Global Information Assurance Certification Paper

Applying the CIS Linux Benchmark v1.1.0 Recommendations to a Mandrake 9.1 Laptop with Higher Security Enabled

Laurie Zirkle
GCUX Practical v1.9, Option 1
Administrivia v2.7
December 23, 2003

ABSTRACT

The Center for Internet Security (CIS) does not have a benchmark or scoring tool available for Mandrake 9.1. This document steps through an installation and comparison of Mandrake 9.1 with the "CIS Linux Benchmark v1.1.0 (Red Hat 7.0 and later)". The intent is not to rewrite the scoring tool software, but to check this installation against the benchmark and make any necessary changes. All changes made to the initial installation are specific to this machine at this site and should not be construed as official recommendations for any other installation.

INTRODUCTION

XYZ has made a laptop available to the system administrator, TNZ. All computers connected to this network from any means (LAN, WAN, modem, WIFI) are checked against the appropriate CIS security benchmarks, with suggestions being implemented in concert with the purpose of the computer.

The function of this laptop is to allow access to the various machines TNZ administers here at XYZ. The chosen operating system is Mandrake 9.1 to be consistent with the majority of XYZ's existing Linux machines. There is only one user for this laptop, whose login is TNZ for the duration of this document. It is the responsibility of TNZ to check the e-mail and log files generated on this laptop.

There is no CIS security benchmark-scoring tool available for this release of Mandrake, so this laptop will have to be checked manually against all the points for the CIS Linux security benchmark. The total "score" from running the benchmark software is of no consequence; the interest is in applying the recommended actions where needed. This paper documents the procedure for the installation and securing of Mandrake 9.1 on this laptop and is based on our own in-house system installation documentation.

It is assumed that the three installation CD's for Mandrake 9.1 are available and that the user has rudimentary Linux file editing skills. The CIS Linux security benchmark this is compared against is available at http://www.cisecurity.org/bench_linux.html.

HARDWARE

Dell Inspiron 8000
Pentium III, 800Mhz
256mb RAM
ATI M4 video controller with 8mb memory
ESS Maestro 3 audio controller

10gb internal hard drive
1 internal floppy drive
1 internal CDROM
1 Cabletron Wireless RoamAbout

RISK FACTORS

The function of this machine is to provide access to the machines that TNZ administers at XYZ. Since this laptop is being used to access XYZ's machines, care must be taken to make the laptop as secure as possible. If it is not secured it can be used by malicious users to gain unauthorized entry into the computers at XYZ.

The X11 window system is needed for some administrative functions run on the remote machines, therefore the display manager on the laptop is activated. There are known vulnerabilities and exploits for the X11 protocol such as session hijacking and packet sniffing. Since X11 is being used for administrative functions, it will have to be secured as best as possible to try to avoid these known vulnerabilities.

SSH (Secure Shell) will be the only means of logging in to the machines at XYZ. There are known exploits for SSH Protocol 1 and the default SSH configuration file values may not be appropriate for this machine.
An Ethernet connection is utilized from inside XYZ to connect to the machines TNZ administers. Network connections are susceptible to a myriad of compromises including sniffing and denial of service.

Physical compromise is also a concern. Without proper password protections a malicious user can gain control of the laptop. A small subset of operations that a malicious user can execute this way is to shutdown, reboot, enter single-user mode or add root-privilege accounts.

INITIAL MANDRAKE INSTALLATION

The initial install is done from CD. After inserting Disc 1 of the Mandrake 9.1 distribution in the CD drive and power cycling the machine, the graphical installation is allowed to start (this is the default action if there is no intervention).

Language

The language screen is the first to appear. The default is English (American), so Next is clicked on to go to the next step.

License Agreement

The license agreement is shown; it is read carefully and in its entirety before accepting or rejecting. The license is agreed to, Accept is chosen and then Next is clicked.

The type of mouse chosen is Standard (the default). Next is clicked.

Different messages appear on the installation screen, as the appropriate drivers are loaded. Once the drivers are loaded the Security screen is displayed.

Security

All of the other computers here that are running Mandrake 9.1 have been installed with the standard level of security; the higher level of security is chosen for this laptop to try to minimize the amount of security-related changes. The Security Administrator's user id (TNZ) is entered in the box below the Security level choice, and then Next is clicked.

Partitioning

Custom disk partitioning is chosen rather than Erase entire disk because the default is to create only / (root), swap and /home[1]. Seven file systems are created:

1. / - root file system
2. /boot - contains the kernel and other configuration files used to boot Mandrake Linux
3. swap - space used for inactive memory pages when physical memory is full
4. /usr - Linux applications
5. /home - user files and data
6. /var - contains dynamic data; used by system processes for things like logging, locks and temporary file space
7. /tmp - temporary user files or temporary space used by user-written programs

The disk-partitioning window will appear. If existing partitions are shown (colored according to the color scheme shown at the top of the window) click Clear all to remove them. Auto allocate will only create / (root), swap and /home. Click on the big clear box under hda to choose a partition. Under Choose action, click the Create box. A small window will appear showing the size, type and mount point. The default sizes, file system types and mount points as they are shown during this install are used.

The first file system created is the / (root) file system. Click on Ok to allocate this file system. The / (root) file system (785mb, Journalised[2] FS) is now shown in the big box. Click on the empty portion of the big box and then on Create for the next file system. This is the /boot file system (800mb, Linux native[3]). Click on Ok, click on the empty portion of the big box, click on Create. This is the swap file system (800mb, Linux swap[4]). Continue with this process (click on OK, click on the empty portion of the big box, click on Create) to create /usr (2526mb, Journalised FS), /home (2565mb, Linux native), /var (1823, Journalised FS) and /tmp (1000mb, Journalised FS). Click on OK to allocate /tmp, then click Done.

A window appears with the message "Partition table of drive hda is going to be written to disk!" Click Ok. The system happily writes the partition information to the disk and creates the partitions.

---

[1] At the very least a separate file system should be made for /var. This directory contains dynamic data and is used by system processes for logging, locks, and temporary file space. Also, /var is system-specific; there is absolutely no reason to allow access to it from other machines.

[2] A "journal" is maintained on disk to insure data integrity and cut down on the time it takes to check the file system after an unclean shutdown.

[3] Not a journaled file system. /boot does not change often so writes to this file system are minimal.

[4] Linux swap is a special file system type that allows fast memory paging.

Now it is time for the package group selection. The packages chosen by default to be installed are:

- Office Workstation - office programs: word processors (kword, abiword), spreadsheets (kspread, gnumeric), pdf viewers, etc.
- Internet station - set of tools to read and send mail and news (pine, mutt, tin …) and to browse the Web
- KDE Workstation - the K Desktop Environment, the basic graphical environment with a collection of accompanying tools.
- Gnome Workstation - a graphical environment with user-friendly set of applications and desktop tools.

First, add the following categories to those already chosen:

- Network Computer (client) - clients for different protocols including ssh.
- Configuration - tools to ease the configuration of your computer.
- Console Tools - editors, shells, file tools, terminals.
- Firewall/router - internet gateway

then uncheck Office Workstation and Gnome Workstation. Click Next. The following appears in a new window:

> You have selected the following server(s): postfix, webmin.
> These servers are activated by default. … Do you really want to install these servers?

Choose No and then click on Next.

Install System

Change CD's as instructed.

Root Password

The root password needs to be set. If Next is clicked without supplying a password, a box will pop up with the following message:

> This password is too short (it must be at least 8 characters long)

A password must be entered and it must be 8 characters in length or longer[5]. Enter a password, verify it by retyping it and click Next.

Add a User

The next task is to add any users that will be allowed to use this laptop. If at least one user is not set up the machine cannot be logged into after the installation is finished and rebooted. This laptop has only one user account, TNZ. Enter the user's real name, the desired user name and an initial password (and verify it). Even though an 8-character password is not required during this step, the chosen password should be at least 8 characters and should include

[5] At this point most people are stumped and enter something extremely simple (or stupid). This is NOT GOOD. The root password should be somewhat complex and include characters, numbers and special characters. Relatively easy to remember phrases, or (even better) first or last letters of a phrase, with numbers and special characters included or added, are good choices. The password should NOT be so difficult to reproduce or type that it has to be written down on a sticky-note and pasted to the side of the monitor. If there is the possibility the password will be forgotten, or it needs to be shared, at the very least store it in an encrypted file somewhere.

upper case, lower case, numeric and special characters. Allow access to only the following for user TNZ:

X programs, network tools and "su"

Click Add user to add the user, then click Next to continue the installation.

Install Bootloader

The boot loader is installed in the default location, which is the first sector of the drive (also known as the Master Boot Record). Click Next.

Summary

After the boot loader is the final configuration. This window lists configurable items. There is no reason to change the keyboard, country, time zone or mouse. Likewise, there is no need to configure a printer or the sound card. To configure the graphical interface, click on Configure across from Graphical interface. Accept the defaults for the time being, clicking on Next after each one:

Flat Panel 1024x768
Rage 128 Mobility
XFree 4.3 with 3-D hardware acceleration
1024x768, 65 thousand colors (16 bit)

Do NOT test the configuration (choose No and click Next), and do NOT allow the graphical interface to start upon booting (choose No and click Next.)

There is no need to configure the network manually. This machine uses the dhcp client software to obtain the name and IP address and the network is automatically enabled during the next reboot.

To configure the Shoreline Firewall (Shorewall) click Configure across from Firewall. To disallow all incoming network connections, uncheck "Everything (no firewall)" and click Next.

The preference for the boot loader is grub[6]. Click Configure across from Bootloader. Set Bootloader to use to be grub. Pick a good password following the previous suggestions for setting a password; verify it by retyping it. Click Next. At this point do not add, modify or remove any of the kernel entries. Click Next.

The last thing to do in this window is to check the boot-time services. Click on Configure (across from Services) and uncheck the following:

Under System: alsa, atd, portmap, rawdevices, sound, xinetd
Under Other: dm, fam
Under File sharing: netfs

Click on Next. The initial installation is almost done. Once back to the list of configurable items, click Next to continue.

Install Updates

The network is not yet operational; no patches can be downloaded at this time. The default for installing updates is no which is correct for this installation. Click Next. The initial installation process is now finished.

[6] At this site grub is preferred over lilo.

Exit Install

Remove the Mandrake 9.1 Disc 3 from the CD drive and click on Reboot.

POST INSTALLATION

There are tasks to execute before the installation phase is considered complete.

Display Setup

The first thing that is done once the laptop is rebooted is to correctly set up the Graphical Display Manager. Use the /etc/X11/XF86Config file that is included in Appendix A. Allow the Display Manager to start on boot:

```
# /sbin/chkconfig --level 3 dm on
#
```

and reboot the laptop:

```
# /sbin/shutdown -r now
#
```

Make a note of which kernel is highlighted in the grub boot window (it is linux-secure). The highlighted kernel is the default kernel that is loaded if there is no manual intervention within 10 seconds. This information is needed later to manually boot a new kernel.

Once the laptop is rebooted, TNZ logs into the console with graphics mode. Using the default window manager (KDE) a terminal window is opened with root privileges; click on the lower left-hand icon (Start Applications), then choose Terminals and click on Konsole - Super User Mode (Terminal Program). Also open a regular non-privileged window (Konsole (Terminal Program)) from under the Terminals menu. Window settings controlling color, font size and window size are reset to TNZ's preferences by the Settings menu at the top of the terminal window. The settings are saved so they don't have to be reset when a new window is opened.

Network Setup

The network is set up automatically by the Mandrake installation. The firewall is set to not allow incoming connections during post installation. This is verified by attempting to connect to the laptop from other machines (ftp, ping, ssh, rpcinfo, telnet) and checking the log entries in /var/log/messages from the shorewall firewall on the laptop.

Install patches and Updates

Installing all available Mandrake 9.1 updates/patches finishes the installation process. The easiest way to do this is via the Mandrake Control Center GUI. The Control Center is started by:

- typing mcc while in the Konsole (root) window,
- clicking on the Mandrake Control Center icon (eighth from the left at the bottom of the screen), or

- clicking on the "Start Applications" icon (first on the left at the bottom of the screen) and then choosing Mandrake Control Center towards the top of the menu.

Once the Control Center window appears, click on "Software Management" and then choose "Mandrake Update". A window appears asking if it is OK to continue (click yes) and if it is ok to get a list of mirrors. Click on "yes" and a new window appears with a list of mirrors. Choose the geographically closest mirror if possible. The program contacts the mirror to generate a list of packages that have updates. Security updates is already checked. Check the boxes next to Bug fixes updates and Normal updates to include their lists. Click on the box next to the software package(s) to update/upgrade it. A description of the software and reason for the update appear on the right-hand side of the highlighted package. If a package has dependencies that need to be updated at the same time the software asks to verify that all should be chosen. Once all the packages to be updated are chosen (this should be everything that is listed), click on Install.

Check for New Kernel

When the updates have finished, the last thing to do is check for new revisions of the kernel. Quit out of the Mandrake Update window and choose the icon above Update to install software packages (RpmDrake helps you install software packages). To search for kernel rpm's, type the word kernel in the box next to the Search button, then click on Search. If a list of kernel packages appears, list the /boot directory in a terminal window and check the numbering of the kernels. The files have numbers something like 2.4.21-0.13 in the names. Compare the numbers from the files in the /boot directory to the numbers in the Mandrake Console Center window. If the numbers shown in the Mandrake Console window are higher than the numbers in the file names of /boot files, then a newer kernel is available.

If a newer kernel is available the next step is determining if it needs to be installed. The MandrakeSecure[7] web resource is used for this. Searching for "kernel" on this web page shows the latest kernel update is 4 months old. The advisory notes that multiple vulnerabilities are fixed. Since the vulnerabilities are security-related, the latest kernel is installed on this laptop.

