create a message-of-the-day for after login.

```
cat <<END_MOTD > /etc/motd
*************************************************
NOTICE TO USERS
Use of this system constitutes consent to security
monitoring and testing. All activity is logged
with your host name and IP address.
*************************************************
END_MOTD
```

4. Create a banner for network access.

```
cp -fp /etc/issue /etc/issue.net
echo "Authorized uses only. All activity may be \
monitored and reported." >> /etc/issue.net
```

5. Protect banners.

```
chown root:root /etc/motd /etc/issue /etc/issue.net
chmod 644 /etc/motd /etc/issue /etc/issue.net
```

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.

DoD Warning banner: http://www.dss.mil/infoas/dod_warning_banner.doc
http://www.voled.doded.mil/voled_web/PrivacySecurityDisclaimer.htm

http://ciac.llnl.gov/ciac/bulletins/j-043.shtml

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
fi
if [ -e /opt/kde/share/config/kdm/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
fi
```

Discussion:

The standard graphical login program for Slackware is kdm, which requires the user to enter their username in one text box and their password in a second text box. The commands above set the warning message on xdm and kdm – in case something other than the default X login GUI was installed. See /etc/rc.d/rc.4 for the order of GUI login tools startup, without Gnome (which is no longer supplied with Slackware) the first one to startup is kdm.

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 configures vsftpd "authorized users only" banner messages.

10 Anti-Virus Consideration

10.1 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	Website	Product
Sophos	http://www.sophos.com/	Commercial
NAI Virus Scan	http://www.mcafee.com/us/products/mcafee/antivirus/desktop/vs_commandline.htm	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)	http://www.antivir.de/en/index.html	Commercial
f-prot Antivirus	http://www.f-prot.com/products/corporate_users/unix/	Commercial
Trend Micro	http://www.trendmicro.com/en/products/linux/overview.htm	Commercial
Computer Associates InoculateIT	http://www.cai.com/	Commercial

11 Remove Backup Files

11.1 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`

Action:

If you configure sendmail by using the M4 macro processor to “compile” the configuration files, by editing sendmail.mc and creating sendmail.cf from it:

```
cd /usr/share/sendmail/cf/cf
echo "define(\`confSMTP_LOGIN_MSG', \`mailer ready')dnl" >>
sendmail.mc
make sendmail.cf
cp -f sendmail.cf /etc/mail/sendmail.cf
chown root:bin /etc/mail/sendmail.cf
chmod 444 /etc/mail/sendmail.cf
```

If you use the method of editing sendmail.cf directly:

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

Discussion:

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

SN.3 Enable TCP SYN Cookie Protection

Action:

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

Discussion:

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

SN.4 Additional LILO Security

Action:

```
chattr +i /etc/lilo.conf
```

Discussion:

Setting the immutable flag on the LILO config file will prevent any changes (accidental or otherwise) to the `lilo.conf` file. If you wish to modify the 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 scripts do you really need?

Perform the action below.

Action:

```
cd /etc/rc.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/rc.d and evaluate which of these remaining services are not necessary. To see what package a script belongs to, use grep to search the files in `/var/log/packages`:

```
grep <scriptname> /var/log/packages/*
```

Note the package file name, then view the first part of the package log in `/var/log/packages` to read about it and decide if it can be safely removed.

If it can, use

```
removepkg /var/log/packages/<package>
```

to remove it.

For example, if there are no Macs in your network, or you do not need a file or print server for Macs, then you probably do not the Appletalk daemons, which are started by the `rc.atalk` script. If you `grep` for `rc.atalk` in `/var/log/packages/*`, you can see that this script is part of the netatalk package. A quick view of the start of the file (view `/var/log/packages/netatalk-2.0.3-i486-1` shows that we can remove this package, and `removepkg /var/log/netatalk-2.0.3-i486-1` will remove the package.

Note: Slackware does not provide dependency checking, so it's up to you to confirm that a package can be safely removed. Also be aware that if files have been changed from their original state, they will not be removed by `removepkg`. The package file contains a list of all files, so you should check if they have all been removed.

In some cases, you will not be able to remove a script because it's part of a package that is needed for other things. This does not happen often as Slackware's package granularity is relatively fine. If it does happen, you may just want to use

```
/etc/rc.d/<scriptname> stop
chmod ugo-x <scriptname>
```

to stop the service and prevent it from running again.

SN.6 Evaluate Every Installed Package

Question:

How much unused software was installed on your system?

Perform the action below.