To install the latest version, choose the kernel- and kernel-secure- files with the largest number (i.e. 2.4.21.0.25), and then click Install. The installation process takes care of adding these kernels to the /boot/grub/* files.
After the new kernel is downloaded and installed, the laptop is rebooted by:

```
# /sbin/shutdown -r now
#
```

Before the kernel actually loads, the grub menu appears with the default kernel highlighted. Before the timeout (which initially is 10 seconds), use the arrow keys to move through the list of available kernels; highlight the new kernel and hit <enter>. (For this particular installation, the new kernel is 2421-25sec). If there are no problems and the new kernel boots and runs successfully, manually edit the /boot/grub/menu.lst and remove or comment out the lines pertaining to older

[7] http://www.mandrakesecure.net/en/advisories/updates.php?dis=9.1

kernels. The new /boot/grub/menu.lst file now has the following kernel boot entries[8]:

```
title 2421-25sec
kernel (hd0,0)/boot/vmlinuz-2.4.21-0.25.mdksecure quiet devfs=mount acpi=off root=/dev/hda1
initrd (hd0,0)/boot/initrd-2.4.21-0.25mdksecure.img

title 2421-25
kernel (hd0,0)/boot/vmlinuz-2.4.21-0.25.mdk quiet devfs=mount acpi=off root=/dev/hda1
initrd (hd0,0)/boot/initrd-2.4.21-0.25mdk.img

title failsafe
kernel (hd0,0)/boot/vmlinuz failsafe devfs=mount acpi=off root=/dev/hda1
initrd (hd0,0)/boot/initrd.img
```

The first entry (2421-25sec) is the default kernel to boot. Towards the top of the /boot/grub/menu.lst file is the entry:

```
default=x
```

Change this to be:

```
default=0
```

so the first entry in the file is booted by default. The laptop now has Mandrake 9.1 with the latest updates and kernel installed.

CIS SECURITY BENCHMARK

The Center for Internet Security (CIS) currently does not support Mandrake 9.1 with the benchmark or tester. The benchmark itself is a good guide for Linux in general, although some of the files and changes are slightly different between versions. It is assumed that the system administrator makes a copy of the original file (using cp -p to keep the original times and permissions) before making any changes. Changes to the system files are done from a privileged window (Konsole - Super User Mode (Terminal Program)).

Operating System Patches

The first step in the benchmark is to apply the latest operating system patches. Patches and upgrades are issued to correct software flaws and security problems. As has been evidenced by the recent spate of Microsoft compromises due to patches not being installed in a timely manner, patch installation needs to be a high priority. On this laptop, patches are already installed as part of the "post installation" procedure.

Modify SSH Configuration

The old remote shell protocols (i.e. rlogin, rsh) have been replaced by the SSH protocols because the old protocols were not secure. Most UNIX™[9]-based machines have a version of SSH, OpenSSH, SSH2, or some other variation that has been adapted for that particular operating system. There are two protocols available with SSH called Protocol 1 and Protocol 2. Known exploits exist for Protocol 1, so this protocol should not be used under any circumstances. This

[8] Using version numbers helps to distinguish between kernels when multiple versions are being tested.
[9] UNIX is a trademark of The Open Group.

laptop runs the OpenSSH client distributed with Mandrake (as opposed to compiling from source). The configuration files and host keys reside in /etc/ssh. This machine does not have the sshd daemon program installed, so the only file in /etc/ssh is ssh_config (client configuration file).

The ssh_config file specifies the settings for the SSH client. The default settings are shown as comments in the file, with any changed settings following at the end. The original settings in this installation are:

```
Host *
        ForwardX11 yes
        Protocol 2,1
                StrictHostKeyChecking no
```

These are changed to:

```
Host *
        ForwardX11 yes
        Protocol 2
                StrictHostKeyChecking ask
```

Setting ForwardX11 to yes allows automatic X11 redirection. The redirection allows X11 programs started from the shell to go through the encrypted SSH channel with the connection to the real X server made from the laptop itself. The DISPLAY variable is not set manually. Setting Protocol to 2 makes Protocol 2 the default with no fallback to Protocol 1. StrickHostKeyChecking is set to ask so TNZ is forced to confirm the host's addition to the user's known host file while hosts with changed keys will cause the connection to be refused.

Disable Non-needed Standard Services

The xinetd daemon starts programs that provide network services. The daemon listens for service requests on the ports associated with each of the services listed in the xinetd configuration, and starts the appropriate server upon request. None of these services are essential for this laptop to function properly. The xinetd service is turned off during the post-installation procedure.

Disable Non-needed Boot Services

UMASK

The default mode for file creation done by the system is set during boot and is implemented by the umask command. Check the setting in the file /etc/init.d/functions by:

```
# /bin/grep umask /etc/init.d/functions
# Make sure umask is sane
umask 022
#
```

A umask of 022 will not allow world-write or group-write on any files that are created. The default umask on this laptop is already set to 022.

XINETD

Xinetd and its predecessor inetd have been used in the past as part of exploit scripts to enable previously closed network ports. These newly enabled ports will usually have root privileges, which in turn can allow a root compromise

to occur. If all services controlled by xinetd are turned off in the above step (Disable Non-needed Standard Services) then the xinetd daemon itself should be turned off. The xinetd daemon is already disabled on this machine as part of the post-installation process. This package is not removed due to the number of dependencies by other software.

SENDMAIL/POSTFIX

The initial installation does not include a mail delivery program. Without a mail delivery agent the output from any system or monitoring program cannot be mailed to TNZ and cron output cannot be mailed to root.

To allow local mail delivery, postfix is installed and configured to run but not accept connections from the outside. To install postfix using the Mandrake Control Center:

- start mcc from the command line or window manager
- choose Software Management
- choose RpmDrake helps you install software packages
- enter postfix into search window
- check postfix and click install
- insert requested CD
- click OK for All requested packages were installed successfully
- click Quit to exit Software Packages Installation
- select Quit under the File menu to quit MCC

Edit the postfix configuration file (/etc/postfix/main.cf) and make the following changes:

- uncomment line 90 (myorigin = $myhostname)
- uncomment line 241 (mynetworks_style = $host)
- comment line 548 (smtpd_banner = $myhostname ESMTP $mail_name ($mail_version) (Mandrake Linux))
- add line 549 (smtpd_banner = $myhostname ESMTP)

Set postfix to start on boot by:

```
# /sbin/chkconfig --level 3 postfix on
#
```

GUI LOGIN AND X FONT SERVER

Allowing X11 connections from remote processes can possibly allow system compromise. Past exploits include keystroke monitoring and session sniffing. Using X11 forwarding via SSH can minimize (but not totally eliminate) these threats because SSH uses an encrypted channel. This machine is not a dedicated server and is running the GUI login.

It is not recommended to have the X font server process run as user root because of possible undiscovered vulnerabilities. The font server should fork and go into the background and it should attempt to run as user xfs. The options for the font server are checked:

```
# /bin/ps gax | grep xfs
xfs -port -1 -daemon -droppriv -user xfs
#
```

Running as a non-root user is the default for this installation.

STANDARD BOOT SERVICES

It is necessary to make sure that all daemons not used or needed at this time are configured NOT to start at system boot. Many of the "standard boot services" have been targets of hackers in the past; others could be targeted in the future. With all non-necessary daemons turned off (and removed, if possible) there is less chance of a compromise from this avenue. The "chkconfig" program queries and updates information for the system boot services. To produce a listing of all services and their status for each system run-level type:

```
# /sbin/chkconfig --list
shorewall       0:off   1:off   2:on    3:on    4:on    5:on    6:off
nfslock         0:off   1:off   2:off   3:off   4:off   5:off   6:off
… …
#
```

The list of disabled services across all run levels on this machine is:

alsa	Linux ALSA sound driver
apmd	Advanced Power Management daemon
atd	"at" daemon; executes commands at a specified time
devfsd	Linux Device File system management daemon
harddrake	hardware probe (can configure changed hardware)
lisa	LAN Information Server
netfs	mount/unmount nfs/smb/ncp mount points
nfslock	nfs file locking
portmap	manage rpc connections
rawdevices	assign raw devices to block devices (used by programs like Oracle)
routed	automatic IP routing
saslauthd	simple authentication and security layer authentication daemon
sound	launches sound system
switchprofile	switch configuration file profile
tmdns	trivial multicast dns responder
xinetd	internet services daemon

To disable these services:

```
# for service in alsa apmd atd devfsd harddrake lisa netfs nfslock portmap \
> rawdevices routed saslauthd sound switchprofile tmdns xinetd
> do
>       /sbin/chkconfig --level 0123456 $service off
> done
#
```

Of this list only the following are removed without causing potential problems due to software dependencies: atd (at), devfsd, harddrake[10], lisa, routed and tmdns. To remove these software packages:

- start MCC from command line or window manager
- choose Software Management
- choose RpmDrake helps you remove software packages

[10] Remove only harddrake, not harddrake-ui.

- enter the package name into the search box (i.e., atd)
- check the box next to the package name and click Remove
- click OK for All requested packages were removed successfully
- click Quit to exit Software Packages Removal
- select Quit under the File menu to quit MCC

Lock Server Accounts

Most server accounts exist to allow daemons to run as users other than "root". In early versions of UNIX™ some of these accounts existed with a generic password or no password at all. It is dangerous to have an account with no password or to leave an account with a default password. Accounts in this state can lead to system compromise in no time at all. This shell loop not only locks the account by adding a "!" at the beginning of the encrypted password string; it also changes that server's shell to /dev/null:

```
# for name in bin daemon adm lp mail news uucp operator games nobody \
> rpm vcsa rpc xfs rpcuser
> do
>         /usr/sbin/usermod -L -s /dev/null $name
> done
#
```

To verify, look at both the /etc/passwd and /etc/shadow files:

```
# cat /etc/passwd
        (contents of password file)
# cat /etc/shadow
        (contents of shadow password file)
#
```

Make sure the shell field for all of the above accounts in the /etc/password file is /dev/null and the password field in /etc/shadow for these accounts has an "!" (exclamation point) as the first character.

Modify Network Parameters

Various low-level network parameters are set or changed to help increase the security of Linux. The settings are defined in the /etc/sysctl.conf file. Some of the recommended settings are already set by default, like net.ipv4.conf.default.rp_filter = 1 to help prevent IP spoofing and net.ipv4.conf.all.log_martians = 1 to log packets with impossible (martian) addresses. Below is a list of parameters that are changed or added, along with the new value and a brief explanation of what the parameter influences.

net.ipv4.tcp.max_syn_backlog = 4096

Default value is 1024. Maximum number of remembered connection requests which have not received an acknowledgement. When this queue is filled, no further incoming SYN connections are processed (SYN flood) and system memory can become exhausted. Systems with >128mb of memory should change this to at least 4096 to help mitigate the effects of SYN flood attacks.

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0
Setting this parameter to 0 will disable source routing.
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
Setting this parameter to 0 will disallow accepting of ICMP source redirects.
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
Setting this parameter to 0 will disallow accepting of ICMP redirect messages for default gateways
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
Setting this parameter to 0 will disable the sending of ICMP redirects

Care should be taken if changing other network parameters, as normal system functionality can be severely hurt.

Check System Logging

It is important to log as much information as possible to keep track of system activity. The syslogd daemon provides this function. System logs are crucial in determining if the system is compromised or is being accessed by users or programs without authority. It is good practice to not only log to the local machine but to also have a central syslog server. Many exploits have erased or modified the local system logs. A central syslog server provides a real-time backup of the system log files.

The AUTHPRIV facility logs authorization and security messages to a secure file, and is implemented by default in this version of Linux. The permissions on the /var/log directory and below are restrictive enough; regular users may list the /var/log directory but are not allowed to read any of the log files, only root is allowed read access.

The machine syslog.full.domain is the central syslog server for the machines that TNZ administers. The facilities and priorities that log to syslog.full.domain are:

- authpriv.* - all authorization messages
- mail.notice - all mail messages with priority normal or above
- cron.=warn - only warning messages from cron
- kern.info - all kernel messages with priority info or above
- daemon.info - all daemon messages with priority info or above

A copy of the /etc/syslog.conf[11] file is available in Appendix B.

Time synchronization is important to correlate logged events with other machines and users. The best way of synchronizing the clock on this laptop with other machines at this site is via NTP (Network Time Protocol). To install NTP from the distribution CD's using the Mandrake Control Center:

- start MCC from command line or window manager

[11] More detailed information about system logging and the different levels and options are available from the manual pages via "man syslogd" and "man syslog.conf".

- choose Software Management
- choose RpmDrake helps you install software packages
- enter ntp into search window
- check ntp-4.1.1-2mdk and click Install
- insert requested CD and click OK
- after ntp is successfully installed click OK
- click quit to exit Software Packages Installation
- choose Mandrake Update helps you apply any fixes …..
- click Yes to contact the mirror
- check listing for updated ntp package
- if updated ntp package exists, check the ntp update , click Install, click OK then click Quit
- if no updated ntp package exists, click Quit.
- exit MCC by clicking Quit under the File Menu

To configure ntp, edit the /etc/ntp.conf file. Comment out line 25:

```
# multicastclient
```

Add the timeservers at the top of the file:

```
server ntpserver1.full.domain
server ntpserver2.full.domain
```

Start the ntp daemon:

```
# /etc/init.d/ntpd start
Starting ntpd:                    [ OK ]
#
```

This daemon automatically starts on boot if /usr/sbin/ntpd is executable and the configuration file /etc/ntp.conf exists.

Modify File System Mounting Options

Custom partitioning is used on this machine. The installation process sets up seven file systems on this machine: /, /boot, /home, /tmp, /usr, /var and swap. For this laptop, there is no need to allow use of devices or SUID (set-user-id) files on most of the file systems. SUID root programs can be used to exploit the system by creating root shells or other programs that when run as root could cause compromise or system destruction.

Since malicious software can still be accessed by a floppy disk or cdrom, these entries in /etc/fstab are also changed. Mounting by regular users is also turned off by deleting the "user" option in the /etc/fstab file for the removable devices. The new /etc/fstab file is:

```
/dev/hda1 / etx3 noatime 1 1
/dev/hda5 /boot ext2 noatime,nodev 1 2
none /dev/pts devpts mode=0620 0 0
/dev/hda8 /home ext2 noatime,nodev,nosuid 1 2
/dev/hdb /mnt/cdrom auto iocharset=iso8859-1,codepage=850,noauto,ro,exec,nodev,nosuid 0 0
/dev/fd0 /mnt/floppy auto iocharset=iso8859-1,sync,codepage=850,noauto,exec,nodev,nosuid 0 0
none /proc proc defaults 0 0
/dev/hda10 /tmp ext3 noatime,nodev,nosuid 1 2
/dev/hda7 /usr ext3 noatime,nodev 1 2
```

```
/dev/hda9 /var ext3 noatime,nodev,nosuid 1 2
/dev/hda6 swap swap defaults 0 0
```

Modify User Console Privileges

By default, Linux gives users logged on via the Console enhanced privileges over removable devices like floppy disks, joysticks, scanners, etc. These are potential security hazards. It is recommended to restrict the privileges that console users have. Even though this laptop has only one user (TNZ), console privileges for the removable devices are disabled. The following devices are commented out at the bottom of the /etc/security/console.perms file (under "permission definitions"):

```
floppy, sound, cdrom, pilot, jaz, zip, ls120, scanner, camera, memstick, flash,
diskonkey, rem_ide, fb, kbd, joystick, v4l, gpm, mainboard, burner, usb
```

Verify passwd, shadow and group File Permissions

Check the file permissions for /etc/passwd, /etc/shadow and /etc/group. No one should have write privileges for /etc/group or /etc/password except for root. The /etc/shadow file does not need to be writable by anyone and only needs to be readable by root. The listing looks like this:

```
# /bin/ls -ls /etc/passwd /etc/shadow /etc/group
4 -rw-r--r--    1 root root     588 Oct 10 13:30 /etc/group
4 -rw-r--r--    1 root root    1240 Oct 13 18:07 /etc/passwd
4 -r--------    1 root root     704 Oct 13 18:07 /etc/shadow
#
```

These are the default permissions for this install.

Sticky Bit Set on World-Writable Directories

Most world-writable directories should have the "sticky bit" set. This bit allows a file to be removed only by the owner, which prevents files being overwritten on multi-user systems. This is a one-user system so this is not that important. However, to check for a list of directories that should have the "sticky-bit" set but don't, execute the following:

```
# find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
#
```

No files are listed by running this find command.

List World-Writable Files

A world-writable file is one that allows anyone and everyone to write to it. This is a potential security vulnerability. To show the list of current world-writable files:

```
# /bin/find / -perm -0002 -type f -xdev -print
#
```

For this installation, no world-writable files exist.

List SUID/SGID System Executables

As mentioned earlier, SUID programs can be used to exploit systems. It is highly recommended that TNZ be familiar with the default list of SUID/SGID files for the system. To find all current SUID/SGID programs:

```
# /bin/find / \( -perm -04000 -o -perm -02000 \) -type f -xdev -print
/sbin/pam_timestamp_check
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd
/sbin/netreport
/bin/ping
/bin/mount
/bin/umount
/bin/su
#
```

/sbin/pam_timestamp_check and /sbin/pwdb_chkpwd verify a calling user's password from a read-protected database (such as /etc/shadow). /sbin/netreport requests notification of network interface changes. /bin/ping sends ICMP ECHO_REQUEST datagrams to a network host. /bin/mount mounts a file system. /bin/umount unmounts a file system. /bin/su allows a user to become a "second user".

The first three files (/sbin/pam_timestamp_check, /sbin/pwdb_chkpwd, /sbin/unix_chkpwd) need root privilege to accomplish their task so the permissions should stay SUID root. The next file (/sbin/netreport) is SGID root and is used by other system programs. It is unclear what will break if SGID root is taken away, so the permissions stay as they are. The next three files (/bin/ping, /bin/mount, /bin/umount) have SUID root permissions taken away by executing the command:

```
# /bin/chmod a-s /bin/ping /bin/mount /bin/umount
#
```

Regular users do not need access to these three programs; TNZ runs the programs as root if needed. The last file (/bin/su) keeps SUID root as these permissions are needed to become a "second user".

Check System Access, Authentication and Authorization

The commands rlogin, rsh and rcp (also referred to as "r-commands") use a weak form of authentication and trust. Exploits exist that will overwrite or add new system names to an existing .rhosts file to gain access. The rlogin, rsh and rcp executables do not exist on this system and there are no entries for rhosts in any of the files in /etc/pam.d. SSH Protocol 1 (also known as the "s-commands") uses an equivalent shost authentication scheme and is disabled during the Modify SSH Configuration task that has previously been executed.

Create symlinks for dangerous files

As stated previously, the "r-commands" have weak access control via the .rhosts and /etc/hosts.equiv files. The "s-commands" (SSH Protocol 1) can also allow weak access control using the .shosts and /etc/shosts.equiv files. The CIS

benchmark recommends creating links from root's .rhosts/.shosts, the /etc/hosts.equiv and /etc/shosts.equiv to /dev/null so any attempts to modify these files are discarded. The "r-commands" are not installed and SSH Protocol 1 is disabled, so these links are not created on this computer[12].

Modify /etc/ftpusers File

Even though an ftp daemon is not currently running on this machine, potential ftp access is restricted. It is prudent to add all accounts listed in /etc/passwd that are not allowed access to ftp to the /etc/ftpusers file. There are known ftp exploits that use local accounts as access points. The following accounts are added to /etc/ftpusers, one per line:

```
root bin daemon adm lp sync shutdown halt mail news uucp operator games
nobody rpm vcsa rpc xfs rpcuser postfix
```

After the /etc/ftpusers file is created the permissions are set for read-only by root:

```
# /bin/chmod 400 /etc/ftpusers
#
```

Check Listening Port for X Server

X servers listen by default on port 6000 for messages from remote clients. As previously mentioned in the section under "Disable Non-needed Boot Services: GUI LOGIN AND X FONT SERVER", X11 has known exploits. Since X authentication is not extremely secure, the X server should not listen for remote clients. This is achieved by adding -nolisten tcp to the server startup command. By default Mandrake 9.1 already has -nolisten tcp on server startup. Running ps and looking for the X server process verifies this:

```
# /bin/ps gax | grep X11
/etc/X11/X -deferglyphs 16 -nolisten tcp -auth /var/run/xauth/A:0-hlquJF
#
```

Restrict at and cron to Authorized Users

There is no reason on this machine to allow anyone but root to run cron jobs. Some earlier versions of cron had flaws that would allow a local user to obtain root privileges. No one at all should be using the "at" command, which was removed in an earlier step. To restrict access to these commands, the /etc/at.deny and /etc/cron.deny files are removed and the user root (and only root) is added to the /etc/at.allow and /etc/cron.allow files. This is the default setup for this installation.

Restrict crontab File Permissions

Only root should have access to the /etc/crontab, /etc/cron.* and /var/spool/cron/* files. Allowing other users write permission can allow system compromise via an unauthorized file in any of these directories. The permissions on /etc/crontab and /etc/cron.* are changed as follows:

```
# /bin/chown -R root:root /etc/crontab /etc/cron.*
# /bin/chmod 400 /etc/crontab
```

[12] Creation of these links were tested and caused TNZ's login to break because /dev/null became mode 600.

```
# /bin/chmod -R go-rwx /etc/cron.*
#
```

The default privileges on /var/spool/cron (700 - read, write, execute by root only) are already correct.

Create Warning Banners

Incoming access points have a warning message or banner to inform any user (authorized or unauthorized) about privacy and monitoring policies. These banners may help successfully prosecute a computer trespasser. The non-existence of warning banners has been used as a defense for intruders ("No warning signs, I didn't know it was off limits …"). Some existing banners give too much system information to potential hackers. It is highly recommended that existing system banners be modified and new ones created where necessary. The warning banner file (with owner root:root, mode 644) is /etc/motd. A very simple "Unauthorized access or use is prohibited. All sessions may be monitored or recorded." is sufficient for this machine.

The /etc/issue and /etc/issue.net files are removed from the system during boot if the security level is set to higher or greater.

Postfix has a banner that is displayed to the connecting machine as part of the initial handshake. Even though no incoming or outgoing SMTP connections are allowed, the banner is modified during the "Disable Non-needed Boot Services: SENDMAIL/POSTFIX" step so that no unnecessary identifying information is revealed.

Configure XINETD Access Control

Even though xinetd is currently turned off, the following line is added to the "defaults" block in /etc/xinetd.conf:

```
only_from = xxx.xxx.0.0/16 yyy.yyy.0.0/16
```

This restricts connections to only the listed networks if the xinetd daemon is running.

Restrict Root Logins to System Console

In general, root should not be allowed to log in directly to a machine from anywhere but the console. Either the su or sudo programs are used to access root functions. (And even su should be restricted pretty tightly. If a system administrator walks away from their terminal or session while in su, even for a few seconds, havoc can result.) By setting the security level to higher during installation of this machine, the /etc/securetty file (which lists where root can log in from) is empty. Direct root logins are not allowed AT ALL from anywhere.

Set LILO/GRUB Password

The boot loader is password protected to help prevent unauthorized access to the system. Without this password protection anyone is allowed to turn the laptop off, back on and then interrupt the process and boot single-user or add options to the boot string. Since this machine is using grub, an encrypted password is added at the top of the file using this process (as root):

```
# grub
grub> md5crypt

Password: **********
Encrypted: averylongstringofwhatlookslikenonsense

grub> quit
#
```

The password is chosen using the same guidelines as for the root password itself. The grub configuration file (/boot/grub/menu.lst) is edited and the very first line becomes:

```
password --md5 averylongstringofwhatlookslikenonsense
```

The --md5 option means the password is encrypted in md5 format[13].

Set Single-User-Mode Authentication

As above, single user mode should be password protected to prevent unauthorized access or changes to the system. Even though the boot loader is protected with a password, an unclean shutdown can cause the system to boot into single-user mode. Without a password anyone can add a root privileged account or cause some other compromise. Requiring the root password when booting into single user mode is the default on this laptop. The following line is added to /etc/inittab by the system installation procedure to request a password for single-user mode:

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

Restrict NFS Client Requests to Privileged Ports

When NFS (Network File System) was originally implemented, the goal was to be able to share files easily between systems. At that time security was not the top priority in designing and coding NFS. The only real way to secure NFS is to turn it off and leave it off. Unfortunately, that is usually not an option. If it needs to be run, care is taken to restrict the client and server side as much as NFS will allow. Setting the "secure" option in the /etc/exports file causes the daemon to ignore requests from clients that do not originate from ports less than 1024, i.e. ignore requests from anything except a root-owned process. NFS is not running on this machine and there is no /etc/exports file (therefore no files are exported).

Verify Password Fields

Accounts that are not password protected are a serious security hazard. Anyone can log into that account and compromise the system within 5 minutes. Verify that all accounts are either locked or have a password by running the command:

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

[13] Setting up an encrypted grub password is covered in the Grub documentation, accessible in Mandrake via "info grub".

This command does not return any output on this machine.

Set Password Expiration Parameters

Even on a one-user system, it is important to routinely change passwords. This site's Internal Audit Department has determined that passwords are changed every 90 days (with a 14 day warning period) and users cannot change their passwords again for at least 14 days. The file controlling password aging is /etc/login.defs. The password-aging part of the file is changed to reflect these constraints:

```
PASS_MAX_DAYS      90
PASS_MIN_DAYS      14
PASS_WARN_AGE      14
```

These changes apply to any new users added, but do not apply to any users that already exist. TNZ is the only user, so to force these limits on that account the following command is run:

```
# /usr/bin/chage -m 14 -M 90 -W 14 tnz
#
```

Verify no '+' Entries in password, shadow or group Files

Verify that there are no entries beginning with '+' in the password, shadow or group files. The '+' is to inform NIS (formerly known as "yellow pages") to include the appropriate map for the rest of the entries of the file. This functionality has been abused by exploits in the past. The entries are checked by:

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

There is no output from this command on this laptop. In addition, NIS is not running on this machine.

Verify Only One UID 0 Account Exists

The user with UID 0, root, has special privileges. There should only be one account with this UID and this is verified by running

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

THERE IS NO NEED TO HAVE MULTIPLE ROOT-PRIVILEGE ACCOUNTS. The sudo program is a good alternative for machines that have multiple people needing root access. Sudo also logs all commands which documents the calling user and the command that is run.

Verify No '.' or Group/World Writable Directories in root's $PATH

Including the current working directory in $PATH can lead to executing programs with unintended consequences. (In the old days, this was a neat trick to pull on unsuspecting friends; alas the good old days are gone.) Commands with the same name as system commands can be in the current working directory. If the current working directory is ahead of the real directory in a user's

$PATH the fake program will be run unless the full path name of the command is used. Hackers have used this concept in the past to install Trojan programs. To check the root's $PATH variable:

```
$ /bin/su - root
Password:
# /bin/echo $PATH
/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/bin:/usr/local/sbin
#
```

The current working directory is not in root's $PATH.
To check for group and world writable files in $PATH, for each directory run

```
# for directory in /sbin /usr/sbin /bin /usr/bin /usr/X11R6/bin /usr/local/bin \
> /usr/local/sbin
> do
>       /bin/echo $directory
>       /bin/find directory -perm -0002 -o -perm -0020 ! -type l -print
> done
/sbin
/usr/sbin
/bin
/usr/bin
/usr/X11R6/bin
/usr/local/bin
/usr/local/sbin
#
```

There is no output from the find command on this machine.