Action:

See Discussion

Discussion:

The default Slackware installation may contain packages that are not necessary in for a server. 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

For example, to remove a unneeded package the administrator can use the `removepkg` tool. When used with the `-warn` flag, the files can be reviewed before actually removing them. See the `removepkg` man page (`man removepkg`) for more information.

```
# removepkg -warn zlib
Only warning... not actually removing any files.
Here's what would be removed (and left behind) if you
removed the package(s):


 --> /usr/lib/libz.so.1 (symlink) was found in another package.
Skipping.
 --> /usr/lib/libz.so (symlink) would be deleted
 --> /usr/lib/libz.so.1.2.3 was found in another package. Skipping.
 --> /usr/doc/zlib-1.2.3/ChangeLog would be deleted
 --> /usr/doc/zlib-1.2.3/FAQ would be deleted
 --> /usr/doc/zlib-1.2.3/INDEX would be deleted
 --> /usr/doc/zlib-1.2.3/README would be deleted
 --> /usr/include/zconf.h would be deleted
 --> /usr/include/zlib.h would be deleted
 --> /usr/lib/libz.a would be deleted
 --> /usr/man/man3/zlib.3.gz would be deleted
 --> /usr/doc/zlib-1.2.3/ (dir) would be deleted if empty
```

Removed software can always be reinstalled if it is needed.

Note: Slackware does not provide dependency checking, so it's up to you to confirm that a package can be safely removed. Also be aware that if files have been changed from their original state, they will not be removed by `removepkg`. The package file contains a list of all files, so you should check if they have all been removed.

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
```

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.

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/rc.d /var/spool/cron/crontabs /etc/cron.* /etc/skel
do
    if [ -d \${DIR}-preCIS ]; then
        echo "Restoring \${DIR}"
        /bin/cp -pr \${DIR}-preCIS \${DIR}
        /bin/rm -rf \${DIR}-preCIS
    fi
done

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/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny \
/etc/csh.login /etc/csh.cshrc /etc/exports /etc/fstab \
/etc/ftpaccess /etc/ftpusers /etc/group \
/etc/hosts.allow /etc/hosts.deny /etc/hosts.equiv \
/etc/inetd.conf /etc/inittab /etc/issue /etc/issue.net \
/etc/lilo.conf /etc/limits.conf /etc/login.defs /etc/motd \
/etc/passwd /etc/profile /etc/proftpd.conf \
/etc/securetty /etc/shadow /etc/suauth /etc/sudoers \
/etc/sysctl.conf /etc/syslog.conf \
/etc/vsftpd.conf /etc/vsftpd.ftpusers \
/etc/X11/xdm/Xresources /etc/X11/xdm/Xservers \
/etc/X11/xinit/xserverrc /opt/kde/share/config/kdm/kdmrc \
/etc/cups/cupsd.conf \
/etc/ssh/ssh_config /etc/ssh/sshd_config \
/root/.bash_profile /root/.bashrc /root/.cshrc /root/.tcshrc; do
    if [ -f ${FILE} ]; then
        # Backup file
        /bin/cp -p ${FILE} ${FILE}-preCIS
        # Add it to the do-restore script
        echo ${FILE} `find ${FILE} -printf "%m"` >> /root/do-
restore.sh
    fi
done

echo "Completed file backups - backing up directories"

for DIR in \
    /etc/rc.d /var/spool/cron/crontabs /etc/cron.* /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."
```

References

The Center for Internet Security
Free benchmark documents and security tools for various OS platforms and applications:
http://www.cisecurity.org/

Slackware
http://www.slackware.com

Patches and related documentation:
http://www.slackware.com/security/
ftp://ftp.slackware.com/pub/slackware/slackware-10.2/patches/

Slackware Book:
http://www.slackbook.org/

General Slackware:
http://wiki.linuxquestions.org/wiki/Slackware
http://wiki.linuxquestions.org/wiki/Slackware-Introduction
http://slackwiki.org/Main_Page

Partitioning:
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/Partition.html
http://twiki.iwethey.org/Main/NixPartitioning

A collection of Slackware Howtos:
http://www.linuxpackages.net/howto/

Other Misc Documentation:

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://www.cisecurity.org/bench_apache.html
http://httpd.apache.org/docs-2.0/misc/security_tips.html
Information on sendmail and DNS:
http://www.sendmail.org/
http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf
OpenSSH (secure encrypted network logins):
http://www.openssh.org
TCP Wrappers source distribution:
ftp.porcupine.org

PortSentry and Logcheck (port and log monitoring tools):
http://sourceforge.net/projects/sentrytools/
Swatch (log monitoring tool):
http://www.oit.ucsb.edu/~eta/swatch/
Open source sendmail (email server) distributions:
ftp://ftp.sendmail.org/
LPRng (Open Source replacement printing system for Unix):
http://www.lprng.org/
CUPS (Common UNIX Printing System):
http://www.cups.org/
sudo (provides fine-grained access controls for superuser activity):
http://www.courtesan.com/sudo/
Tripwire – file modification utility
http://www.tripwire.org
DoD Warning banner:
http://www.dss.mil/infoas/dod_warning_banner.doc
General Warning banners:
http://www.voled.doded.mil/voled_web/PrivacySecurityDisclaimer.htm
http://ciac.llnl.gov/ciac/bulletins/j-043.shtml