Verify Permissions on User Home Directories

The default permissions on user home directories for this installation are already set to 700 (read/write/execute by owner only). Check home directory permissions:

```
# /bin/ls -ls /home
4 drwx------  28  tnz     tnz      4096  Nov 1  12:14  tnz
#
```

No User Dot-files should be World Writable

The "dot" files (.login, .cshrc, .profile) set up the user's environment. If a "dot" file is world-writable than anyone can edit the file and make any changes they like. (For example, it was great fun to changes a user's .plan file without their knowledge and then have the information show up in "finger".) This can lead to a potential compromise. The default permissions for file creation are already set to not allow world writable files. Check the file permissions:

```
# /bin/ls -la /home/tnz
drwx------      3       tnz     tnz     4096 Nov  1 13:41 .
drwxr-x--x     4       tnz     tnz     4096 Nov  1 13:41 ..
-rw-r--r--     1       tnz     tnz       24  Nov  1 13:41 .bash_logout
-rw-r--r--     1       tnz     tnz      191 Nov  1 13:41 .bash_profile
-rw-r--r--     1       tnz     tnz      124 Nov  1 13:41 .bashrc
```

```
-rw-r--r--    1    tnz    tnz     141 Nov  1 13:41 .mailcap
-rw-r--r--    1    tnz    tnz    3761 Nov  1 13:41 .screenrc
drwx------    2    tnz    tnz    4096 Nov  1 13:41 tmp
#
```

Set Default UMASK in Shell Configuration Files

Set the default UMASK for users to 077 (no read/write/execute by world). This is different than the UMASK set earlier in the document under "Disable Non-needed Boot Services". The UMASK in that section is for system- and daemon-created files; this UMASK is for user-created files. Note that the user can override this by adding a UMASK variable to their shell startup file. To set the default user UMASK, create the following two files that are executed at login time:

```
# /bin/echo "umask 077" > /etc/profile.d/localvars.sh
# /bin/echo "umask 077" > /etc/profile.d/localvars.csh
# /bin/chmod 755 /etc/profile.d/localvars.sh /etc/profile.d/localvars.csh
#
```

Disable Core Dumps

There is no reason to have core dumps enabled on this laptop. Core dumps contain important system configuration data, which can be valuable to an intruder. Core dumps are disabled by editing /etc/security/limits.conf. The original file has all lines commented out. The modified file has the following two lines added or uncommented:

```
*       soft    core    0
*       hard    core    0
```

Set BIOS Password

There are three BIOS passwords that can be set on a Dell Inspiron 8000:

Primary Password (password must be entered for system to boot)
Admin Password (password must be entered to make System Setup changes)
System Primary/Hard-disk drive Password
(prevents the hard drive from booting unless password is entered)

If the Primary Password is lost or forgotten, the only way to recover is to contact Dell by phone, as each laptop has a unique master password. Only after Dell is satisfied about the identity of the owner, they will give out the master primary BIOS password for the laptop. The Admin Password is disabled if the Primary Password is enabled and the Primary Password is disabled if the Admin Password is enabled. The Admin and System Primary passwords are set on this laptop.

Enter BIOS mode by typing Fn/Setup (while holding down the Fn key press the F1 key). Advance to page 6 by Alt-P (while holding down the Alt key press the p key). Set[14] the Admin Password by:

- highlight the Admin Password field using the up/down arrow keys
- press right or left arrow key

[14] Press the escape key to abort the procedure. To disable password enter a zero-length password (i.e., just hit return when prompted to enter password).

- enter new password (at least 4 characters, maximum of 8 characters)[15]
- retype password

The Admin Password field is now locked until the Configure Setup field is enabled. To enable Configure Setup so the BIOS setup fields can be changed:

- highlight the Configure Setup field using the up/down arrow keys
- press right or left arrow key
- enter the Admin Password

(After configuring other BIOS setup fields, return to page 6, highlight the Configure Setup field and press left or right arrow to disable setup configuration.)
The System Primary password is enabled the same way as the Admin Password:

- highlight the System Primary field using the up/down arrow keys
- press right or left arrow key
- enter new password (at least 4 characters, maximum of 8 characters)
- retype password
- WAIT (could be up to a minute) until the field is changed to Enabled

BIOS password setup is complete.

UPKEEP AND MAINTENANCE

Once the system has been installed and tightened down, periodic maintenance and checks are done to insure the integrity and security of the system. It is the responsibility of TNZ to check log files and read e-mail at least daily on this system while it is up and running. The order in which these checks and other periodic maintenance procedures are presented here is random.

Backups

The dump command does not exist on this laptop. Dump is installed from the distribution CDs following the same installation procedure as for NTP earlier. The dump software package includes both dump and restore.

There is enough disk space on this laptop to store the backups on disk. These backups are also copied to another machine, which is backed up on a nightly basis. The directory /home/backups is created with permissions root:root and mode 700.

An initial level 0 dump is performed on each file system except /home; only the tnz directory under /home is dumped.

```
# /sbin/dump 0uf /home/backups/laptop.root.0 /
        (dump program output goes to stdout)
# /sbin/dump 0uf /home/backups/laptop.boot.0 /boot
        (dump program output goes to stdout)
# /sbin/dump 0uf /home/backups/laptop.usr.0 /usr
        (dump program output goes to stdout)
# /sbin/dump 0uf /home/backups/laptop.var.0 /var
        (dump program output goes to stdout)
# /sbin/dump 0f /home/backups/laptop.hometnz.0 /home/tnz
        (dump program output goes to stdout)
```

[15] Passwords are chosen according to the guidelines given earlier in the document.

These are transferred to a machine that has nightly backups performed.

```
# cd /home/backups
# /usr/sbin/sftp tnz@backedupmachine.full.domain
tnz@backedupmachine.full.domain's password:
sftp> cd laptop.backups
sftp> put laptop.*
Uploading laptop.boot.0 …
Uploading laptop.hometnz.0 …
Uploading laptop.root.0 …
Uploading laptop.usr.0 …
Uploading laptop.var.0 …
sftp> quit
#
```

The backup routines are scripted. Incremental backups are done right after the laptop boots and once every day while the laptop is up and running. A mail message is sent to TNZ on the laptop with the dump output after each time the script runs as a reminder to transfer the files to backedupmachine.full.domain. The transfer is not automated.[16] The incremental backup script is shown in Appendix C. Monthly level 0 dumps are run from /etc/cron.monthly by a similar script.

MSEC

Mandrake Security Tools (msec) is a set of scripts to monitor different aspects of the system. The scripts are run on a predetermined basis according to the security level of the machine. This laptop is currently installed with a security level equivalent to 4.

The "security check" checks the following things: files belonging to packages that have been modified, configuration files belonging to packages that have been modified and network ports that are listening. The "diff check" checks for modifications to listening ports, changed packages (rpms), package files that have been modified and configuration files that have been modified. These checks are done against listings created during the initial installation phase.

By default these reports are run nightly with the results being e-mailed to TNZ. Following are the settings for a security level 4 machine:

CHECK_SHADOW=yes	check for empty passwords in /etc/shadow
CHECK_SUID_MD5=yes	verify MD5 checksum of suid/sgid files
CHECK_UNOWNED=yes	report unowned files
CHECK_SECURITY=yes	run daily security checks
CHECK_PASSWD=yes	check for empty passwords in /etc/passwd check for no passwords in /etc/shadow check for users with UID 0 (other than root)
SYSLOG_WARN=yes	report check results to syslog
CHECK_SUID_ROOT=yes	check additions/removals of suid root files
CHECK_PERMS=yes	check permissions of files in users' directory
MAIL_EMPTY_CONTENT=yes	

[16] The laptop is not always connected to the network. The reminder is sent to TNZ so that the files can be transferred if the connection is currently up.

CHECK_WRITABLE=yes	check for world-writable files/directories
CHKROOTKIT_CHECK=yes	check for rootkits
CHECK_PROMISC=yes	check for promiscuous network devices
CHECK_SGID=yes	check additions/removals of sgid root files
RPM_CHECK=yes	run checks against rpm database
TTY_WARN=yes	report check results to tty
MAIL_WARN=yes	report check results via mail
CHECK_OPEN_PORT=yes	check for open network ports

System defaults can be changed by editing files under /etc/security/msec. The perm.local file allows different permissions/owners/groups, the level.local file will override the default rules and the security.conf file will change the active security level. No options or defaults are changed for this machine. Samples of the mail messages from msec are available in Appendix D.

Logcheck

Logcheck is a program that extracts specified log entries and e-mails them to a designated recipient. Logcheck is not installed during the installation process and is manually installed following the previous instructions for NTP and dump.

The shell script /usr/bin/logcheck.sh runs once a day from /etc/cron.daily. The configuration files that determine which log entries get reported and which log entries are ignored live in /etc/logcheck. The hacking file contains a list of known active attack messages to look for. The violations file contains other patterns to look for. The ignore file lists attack messages to ignore and the violations.ignore file lists other patterns to not look for.

The /usr/sbin/logcheck.sh script is modified to send the output to TNZ (by default root is the recipient). The following pattern is added to /etc/logcheck/ignore and /etc/logcheck/violations.ignore:

```
Shorewall
```

to suppress the Shorewall firewall log messages of denied packets.

Daily Shorewall log messages are sent separately to TNZ. The logcheck files are copied to the /usr/local hierarchy for local modifications. The original logcheck script (/usr/bin/logcheck.sh.OEM) is copied to /usr/local/bin/logcheck.sh and the /etc/logcheck directory is copied to /usr/local/etc/logcheck. To make the log entries more readable at a glance, the /usr/local/bin/logcheck.sh file is modified to only extract certain fields of the Shorewall log messages. Fields extracted for TCP and UDP protocol messages are date, machine name, source address, destination address, protocol, source port and destination port. Fields extracted for ICMP protocol messages are date, machine, source address, destination address, source port, destination port and window size. The Subject of the mail message is easily filtered by procmail (Shorewall Messages). The only entry in /usr/local/etc/logcheck/violations is

```
kernel: Shorewall
```

and /usr/local/etc/logcheck/violations.ignore contains only

```
198.82.168.255
```

to discard broadcast messages. The differences between /usr/bin/logcheck.sh file and /usr/local/bin/logcheck.sh are in Appendix E.

Tripwire

Tripwire is a file integrity scanner. A list of files is checked against a database and the changes are flagged. The software is not installed during the initial installation phase; it is installed manually following the procedure documented previously for NTP, postfix and logcheck.

Tripwire is initially set up:

```
# /etc/tripwire/twinstall.sh
...
#
```

Good passwords that are relatively easy to remember but hard to guess are used for the local and site keys[17]. The database is initialized:

```
# /usr/sbin/tripwire --init
...
#
```

Tripwire looks for the files listed in /etc/tripwire/tw.pol (its policy file) and prints an error to standard output (in this case, the laptop screen) for every file it does not find. These are manually commented out from the text version of the policy file (/etc/tripwire/twpol.txt) then twadmin is used to recreate the compressed tw.pol file:

```
# /usr/sbin/twadmin --create-polfile twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
#
```

No changes are made to the configuration file twcfg.txt. The database is initialized again with the new policy file. The twpol.txt and twcfg.txt text files are removed. The plaintext copies of these files are a potential security risk. If an intruder can read the policy and configuration files they will know which files and directories are being monitored. These files can be regenerated using /usr/sbin/twadmin --print-polfile and /usr/sbin/twadmin --print-cfgfile, respectively. The modes of the /var/lib/tripwire and /var/lib/tripwire/report directories are changed to allow only root access:

```
# /bin/chmod 700 /var/lib/tripwire /var/lib/tripwire/report
#
```

By default, tripwire runs once per night from /etc/cron.daily with the results stored in /var/lib/tripwire/report. The results can be viewed using twprint to print the encrypted tripwire report:

```
# /usr/sbin/twprint --print-report -r /var/lib/tripwire/report/filename
#
```

where filename is similar to

```
laptop.full.domain-20031010-0120001.twr
```

Rather than hunt for the file name manually each day the /etc/cron.daily/tripwire-check shell script is modified to run the local shell script

[17] Passwords are chosen according to the guidelines given earlier in the document.

/usr/local/sbin/tripwire_monitor.sh. The local shell script e-mails the standard output of the tripwire check to TNZ. These files are listed in Appendix F, along with sample tripwire output.

Patch Administration

To keep abreast of updated rpm packages, a shell script is run from /etc/cron.daily. The shell script looks for updated rpms and mails the list to TNZ. The listing for /usr/local/sbin/update_check.sh is in Appendix G. It is TNZ's responsibility to check for updates every day. If /usr/local/sbin/update_check.sh generates a list, TNZ looks up the advisories on the MandrakeSecure[18] site to discover the reason for the patch or update. All security updates for this laptop are installed immediately upon notification. New kernels are installed if the present kernel has security vulnerabilities that are fixed in the newer version. Bug fix and normal updates are installed as soon as possible if vulnerabilities are involved.

CHECK CONFIGURATION

Access Passwords

The configuration is checked for proper password-protected access starting with the laptop turned off.

SYSTEM PRIMARY PASSWORD

The power button is pressed to start the laptop. Before the laptop will start the BIOS checking and boot process, the System Primary Password (hard-drive password) is required. A bogus password is entered, with the result:

> Invalid password
> [Press ENTER to retry]

Enter is pressed and the correct System Primary Password is entered. The system starts to boot.

GRUB PASSWORD

System checking is performed and the GRUB menu is displayed with the default kernel highlighted along with the following message:

> Use the up and down keys to select which entry is highlighted. Press enter to boot the selected OS or 'p' to enter a password to unlock the next set of features.

Pressing enter or doing nothing will allow the laptop to boot into multi-user mode. Pressing 'p' will ask for a password. This password is the one that was set in the "Set LILO/GRUB Password' section previously. 'p' is pressed and a bogus password is entered. The system responds with

> Failed!
> Press any key to continue

Any key is pressed and the default kernel is highlighted and the message is displayed again:

> Use the up and down keys to select which entry is highlighted. Press enter to boot the selected OS or 'p' to enter a password to unlock the next set of features.

[18] http://www.mandrakesecure.net/en/advisories/updates.php?dis=9.1

If no key is pressed the default kernel will boot.

The 'p' key is pressed and the correct password is entered. The screen is redrawn with the default kernel highlighted and this message is displayed:

> Use the up and down keys to select which entry is highlighted. Press enter to boot the selected OS, 'e' to edit the commands before booting, or 'c' for a command line.

'e' is entered to edit the commands. The default kernel with its default options is highlighted. The message is:

> Use the up and down arrow keys to select which entry is highlighted. Press 'b' to boot, 'e' to edit the selected command in the boot sequence, 'c' for a command-line, 'o' to open new line after ('0' for before) the selected line, 'd' to remove the selected line, or escape to go back to the main menu.

SINGLE USER MODE PASSWORD

'e' is entered again to edit the highlighted command (in this case the default kernel and its options). The edit function of grub begins. The line to be edited is shown as:

> grub edit> kernel (hd0,4)/vmlinuz-secure root=/dev/hda1 quiet acpi=off

and the cursor is at the end of the line. A space followed by the word "single" and the <enter> key is typed. The default kernel and options followed by the word single is highlighted and the same message as above is displayed. This time the 'b' key is entered to boot the laptop with the default kernel into single user mode. The laptop will boot to the point of entry to single user mode. The laptop displays:

> …
> Give root password for maintenance
> (or type Control-D for normal startup):

A bogus root password is entered and the laptop responds with:

> Login incorrect.
> Give root password for maintenance
> (or type Control-D for normal startup):

The root password is entered and the machine boots into single user mode.

ADMIN PASSWORD (BIOS SETUP)

BIOS setup mode is entered by the Fn/Setup key combination. None of the settings can be changed using the left or right arrow keys. The only way to change the settings is to go to Page 6 and enable Configure Setup (highlight the Configure Setup field, press the left or right arrow key, enter Admin Password). After BIOS setup changes are made, disable Configure Setup (highlight Configure Setup field and press the left or right arrow).

All of the access passwords are now tested and restrict access as they are supposed to.

File Permissions

File creation permissions are checked. As the regular user a file is created by touch filename and the permissions are checked:

> $ /bin/touch filename
> $ /bin/ls -ls filename

```
0 -rw-------  1  user  user         0   Oct 26 19:03 filename
$
```

An existing file created by the system is checked for permissions:

```
# ls -ls /var/tmp/patch-list
4 -rw-r--r--  1   root  root          103 Oct 26 19:03 /var/tmp/patch-list
#
```

The permissions on both created files are correct. The user-created file is readable and writable by only the owner; the system-created file is readable by everyone but only writable by root.

Removable Media File System Mounting

A cdrom is placed in the cd drive. It is not mounted automatically and the user cannot mount it:

```
$ /bin/mount /mnt/cdrom
mount: you must specify the filesystem type
$ /bin/mount -t iso9660 /dev/hdb /mnt/cdrom
mount: block device /dev/hdb is write-protected, mounting read-only
mount: cannot mount block device /dev/hdb read-only
$
```

Only root can successfully mount the cdrom:

```
# /bin/mount /mnt/cdrom
# /bin/mount
…
/dev/hdb on /mnt/cdrom type iso9660 (ro,nosuid,nodev,iocharset=iso8859-
1,codepage=850)
# /bin/umount /mnt/cdrom
#
```

A formatted floppy disk with a file system is inserted into the floppy drive. It is not mounted automatically and the user cannot mount it:

```
$ /bin/mount /mnt/floppy
mount: block device /dev/fd0 is write-protected, mounting read-only
mount: cannot mount block device /dev/fd0 read-only
$
```

Only root can successfully mount the floppy disk:

```
# /bin/mount /mnt/floppy
# /bin/mount
…
/dev/fd0 on /mnt/floppy type ext2 (rw,nosuid,nodev,sync,iocharset=iso8859-
1,codepage=850)
# /bin/umount /mnt/floppy
#
```

Regular users cannot mount removable file systems; only root can mount removable file systems.

SSH Configuration

SSH sessions are started from the laptop to remote machines. Without manually setting the display, windows are displayed on the laptop properly:

$ /usr/bin/ssh remote.full.domain
Authorized use only. All activity may be monitored or reported.
Password:
$ remote> /usr/X11/bin/xterm &
$ remote>
(xterm displays on laptop)

This is the correct behavior for .Xauthority permissions. However, attempts to manually set the display back to the laptop and display windows fail:

$ /usr/bin/ssh remote.full.domain
Authorized use only. All activity may be monitored or reported.
Password:
This is remote.full.domain. Unauthorized access or use is prohibited. All sessions may be monitored or recorded.
$ remote> DISPLAY=laptop.full.domain:0;export DISPLAY
$ remote> /usr/X11/bin/xterm &
$ remote> xterm Xt error: Can't open display: laptop.full.domain:0

The log file has entries for the failed xterm attempts:

…
Nov 1 09:53:28 local localhost kernel: Shorewall: net2all:DROP:IN=eth0 OUT= MAC=11:11:11:11:11:11:99:99:99:99:99:99:99:99 SRC=555.555.555.555 DST=222.222.222.222 LEN=44 TOS=0x00 PREC=0x00 TTL=63 ID=34096 DF PROTO=TCP SPT=1219 DPT=6000 WINDOW=57344 RES=0x00 SYN URGP=0
…

An ssh session is started from the laptop to a remote machine that the laptop has never connected to before. TNZ is forced to accept or deny the connection attempt:

$ /usr/bin/ssh remote.full.machine
The authenticity of host 'remote.full.domain (666.666.666.666)' can't be established.
DSA key fingerprint is 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'remote.full.domain,666.666.666.666' (DSA) to the list of known hosts.
Authorized access only. All activity is monitored and reported.
Password:
remote$

An ssh session is started from the laptop to a remote machine for which the key has changed. The connection is refused.

$ /usr/bin/ssh changedkey.full.domain
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man in the middle attack)!
It is also possible that the DSA host key has just been changed.
The fingerprint for the DSA key sent by the remote host is
73:e0:a5:40:9f:f4:c6:c7:d7:f9:73:0d:b3:69:63:30.

```
Please contact your system administrator.
Add correct host key in /tnz/.ssh/known_hosts to get rid of this message.
Offending key in /tnz/.ssh/known_hosts:1
DSA host key for changedkey.full.domain has changed and you have requested
strict checking.
Host key verification failed.
$
```

An ssh connection is attempted to a machine that only speaks Protocol 1 and does not understand Protocol 2. The connection is not made.

```
$ /usr/bin/ssh procotol1.full.domain
Protocol major versions differ: 2 vs. 1
$
```

SSH is configured properly for this laptop.

Shorewall

Shorewall is used to configure the Netfilter firewall. During the "Summary" part of the installation procedure, the firewall is configured to disallow all incoming network connections. Nmap is used to verify there are no connections allowed from remote machines. Nmap is run from a remote machine.
The first nmap scan is a simple TCP SYN scan of the reserved ports on the laptop:

```
# /usr/local/bin/nmap -v 222.222.222.222
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-17 08:11 EST
Host 222.222.222.222 appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.188 seconds
#
```

The second scan is the same as the previous one, but without using ping to determine if the laptop is up or down:

```
# /usr/local/bin/nmap -v -P0 222.222.222.222
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-17 08:18 EST
Host laptop.full.domain (222.222.222.222) appears to be up … good.
Initiating SYN Stealth Scan against laptop.full.domain (222.222.222.222) at 08:18
The SYN Stealth Scan took 107 seconds to scan 1657 ports.
Interesting ports on laptop.full.domain (222.222.222.222)
(The 1655 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
113/tcp   closed   auth
135/tcp   closed   msrpc
Nmap run completed -- 1 IP address (1 host up) scanned in 106.615 seconds
#
```

The third scan is a TCP SYN scan of all ports:

```
# /usr/local/bin/nmap -v -p0-65535 -P0 222.222.222.222
WARNING: Scanning "port 0" is supported, but unusual.

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-17 08:38 EST
Interesting ports on laptop.full.domain (222.222.222.222)
```

```
(The 65534 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
113/tcp   closed   auth
135/tcp   closed   msrpc
Nmap run completed -- 1 IP address (1 host up) scanned in 20213.102 seconds
#
```

The fourth scan is an attempt to identify the operating system running on the laptop:

```
# /usr/local/bin/nmap -v -P0 -O 222.222.222.222
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-17 11:20 EST
Host laptop.full.domain (222.222.222.222) appears to be up ... good.
Initiating SYN Stealth Scan against laptop.full.domain (222.222.222.222) at 11:20
The SYN Stealth Scan took 300 seconds to scan 1657 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least
1 open and 1 closed TCP port
Interesting ports on laptop.full.domain (222.222.222.222):
(The 1655 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
113/tcp   closed auth
135/tcp   closed msrpc
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.48%P=i386-unknown-freebsd4.8%D=12/17%Time=3FE08386%O=-1%C=113)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Nmap run completed -- 1 IP address (1 host up) scanned in 315.501 seconds
#
```

These same tests were run from two other remote machines, one on a different subnet and one from offsite with the same results. The showing of ports 113 and 135 as closed is normal. Port 113 “answers” to prevent outgoing connection problems with services that use the Auth mechanism and port 135 “answers” to cut down on unnecessary MSWindows chatter.

The firewall is doing its job by not allowing incoming connections. This is verified by the log messages from Shorewall during these nmap runs (only a few shown here for brevity):

```
Dec  1 09:53:22 local localhost kernel: Shorewall: net2all:DROP:IN=eth0 OUT=
MAC=11:11:11:11:11:11:99:99:99:99:99:99:99:99 SRC=555.555.555.555
DST=222.222.222.222 LEN=40 TOS=0x00 PREC=0x00 TTL=42 ID=60610
PROTO=TCP SPT=49634 DPT=20506 WINDOW=4096 RES=0x00 SYN URGP=0
Dec  1 09:53:28 local localhost kernel: Shorewall: net2all:DROP:IN=eth0 OUT=
MAC=11:11:11:11:11:11:99:99:99:99:99:99:99:99 SRC=555.555.555.555
DST=222.222.222.222 LEN=44 TOS=0x00 PREC=0x00 TTL=54 ID=64556
PROTO=TCP SPT=49633 DPT=12631 WINDOW=4096 RES=0x00 SYN URGP=0
```

File Restore

Backups are useless if they cannot be used to restore files. Restore is used to list each backup and then to do a test extraction. To generate a list of files in a dump:

```
# /bin/restore -tf /home/backups/laptop.hometnz.0
        (output to screen)
#
```

To extract all the files:

```
# /bin/restore -xf /home/backups/laptop.hometnz.0
        (output to screen)
```

To extract only select files:

```
# /bin/restore -xf /home/backups/laptop.hometnz.0 ./tnz/mbox ./tnz/.profile
        (output to screen)
#
```

Only one listing and test extraction is shown in Appendix H. The restored files are compared to existing files that have not been modified since the level 0 dump. Text files are compared both visually (i.e. using /bin/cat, /bin/more or an editor) and by listing (/bin/ls –ls) and comparing owner, size and modification date. Non-text files are compared by listing only.

APPENDIX A - XF86CONFIG

Anything after the # sign is treated as a comment. Comments may appear anywhere in the file, not just at the beginning of a line.

/etc/X11/XF86Config

```
# Specify which dynamically loadable modules to load
Section “Module”
Load “dbe”                      # double buffer extension
Load “type1”                    # type1 font module
Load “speedo”           # freetype font module
Subsection “extmod”     # load miscellaneous modules
                Option “omit xfree86-dga”       # do not initialize dga extension
EndSubsection
EndSection

# Set default font and rgb paths
Section “Files”
        RgbPath “/usr/X11R6/lib/X11/rgb”
        FontPath “/usr/X11R6/lib/X11/fonts/misc/”
        FontPath “/usr/X11R6/lib/X11/lfonts/75dpi/:unscaled”
        FontPath “/usr/X11R6/lib/X11/fonts/100dpi/:unscaled”
        FontPath “/usr/X11R6/lib/X11/fonts/Speedo/”
        FontPath “/usr/X11R6/lib/fonts/Type1/”
        FontPath “/usr/X11R6/lib/fonts/75dpi/”
        FontPath “/usr/X11R6/lib/fonts/100dpi/”
EndSection

# Set keyboard type and options
Section “InputDevice”
        Identifier “Keyboard1”
        Driver “Keyboard”
        Option “XkbModel” “pc101”
        Option “XkbLayout” “us”
        Option “AutoRepeat” “500 30”
        Option “XkbRules” “xfree86”
EndSection

# Set mouse type and options
Section “InputDevice”
        Identifier “Mouse1”
        Driver “mouse”
        Option “Protocol” “Auto”
        Option “Device” “/dev/mouse”
        Option “Emulate3Buttons”
EndSection
```

```
#Set monitor type and options
Section “Monitor”
        Identifier “My Monitor”
        HorizSync 31.5 - 82.0
        VertRefresh 40-150
EndSection

# Set graphics device and options
Section “Device”
        Identifier “** ATI Rage 128 based (generic)                [r128]”
        Driver “r128”
EndSection

# Set screen options
Section “Screen”
        Identifier “Screen1”
        Device “** ATI Rage 128 based (generic)          [r128]”
        Monitor “My Monitor”
        DefaultColorDepth 24
        Subsection “Display”
                Depth 24
                Modes “1280x1024” “1280x960” “1024x768” “800x600” “640x480”
        EndSubsection
        DefaultDepth 24
EndSection

# Set up of server layout.
Section “ServerLayout”
        Identifier “Simple Layout”
        InputDevice “Mouse1” “CorePointer”
        InputDevice “Keyboard1” “CoreKeyboard”
        Screen “Screen1”
EndSection
```

APPENDIX B - SYSLOG.CONF

This is the local configuration file for the syslog daemon. The local modifications are added at the end of the file.

/etc/syslog.conf:

```
# Log all auth messages
auth.*                                  /var/log/auth.log

# Log everything except auth and authpriv messages
*.*;auth,authpriv.none                  -/var/log/syslog

# Log all user messages
user.*                                  -/var/log/user.log

# Log anything except mail and authpriv of level info or higher
*.info;mail.none;authpriv.none     -/var/log/messages

# Log all authpriv
authpriv.*                              /var/log/secure

# Mail logging
mail.=debug;mail.=info;mail.=notice     -/var/log/mail/info
mail.=warn                              -/var/log/mail/warnings
mail.err                                -/var/log/mail/errors

# Cron logging
cron.=debug;cron.=info;cron.=notice     -/var/log/cron/info
cron.=warn                              -/var/log/cron/warnings
cron.err                                -/var/log/cron/errors

# Kernel logging
kern.=debug;kern.=info;kern.=notice     -/var/log/kernel/info
kern.=warn                              -/var/log/kernel/warnings
kern.err                                -/var/log/kernel/errors

# Daemon logging
daemon.=debug;daemon.=info;daemon.=notice  -/var/log/daemons/info
daemon.=warn                            -/var/log/daemons/warnings
daemon.err                              -/var/log/daemons/errors

# Save a separate copy of boot messages
local7.*                                -/var/log/boot.log

# Mandrake Linux configuration tools
local1.*                                -/var/log/explanations
```

```
# Local modifications
# Local syslog server
authpriv.*                      @syslog.full.domain
mail.notice                     @syslog.full.domain
cron.=warn                      @syslog.full.domain
kern.info                       @syslog.full.domain
daemon.info                     @syslog.full.domain
```

APPENDIX C - BACKUP SCRIPT

/usr/local/sbin/routine_backup.sh

```
#!/bin/sh
# Simple incremental backup script.  Run at boot from /etc/rc.local and daily from /etc/cron.daily.
# File systems and directories: /, /boot, /var, /usr, /home/tnz
# Dump files written to /home/backups, output mailed to administrator upon finish

# Temporary file directory location: /var/tmp
TMPDIR=/var/tmp

# no static filename
suffix=`date +"%Y%m%d.%H%M%S"`

# temporary mail file
msgfile=${TMPDIR}backup${suffix}

# create mail headers
echo "From: TNZ <tnz@laptop.full.domain>" > $msgfile
echo "To: tnz" >> $msgfile
echo "Subject: Incremental laptop backup results" >> $msgfile
echo "" >> $msgfile

# backups
for directory in / /boot /var /usr /home/tnz
do
        if [ $directory = "/" \ ; then
                name=root
                options=9uf
        elif [ $directory = "/home/tnz" ] ; then
                name='echo $directory | sed 's/\//g'`
                options=9f
        else
                name='echo $directory | sed 's/\//g'`
                options=9uf
        fi
        /sbin/dump $options /home/backups/laptop.${name}.9  $directory >> $msgfile 2>&1
done

# send message
/usr/lib/sendmail -oi -t < $msgfile

# remove temporary mail file
sleep 1
rm -f $msgfile
exit 0
```

APPENDIX D - MSEC OUTPUT

This is a sample of the mail messages from MSEC that are sent to TNZ. These reports are sent once a day.

From root@laptop.full.domain
To: tnz@laptop.full.domain
Subject: [msec] *** Diff Check on laptop.full.domain, Date/Time/Year ***

Security Warning: Change in World Writable Files found :
- Newly added writable file : /tmp/.ICE-unix/dcop10057-1071082513

Security Warning: There are modifications for port listening on your machine :
- Opened ports : tcp 0 0 localhost:smtp *:* LISTEN 28560/master
- Opened ports : udp 0 0 *:syslog *:* 3076/syslogd
- Opened ports : udp 0 0 *:bootpc *:* 17755/dhclient
- Opened ports : udp 0 0 laptop.full.domain:ntp *:* 31495/ntpd
- Opened ports : udp 0 0 localhost:ntp *:* 31495/ntpd
- Opened ports : udp 0 0 *:ntp *:* 31495/ntpd
- Closed ports : tcp 0 0 localhost:smtp *:* LISTEN 2554/master
- Closed ports : udp 0 0 *:bootpc *:* 1160/dhclient

Security Warning: These packages have changed on the system :
- Newly installed package : ntp-4.1.1-2mdk 1071071321
- No longer present package : harddrake-9.1-31.3mdk 1070987237

Security Warning: These config files belonging to packages have changed of status on the system:
- Newly modified : /etc/motd
- Newly modified : /etc/ntp.conf
- Newly modified : /etc/security/console.perms

From root@laptop.full.domain
To: tnz@laptop.full.domain
Subject: [msec] *** Security Check on laptop.full.domain, Date/Time/Year ***

Security Warning: World Writable files found :
- /tmp/.ICE-unix
- /tmp/.ICE-unix/dcop10057-1071082513
- /tmp/.X11-unix
- /tmp/.X11-unix/X0
- /tmp/.font-unix
- /tmp/.font-unix/fs-1
- /var/spool/postfix/private/bounce
- /var/spool/postfix/private/bsmtp
- /var/spool/postfix/private/cyrus
- /var/spool/postfix/private/defer

- /var/spool/postfix/private/error
- /var/spool/postfix/private/ifmail
- /var/spool/postfix/private/lmtp
- /var/spool/postfix/private/local
- /var/spool/postfix/private/maildrop
- /var/spool/postfix/private/old-cyrus
- /var/spool/postfix/private/proxymap
- /var/spool/postfix/private/relay
- /var/spool/postfix/private/rewrite
- /var/spool/postfix/private/smtp
- /var/spool/postfix/private/uucp
- /var/spool/postfix/private/virtual
- /var/spool/postfix/public/cleanup
- /var/spool/postfix/public/flush
- /var/spool/postfix/public/pickup
- /var/spool/postfix/public/qmgr
- /var/spool/postfix/public/showq

Security Warning: These files belonging to packages are modified on the system :

- /boot/grub/stage2
- /boot/message-graphic
- /usr/X11R6/lib/X11/fonts/TTF/fonts.cache-1
- /usr/X11R6/lib/X11/fonts/Type1/fonts.cache-1
- /usr/X11R6/lib/X11/icewm/menu
- /usr/X11R6/lib/X11/icewm/preferences

Security Warning: These config files belonging to packages are modified on the system :

- /etc/X11/fs/config
- /etc/X11/xdm/Xservers
- /etc/host.conf
- /etc/hosts.deny
- /etc/info-dir
- /etc/inittab
- /etc/login.defs
- /etc/modules.conf
- /etc/motd
- /etc/mtools.conf
- /etc/ntp.conf
- /etc/pam.d/system-auth
- /etc/pam.d/xdm
- /etc/securetty
- /etc/security/console.perms
- /etc/shells
- /etc/shorewall/interfaces
- /etc/shorewall/policy
- /etc/shorewall/zones
- /etc/ssh/ssh_config

- /etc/sysconfig/msec
- /etc/sysconfig/pcmcia
- /etc/sysctl.conf
- /etc/syslog.conf
- /etc/xinetd.d/fam
- /etc/xml/catalog
- /usr/share/config/kdeglobals
- /usr/share/config/kdesktoprc
- /usr/share/config/kdm/kdmrc
- /usr/share/config/konquerorrc
- /usr/share/sgml/docbook/xmlcatalog

These are the ports listening on your machine :
Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	localhost:smtp	*:*	LISTEN	28560/master
udp	0	0	*:syslog	*:*		3076/syslogd
udp	0	0	*:bootpc	*:*		17755/dhclient
udp	0	0	machine.full.dom:ntp	*:*		31495/ntpd
udp	0	0	localhost:ntp	*:*		31495/ntpd
udp	0	0	*:ntp	*:*		31495/ntpd

APPENDIX E - LOGCHECK CHANGES

This is the output from “diff” to show the local modifications made to /usr/local/bin/logcheck.sh to only check for Shorewall syslog entries. The logcheck.sh file is the modified file; the logcheck.sh.OEM file is the original.

```
# diff /usr/bin/logcheck.sh.OEM /usr/local/bin/logcheck.sh
2a3,4
> # Locally modified for Shorewall messages
> #
42c44
< SYSADMIN=root
---
> SYSADMIN=tnz
55c57
< TMPDIR=/var/lib/logcheck
---
> TMPDIR=/var/lib/local_logcheck
92c94
< HACKING_FILE=/etc/logcheck/hacking
---
> HACKING_FILE=/usr/local/etc/logcheck/hacking
101c103
< VIOLATIONS_FILE=/etc/logcheck/violations
---
> VIOLATIONS_FILE=/usr/local/etc/logcheck/violations
118c120
< VIOLATIONS_IGNORE_FILE=/etc/logcheck/violations.ignore
---
> VIOLATIONS_IGNORE_FILE=/usr/local/etc/logcheck/violations.ignore
125c127
< IGNORE_FILE=/etc/logcheck/ignore
---
> IGNORE_FILE=/usr/local/etc/logcheck/ignore
169,174c171,177
< $LOGTAIL /var/log/messages > $TMPDIR/check.$$
< $LOGTAIL /var/log/secure >> $TMPDIR/check.$$
< $LOGTAIL /var/log/mail/info >> $TMPDIR/check.$$
< $LOGTAIL /var/log/mail/warnings >> $TMPDIR/check.$$
< $LOGTAIL /var/log/news/info >> $TMPDIR/check.$$
< $LOGTAIL /var/log/news/warnings >> $TMPDIR/check.$$
---
> $LOGTAIL /var/log/syslog > $TMPDIR/check.$$
> # $LOGTAIL /var/log/messages > $TMPDIR/check.$$
> # $LOGTAIL /var/log/secure >> $TMPDIR/check.$$
> # $LOGTAIL /var/log/mail/info >> $TMPDIR/check.$$
> # $LOGTAIL /var/log/mail/warnings >> $TMPDIR/check.$$
```

```
> # $LOGTAIL /var/log/news/info >> $TMPDIR/check.$$
> # $LOGTAIL /var/log/news/warnings >> $TMPDIR/check.$$
232,241c235,244
< if [ -f "$HACKING_FILE" ]; then
<         if $GREP -i -f $HACKING_FILE $TMPDIR/check.$$ > $TMPDIR/checkoutput.$$; then
<                 echo >> $TMPDIR/checkreport.$$
<                 echo "Active System Attack Alerts" >> $TMPDIR/checkreport.$$
<                 echo "=-=-=-=-=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
<                 cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
<                 FOUND=1
<                 ATTACK=1
<         fi
< fi
---
> # if [ -f "$HACKING_FILE" ]; then
> #       if $GREP -i -f $HACKING_FILE $TMPDIR/check.$$ > $TMPDIR/checkoutput.$$; then
> #               echo >> $TMPDIR/checkreport.$$
> #             echo "Active System Attack Alerts" >> $TMPDIR/checkreport.$$
> #             echo "=-=-=-=-=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
> #               cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
> #               FOUND=1
> #               ATTACK=1
> #       fi
> # fi
245,252c248,255
<         if $GREP -i -f $VIOLATIONS_FILE $TMPDIR/check.$$ |
<           $GREP -v -f $VIOLATIONS_IGNORE_FILE > $TMPDIR/checkoutput.$$; then
<                 echo >> $TMPDIR/checkreport.$$
<                 echo "Security Violations" >> $TMPDIR/checkreport.$$
<                 echo "=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
<                 cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
<                 FOUND=1
<         fi
---
>         if $GREP -i -f $VIOLATIONS_FILE $TMPDIR/check.$$ |
>           $GREP -v -f $VIOLATIONS_IGNORE_FILE > $TMPDIR/checkoutput.$$; then
>                 echo >> $TMPDIR/checkreport.$$
>                 # echo "Unusual System Events" >> $TMPDIR/checkreport.$$
>             # echo "=-=-=-=-=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
>                 cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
>                 FOUND=1
>         fi
256,264c259,267
< if [ -f "$IGNORE_FILE" ]; then
<         if $GREP -v -f $IGNORE_FILE $TMPDIR/check.$$ > $TMPDIR/checkoutput.$$; then
<                 echo >> $TMPDIR/checkreport.$$
<                 echo "Unusual System Events" >> $TMPDIR/checkreport.$$
```

```
<                       echo "=-=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
<                       cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
<                       FOUND=1
<               fi
< fi
---
> # if [ -f "$IGNORE_FILE" ]; then
> #       if $GREP -v -f $IGNORE_FILE $TMPDIR/check.$$ > $TMPDIR/checkoutput.$$; then
> #               echo >> $TMPDIR/checkreport.$$
> #               echo "Unusual System Events" >> $TMPDIR/checkreport.$$
> #               echo "=-=-=-=-=-=-=-=-=-=-=" >> $TMPDIR/checkreport.$$
> #               cat $TMPDIR/checkoutput.$$ >> $TMPDIR/checkreport.$$
> #               FOUND=1
> #       fi
> # fi
269c272,273
<               cat $TMPDIR/checkreport.$$ | $MAIL -s "$HOSTNAME $DATE ACTIVE SYSTEM
ATTACK!" $SYSADMIN
---
> #       cat $TMPDIR/checkreport.$$ | $MAIL -s "$HOSTNAME $DATE ACTIVE SYSTEM
ATTACK!" $SYSADMIN
>               cat $TMPDIR/checkreport.$$ | /usr/bin/awk ' { print $1, $2, $3, $9, $10, $16, $17, $18, $19
} '| $MAIL -s "Shorewall Messages" $SYSADMIN
271c275,276
<               cat $TMPDIR/checkreport.$$ | $MAIL -s "$HOSTNAME $DATE system check"
$SYSADMIN
---
> #       cat $TMPDIR/checkreport.$$ | $MAIL -s "$HOSTNAME $DATE system check"
$SYSADMIN
>               cat $TMPDIR/checkreport.$$ | /usr/bin/awk ' { print $1, $2, $3, $9, $10, $16, $17, $18, $19
} '| $MAIL -s "Shorewall Messages" $SYSADMIN
```

APPENDIX F - TRIPWIRE

/etc/cron.daily/tripwire-check

```
#!/bin/sh
HOST_NAME=`uname -n`
if [ -e /var/lib/tripwire/${HOST_NAME}.twd ] ; then
        echo "****    Error: Tripwire database for ${HOST_NAME} not found.    ****"
        echo "****    Run "/etc/tripwire/twinstall.sh" and/or "tripwire --init".    ****"
else
        test -f /etc/tripwire/tw.cfg && /bin/sh /usr/local/sbin/tripwire_monitor.sh
fi
```

/usr/local/sbin/tripwire_monitor.sh

```
#!/bin/sh
DESTDIR=/var/tmp
suffix=`date +"%Y%m%d.%H%M%S"`
msgfile=${DESTDIR}/tripwire-message.${suffix}
echo "From: TNZ <tnz@laptop.full.domain>" > $msgfile
echo "To: tnz" >> $msgfile
echo "Subject: Tripwire output" >> $msgfile
echo >> $msgfile
/usr/sbin/tripwire -m -c >> $msgfile 2>&1
/usr/sbin/sendmail -oi -t < &msgfile
sleep 1
rm -f $msgfile
exit0
```

Sample output from /usr/local/sbin/tripwire_monitor.sh

```
From tnz@laptop.full.domain  Thu Dec  3 09:22:05 2003
To: tnz@laptop.full.domain

Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
### Warning: File system error.
### Filename: /etc/tripwire/localhost-local.key
### No such file or directory
### Continuing...
Wrote report file: /var/lib/tripwire/report/laptop.full.domain-20031203-092043.twr


Tripwire(R) 2.3.0 Integrity Check Report
```

Report generated by: root
Report created on: Thu 03 Dec 2003 09:20:43 AM EST
Database last updated on: Never

==========
Report Summary:
==========

Host name: laptop.full.domain
Host IP address: 222.222.222.222
Host ID: None
Policy file used: /etc/tripwire/tw.pol
Configuration file used: /etc/tripwire/tw.cfg
Database file used: /var/lib/tripwire/laptop.full.domain.twd
Command line used: /usr/sbin/tripwire -m c

==========
Rule Summary:
==========

Section: Unix File System

Rule Name	Severity	Level	Added	Removed	Modified
Invariant Directories	66	0	0	0	
Temporary directories	33	0	0	0	
* Tripwire Data Files	100	1	0	1	
Critical devices	100	0	0	0	
User binaries	66	0	0	0	
Tripwire Binaries	100	0	0	0	
Libraries	66	0	0	0	
Operating System Utilities	100	0	0	0	
File System and Disk Administraton Programs	100	0	0	0	
Kernel Administration Programs	100	0	0	0	
Networking Programs	100	0	0	0	
System Administration Programs	100	0	0	0	
Hardware and Device Control Programs	100	0	0	0	
System Information Programs		0	0	0	
Application Information Programs	100	0	0	0	
Shell Related Programs	100	0	0	0	
Critical Utility Sym-Links	100	0	0	0	
Shell Binaries	100	0	0	0	
* Critical system boot files	100	0	0	5	
* System boot changes	100	28	1	56	
OS executables and libraries	100	0	0	0	
* Critical configuration files	100	2	0	3	

Security Control	100	0	0	0
Login Scripts	100	0	0	0
* Root config files	100	2	2	5

Total objects scanned: 17614
Total violations found: 106

==========
Object Summary:
==========

Section: Unix File System

Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100

Added:
"/var/lib/tripwire/laptop.full.domain.twd.bak"

Rule Name: System boot changes (/var/log)
Severity Level: 100

Added:
"/var/log/mail/errors.1.gz"
"/var/log/mail/info.1.gz"
"/var/log/mail/warnings.1.gz"
"/var/log/lpr/errors.1.gz"
"/var/log/lpr/info.1.gz"
"/var/log/lpr/warnings.1.gz"
"/var/log/kernel/errors.1.gz"
"/var/log/kernel/info.1.gz"
"/var/log/kernel/warnings.1.gz"
"/var/log/cron/errors.1.gz"
"/var/log/cron/info.1.gz"
"/var/log/cron/warnings.1.gz"
"/var/log/news/news.err.1.gz"
"/var/log/news/news.crit.1.gz"
"/var/log/news/news.notice.1.gz"
"/var/log/daemons/errors.1.gz"
"/var/log/daemons/info.1.gz"
"/var/log/daemons/warnings.1.gz"
"/var/log/rpmpkgs.1.gz"
"/var/log/auth.log.1.gz"
"/var/log/syslog.1.gz"
"/var/log/user.log.1.gz"

"/var/log/secure.1.gz"
"/var/log/messages.1.gz"
"/var/log/boot.log.1.gz"
"/var/log/urpmi.log.1.gz"
"/var/log/explanations.1.gz"

Modified:
"/var/log/auth.log"
"/var/log/boot.log"
"/var/log/cron/errors"
"/var/log/cron/info"
"/var/log/cron/warnings"
"/var/log/daemons/errors"
"/var/log/daemons/info"
"/var/log/daemons/warnings"
"/var/log/explanations"
"/var/log/kernel/errors"
"/var/log/kernel/info"
"/var/log/kernel/warnings"
"/var/log/ksyms.0"
"/var/log/ksyms.1"
"/var/log/ksyms.2"
"/var/log/ksyms.3"
"/var/log/ksyms.4"
"/var/log/ksyms.5"
"/var/log/ksyms.6"
"/var/log/lpr/errors"
"/var/log/lpr/info"
"/var/log/lpr/warnings"
"/var/log/mail/errors"
"/var/log/mail/info"
"/var/log/mail/warnings"
"/var/log/messages"
"/var/log/news/news.crit"
"/var/log/news/news.err"
"/var/log/news/news.notice"
"/var/log/rpmpkgs"
"/var/log/secure"
"/var/log/security/open_port.today"
"/var/log/security/open_port.yesterday"
"/var/log/security/rpm-qa.today"
"/var/log/security/rpm-qa.yesterday"
"/var/log/security/rpm-va-config.today"
"/var/log/security/rpm-va-config.yesterday"
"/var/log/security/rpm-va.today"
"/var/log/security/rpm-va.yesterday"
"/var/log/security/sgid.today"
"/var/log/security/sgid.yesterday"
"/var/log/security/suid_md5.today"
"/var/log/security/suid_md5.yesterday"
"/var/log/security/suid_root.today"

"/var/log/security/suid_root.yesterday"
"/var/log/security/unowned_group.today"
"/var/log/security/unowned_group.yesterday"
"/var/log/security/unowned_user.today"
"/var/log/security/unowned_user.yesterday"
"/var/log/security/writable.today"
"/var/log/security/writable.yesterday"
"/var/log/syslog"
"/var/log/urpmi.log"
"/var/log/user.log"

Rule Name: System boot changes (/var/run)
Severity Level: 100

Added:
"/var/run/xauth/A:0-hlquJF"

Removed:
"/var/run/xauth/A:0-FfeYTy"

Modified:
"/var/run/console.lock"

Rule Name: Tripwire Data Files (/etc/tripwire/tw.pol)
Severity Level: 100

Modified:
"/etc/tripwire/tw.pol"

Rule Name: Critical configuration files (/etc/cron.daily)
Severity Level: 100

Added:
"/etc/cron.daily/shorewall_check.sh"

Modified:
"/etc/cron.daily"

Rule Name: Critical configuration files (/etc/cron.monthly)
Severity Level: 100

Added:
"/etc/cron.monthly/level0_backup.sh"

Modified:
"/etc/cron.monthly"

Rule Name: Critical configuration files (/etc/rc.d/init.d)
Severity Level: 100

Modified:
"/etc/rc.d/init.d"

Rule Name: Critical system boot files (/boot)
Severity Level: 100

Modified:
"/boot"
"/boot/config"
"/boot/grub"
"/boot/grub/menu.lst"
"/boot/kernel.h"

Rule Name: System boot changes (/dev/log)
Severity Level: 100

Modified:
"/dev/log"

Rule Name: Root config files (/root)
Severity Level: 100

Added:
"/root/.xauth1AiF7T"
"/root/mbox"

Removed:
"/root/.xauth35uOdj"
"/root/.xauthVVKV9m"

Modified:
"/root"
"/root/.fonts.cache-1"
"/root/.rpmdrake"
"/root/.viminfo"
"/root/tmp"

```
================================================================================
Error Report:
================================================================================

--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

1.   File system error.
     Filename: /etc/tripwire/localhost-local.key
     No such file or directory

--------------------------------------------------------------------------------
*** End of report ***

Tripwire 2.3 Portions copyright 2000 Tripwire, Inc. Tripwire is a registered
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;
for details use --version. This is free software which may be redistributed
or modified only under certain conditions; see COPYING for details.
All rights reserved.
Integrity check complete.
```

APPENDIX G - CHECK FOR UPDATES

/usr/local/sbin/update_check.sh

```
#!/bin/sh
DESTDIR=/var/tmp
suffix=`date +"%Y%m%d.%H%M%S"`
msgfile=${DESTDIR}patch-list${suffix}
echo "From: TNZ <tnz@laptop.full.domain>" > $msgfile
echo "To: tnz@laptop.full.domain" >> $msgfile
echo "Subject: Mandrake update check" >>& msgfile
echo >> $msgfile
/usr/sbin/urpmi.update update_source >> /dev/null 2>&1
/usr/bin/urpmq --auto-select >>$msgfile 2>&1
/usr/lib/sendmail -oi -t <$msgfile
sleep 1
rm $msgfile
exit 0
```

Sample output from /usr/local/sbin/update_check.sh.

```
From tnz@laptop.full.domain  Thu Dec 18 09:35:35 2003
To: tnz@laptop.full.domain
Subject: Mandrake update check

XFree86
coreutils
glibc
gnupg
lftp
rsync
screen
```

APPENDIX H - RESTORE

List the contents of the backup media:

```
# /sbin/restore tf /home/backups/laptop.hometnz.0
Dump   date: Fri Dec 12 13:17:45 2003
Dumped from: the epoch
Level 0 dump of /home (dir /tnz) on laptop.full.domain:/dev/hda7
Label: none
        2       .
    32385       ./tnz
    64769       ./tnz/tmp
    32386       ./tnz/.screenrc
    32387       ./tnz/.bash_logout
    32388       ./tnz/.bash_profile
    32389       ./tnz/.bashrc
    32390       ./tnz/.mailcap
    32391       ./tnz/.bash_history
    32392       ./tnz/.wmrc
    32394       ./tnz/.xsession-errors
    32395       ./tnz/.drakfw
    97153       ./tnz/.kde
   129537       ./tnz/.kde/share
   161921       ./tnz/.kde/share/config
   161930       ./tnz/.kde/share/config/kdeglobals
   161934       ./tnz/.kde/share/config/kwinrc
   161937       ./tnz/.kde/share/config/knewstickerappletrc
   161925       ./tnz/.kde/share/config/kcookiejarrc
   161940       ./tnz/.kde/share/config/kdeprintrc
   161928       ./tnz/.kde/share/config/kio_httprc
   161922       ./tnz/.kde/share/config/kioslaverc
   161927       ./tnz/.kde/share/config/kcmdisplayrc
   161929       ./tnz/.kde/share/config/dummy
   161945       ./tnz/.kde/share/config/ksmserverrc
   161947       ./tnz/.kde/share/config/konsolerc
   161926       ./tnz/.kde/share/config/kickerrc
   161932       ./tnz/.kde/share/config/klipperrc
   161923       ./tnz/.kde/share/config/kmailrc
   161933       ./tnz/.kde/share/config/kpgprc
   161936       ./tnz/.kde/share/config/kmail.eventsrc
   178114       ./tnz/.kde/share/config/session
   178117
        ./tnz/.kde/share/config/session/konsole_117f000001000107098601500000151140010_10
71082441_426022
   178118
        ./tnz/.kde/share/config/session/kwin_117f000001000107098598700000151140000_10710
82441_469101
```

161942 ./tnz/.kde/share/config/kcminitrc
161938 ./tnz/.kde/share/config/knewsticker_appletrc
161939 ./tnz/.kde/share/config/noatunrc
161935 ./tnz/.kde/share/config/kconf_updaterc
161946 ./tnz/.kde/share/config/mandrakegalaxyrc
161943 ./tnz/.kde/share/config/kcmnspluginrc
161944 ./tnz/.kde/share/config/kdesktoprc
161941 ./tnz/.kde/share/config/kab2kabcrc
161924 ./tnz/.kde/share/config/kalarmdrc
242881 ./tnz/.kde/share/apps
259073 ./tnz/.kde/share/apps/konqueror
259074 ./tnz/.kde/share/apps/konqueror/bookmarks.xml
16193 ./tnz/.kde/share/apps/nsplugins
16194 ./tnz/.kde/share/apps/nsplugins/cache
16195 ./tnz/.kde/share/apps/nsplugins/pluginsinfo
97157 ./tnz/.kde/share/apps/kabc
178115 ./tnz/.kde/share/apps/kabc/lock
97158 ./tnz/.kde/share/apps/kabc/std.vcf
113345 ./tnz/.kde/share/apps/kmail
145729 ./tnz/.kde/share/apps/kab
226692 ./tnz/.kde/share/apps/kalarmd
275270 ./tnz/.kde/share/apps/kfile
291457 ./tnz/.kde/share/servicetypes
64770 ./tnz/.kde/share/mimelnk
97156 ./tnz/.kde/share/applnk-mdk
194307 ./tnz/.kde/share/applnk-mdk/Terminals
242883 ./tnz/.kde/share/applnk-mdk/Networking
97159 ./tnz/.kde/share/applnk-mdk/Networking/WWW
113346 ./tnz/.kde/share/applnk-mdk/Networking/Mail
129540 ./tnz/.kde/share/applnk-mdk/.hidden
145730 ./tnz/.kde/share/applnk-mdk/Configuration
178116 ./tnz/.kde/share/applnk-mdk/Applications
194308 ./tnz/.kde/share/applnk-mdk/Applications/Editors
242884 ./tnz/.kde/share/applnk-mdk/Office
291460 ./tnz/.kde/share/applnk-mdk/Documentation
129538 ./tnz/.kde/share/services
129539 ./tnz/.kde/share/services/nsplugin.desktop
242882 ./tnz/.kde/share/fonts
291458 ./tnz/.kde/share/fonts/override
291459 ./tnz/.kde/share/fonts/override/fonts.dir
242885 ./tnz/.kde/share/fonts/fonts.dir
226689 ./tnz/.kde/Autostart
226691 ./tnz/.kde/Autostart/.directory
97154 ./tnz/.kde/tmp-localhost
97155 ./tnz/.kde/socket-localhost
97160 ./tnz/.kde/socket-hc652a895.dhcp.vt.edu
97161 ./tnz/.kde/tmp-hc652a895.dhcp.vt.edu

```
 32397	./tnz/.Xauthority
 32396	./tnz/.gtkrc
 32398	./tnz/.gtkrc-2.0
178113	./tnz/Documents
 32407	./tnz/.fonts.cache-1
194305	./tnz/.gnome2
194306	./tnz/.gnome2/gdm
 32399	./tnz/.desktop
210497	./tnz/Desktop
210498	./tnz/Desktop/.ArrangeIcons
210499	./tnz/Desktop/Welcome.desktop
210500	./tnz/Desktop/.directory-mdkgalaxy
210501	./tnz/Desktop/Home.desktop
210502	./tnz/Desktop/.home
210503	./tnz/Desktop/.directory
 80961	./tnz/Desktop/Trash
 80962	./tnz/Desktop/Trash/.directory
275265	./tnz/.qt
275266	./tnz/.qt/.qt_plugins_3.1rc.lock
275267	./tnz/.qt/qt_plugins_3.1rc
275268	./tnz/.qt/.qtrc.lock
275269	./tnz/.qt/qtrc
 32393	./tnz/.DCOPserver_hc652a895.dhcp.vt.edu__0
226690	./tnz/.ssh
226693	./tnz/.ssh/known_hosts
 32402	./tnz/.gtkrc-kde
 32401	./tnz/mbox
 32400	./tnz/.mcoprc
 32406	./tnz/.ICEauthority
 32403	./tnz/.DCOPserver_hc652a895.dhcp.vt.edu_:0
```

Extract all files from the dump media

```
# /bin/mkdir /home/RESTORE
# cd /home/RESTORE
# /sbin/restore xvf /home/backups/laptop.hometnz.0
Verify tape and initialize maps
Input is from file/pipe
Input block size is 32
Dump   date: Fri Dec 12 13:17:45 2003
Dumped from: the epoch
Level 0 dump of /home (dir /tnz) on laptop.full.domain:/dev/hda7
Label: none
Extract directories from tape
Initialize symbol table.
/sbin/restore: ./tnz: File exists
/sbin/restore: ./tnz/tmp: File exists
/sbin/restore: ./tnz/.kde: File exists
```

```
/sbin/restore: ./tnz/.kde/share: File exists
/sbin/restore: ./tnz/.kde/share/config: File exists
/sbin/restore: ./tnz/.kde/share/config/session: File exists
/sbin/restore: ./tnz/.kde/share/apps: File exists
/sbin/restore: ./tnz/.kde/share/apps/konqueror: File exists
/sbin/restore: ./tnz/.kde/share/apps/nsplugins: File exists
/sbin/restore: ./tnz/.kde/share/apps/kabc: File exists
/sbin/restore: ./tnz/.kde/share/apps/kabc/lock: File exists
/sbin/restore: ./tnz/.kde/share/apps/kmail: File exists
/sbin/restore: ./tnz/.kde/share/apps/kab: File exists
/sbin/restore: ./tnz/.kde/share/apps/kalarmd: File exists
/sbin/restore: ./tnz/.kde/share/apps/kfile: File exists
/sbin/restore: ./tnz/.kde/share/servicetypes: File exists
/sbin/restore: ./tnz/.kde/share/mimelnk: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Terminals: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Networking: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Networking/WWW: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Networking/Mail: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/.hidden: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Configuration: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Applications: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Applications/Editors: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Office: File exists
/sbin/restore: ./tnz/.kde/share/applnk-mdk/Documentation: File exists
/sbin/restore: ./tnz/.kde/share/services: File exists
/sbin/restore: ./tnz/.kde/share/fonts: File exists
/sbin/restore: ./tnz/.kde/share/fonts/override: File exists
/sbin/restore: ./tnz/.kde/Autostart: File exists
/sbin/restore: ./tnz/Documents: File exists
/sbin/restore: ./tnz/.gnome2: File exists
/sbin/restore: ./tnz/Desktop: File exists
/sbin/restore: ./tnz/Desktop/Trash: File exists
/sbin/restore: ./tnz/.qt: File exists
/sbin/restore: ./tnz/.ssh: File exists
Extract requested files
You have not read any volumes yet.
Unless you know which volume your file(s) are on you should start
with the last volume and work towards the first.
Specify next volume # (none if no more volumes): 1
extract file ./tnz/.kde/share/apps/nsplugins/cache
extract file ./tnz/.kde/share/apps/nsplugins/pluginsinfo
extract file ./tnz/.screenrc
extract file ./tnz/.bash_logout
extract file ./tnz/.bash_profile
extract file ./tnz/.bashrc
extract file ./tnz/.mailcap
```

```
extract file ./tnz/.bash_history
extract file ./tnz/.wmrc
extract file ./tnz/.DCOPserver_hc652a895.dhcp.vt.edu__0
extract file ./tnz/.xsession-errors
extract file ./tnz/.drakfw
extract file ./tnz/.gtkrc
extract file ./tnz/.Xauthority
extract file ./tnz/.gtkrc-2.0
extract file ./tnz/.desktop
extract file ./tnz/.mcoprc
extract file ./tnz/mbox
extract file ./tnz/.gtkrc-kde
Create symbolic link ./tnz/.DCOPserver_hc652a895.dhcp.vt.edu_:0-
>/home/lat/.DCOPserver_hc652a895.dhcp.vt.edu__0
extract file ./tnz/.ICEauthority
extract file ./tnz/.fonts.cache-1
extract file ./tnz/Desktop/Trash/.directory
Create symbolic link ./tnz/.kde/tmp-localhost->/tmp/kde-lat
Create symbolic link ./tnz/.kde/socket-localhost->/tmp/ksocket-lat
extract file ./tnz/.kde/share/apps/kabc/std.vcf
Create symbolic link ./tnz/.kde/socket-hc652a895.dhcp.vt.edu->/tmp/ksocket-lat
Create symbolic link ./tnz/.kde/tmp-hc652a895.dhcp.vt.edu->/tmp/kde-lat
extract file ./tnz/.kde/share/services/nsplugin.desktop
extract file ./tnz/.kde/share/config/kioslaverc
extract file ./tnz/.kde/share/config/kmailrc
extract file ./tnz/.kde/share/config/kalarmdrc
extract file ./tnz/.kde/share/config/kcookiejarrc
extract file ./tnz/.kde/share/config/kickerrc
extract file ./tnz/.kde/share/config/kcmdisplayrc
extract file ./tnz/.kde/share/config/kio_httprc
extract file ./tnz/.kde/share/config/dummy
extract file ./tnz/.kde/share/config/kdeglobals
extract file ./tnz/.kde/share/config/klipperrc
extract file ./tnz/.kde/share/config/kpgprc
extract file ./tnz/.kde/share/config/kwinrc
extract file ./tnz/.kde/share/config/kconf_updaterc
extract file ./tnz/.kde/share/config/kmail.eventsrc
extract file ./tnz/.kde/share/config/knewstickerappletrc
extract file ./tnz/.kde/share/config/knewsticker_appletrc
extract file ./tnz/.kde/share/config/noatunrc
extract file ./tnz/.kde/share/config/kdeprintrc
extract file ./tnz/.kde/share/config/kab2kabcrc
extract file ./tnz/.kde/share/config/kcminitrc
extract file ./tnz/.kde/share/config/kcmnspluginrc
extract file ./tnz/.kde/share/config/kdesktoprc
extract file ./tnz/.kde/share/config/ksmserverrc
extract file ./tnz/.kde/share/config/mandrakegalaxyrc
```

```
extract file ./tnz/.kde/share/config/konsolerc
extract file
./tnz/.kde/share/config/session/konsole_117f000001000107098601500000151140010_107108244
1_426022
extract file
./tnz/.kde/share/config/session/kwin_117f000001000107098598700000151140000_1071082441_4
69101
extract file ./tnz/.gnome2/gdm
extract file ./tnz/Desktop/.ArrangeIcons
extract file ./tnz/Desktop/Welcome.desktop
extract file ./tnz/Desktop/.directory-mdkgalaxy
extract file ./tnz/Desktop/Home.desktop
extract file ./tnz/Desktop/.home
extract file ./tnz/Desktop/.directory
extract file ./tnz/.kde/Autostart/.directory
extract file ./tnz/.ssh/known_hosts
extract file ./tnz/.kde/share/fonts/fonts.dir
extract file ./tnz/.kde/share/apps/konqueror/bookmarks.xml
extract file ./tnz/.qt/.qt_plugins_3.1rc.lock
extract file ./tnz/.qt/qt_plugins_3.1rc
extract file ./tnz/.qt/.qtrc.lock
extract file ./tnz/.qt/qtrc
extract file ./tnz/.kde/share/fonts/override/fonts.dir
Add links
Set directory mode, owner, and times.
set owner/mode for '.'? [yn] y
#
```

REFERENCES

The Center for Internet Security$_{SM}$. Linux Benchmark v1.1.0 (Red Hat Linux 7.0 and later). Revised October 15, 2003. URL: http://cisecurity.org/bench_linux.html (Oct. 20, 2003).

The Center for Internet Security$_{SM}$. Solaris Benchmark v1.2.0. Revised March 17, 2003. URL: http://cisecurity.org/bench_solaris.html (April 2, 2003).

Garfinkel, Simson. Spafford, Gene. Practical UNIX & Internet Security, 2nd Edition. Sebastopol: O'Reilly & Associates, Inc., 1996. 118 - 128, 605 - 633.

McClure, Stuart. Scambray, Joel. Kurtz, George. Hacking Exposed: Network Security Secrets & Solutions, Third Edition. Berkeley: The McGraw-Hill Companies, 2001. 313 - 387, 570, 578, 582 - 583

Cole, Eric. Hackers Beware: Defending Your Network From the Wiley Hacker. Indianapolis: New Riders Publishing, 2003. 479 - 491, 591 - 593, 706 - 707, 719 - 729.

Wood, Patrick H. Kochan, Stephen G. UNIX™ System Security. Pipeline Associates, Inc., 1985. 159 - 167.

Foxley, Eric. UNIX™ for Super-Users. Addison-Wesley Publishers Limited, 1985. 133 - 138.

Bellovin, S. M. "Security Problems in the TCP/IP Protocol Suite." Computer Communication Review Volume 19, Number 2 (1989). 32 – 48

Cole, Eric. "Protecting Your UNIX Systems - An Overview." SysAdmin Magazine Volume 12 Number 6 (2003). 47 - 50.

McDuffee, Keith. "Securing Linux Systems with grsecurity." SysAdmin Magazine Volume 12 Number 9 (2003). 39 - 43.

Puryear, Dustin. "Linux Kernel Tuning Using System Control." SysAdmin Magazine Volume12 Number 11). 6 - 10.

Friedl, Stephen. "Analyze This!" Linux Magazine Volume 5 Issue 5 (2003). 20 - 25.

Gleditsch, Arne Georg. Gjermshus, Per Kristian. "Cross Referencing Linux." 2001. URL: http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt (Oct. 1, 2003)

Meijer, Jan. "SSH v1 vulnerabilities actively exploited." Version 1. Nov. 20, 2001. URL: http://cert-nl.surfnet.nl/i/2001/I-01-08.htm (Sept. 10, 2003).

CERT/CC. "CERT® Advisory CA-2001-35 Recent Activity Against Secure Shell Daemons." Dec. 14, 2001. URL: http://www.cert.org/advisories/CA-2001-35.html (October 15, 2003).

CERT/CC. "UNIX Security Checklist v2.0". Oct. 8, 2001. URL: http://www.cert.org/tech_tips/usc20_full.html (October 15, 2003).

Daviel, A. "X11". Network Security. URL: http://vancouver-webpages.com/security/X11.html (October 15, 2003).

X Consortium. "X Authentication Vulnerability." CERT Vendor-Initiated Bulletin VB-95:08. Nov. 2, 1995. URL: http://www.cert.org/vendor_bulletins/VB-95:08.X_Authentication_Vul (October 15, 2003).

Fenzi, Keven. Wreski, Dave. "Files and File System Security." Linux Security HOWTO. Jun 11, 2002. Version 2.0. URL: http://www.linuxsecurity.com/docs/LDP/Security-HOWTO/file-security.html (October 15, 2003).

Fadia, Ankit. "FTP Exploits." URL: http://blacksun.box.sk/ftp_exploit.html (October 20, 2003).

Beale, Jay. "Killing Daemons! (Minimize Access Points to Secure Linux Boxes)." 2000. URL: http://www.bastille-linux.org/jay/killing-daemons.html (October 21, 2003).

Zweije, Vincent. "Remote X Apps mini-HOWTO". December 8, 2001. Version 0.7.5. URL: http://www.tldp.org/HOWTO/Remote-X-Apps.html (November 20, 2003).

U.S. Department of Energy Computer Incident Advisory Capability. "J-043g: Creating Login Banners". June 19, 1999, revised May 9, 2000. URL: http://www.ciac.org/ciac/bulletins/j-043.shtml (November 28, 2003).

Yama. "FEATURE: How to upgrade Mandrake easily with only one reboot". June 24, 2003. URL: http://www.pclinuxonline.com/modules.php?name=News&file=article&sid=7018 (November 28, 2003).