GCUX Practical Assignment

GCUX Version 3.0

Option 2

Securing Fedora Core 1 With VSFTPD

Justin Andrusk
Unix Security
Track / New
Orleans, LA

Table of Contents

Abstract

This document will provide a detailed procedure for securing a Fedora 1 Core server running vsftpd. The main goal is to implement a solution that would provide a secure FTP server that offers anonymous logins. Our target for this document will be for individuals and companies with small budgets.

Anonymous FTP servers have a long history of having exploitable buffer overflows discovered routinely.

VFTPD is an FTP daemon that can be used to offer FTP services. It has long history of being a secure and robust FTP Server. Unlike a lot of its counterparts, vsftpd has not encountered the number of buffer overflow vulnerabilities that wu-ftpd and others have experienced. It also approaches a more secure philosophy towards design.

Part of the design philosophy of vsftpd is not to abuse the use of the root user as most FTP daemons with long history of vulnerabilities often do. It also incorporates chroot-based functions to further enhance the security of the filesystem. The designers have also written the daemon in such a way as to not be susceptible to buffer overflows.

Another key security feature is not relying on insecure child processes for common functions such as making system calls to the ls command to list directory items. Even if your code is secure, but you incorporate insecure child processes, you have just subverted to security model.

Server Specification

Server Role

The server's role is to provide anonymous FTP services to the public. The server will only provide download access to the FTP server. Anonymous users will not be able to create or upload files for directories to the server.

The data that will be served on the server will be Linux device drivers for uncommon hardware. Should the system go down the data would be restored from the /mnt/backup partition as part of the restoration process.

Hardware Requirements

Component	Description
Eth0	NIC for External Network
Eth1	NIC for Internal Network
Storage	(2) 30 GB Adaptec 29320-R X SCSI-FAST Hard disk. Second disk used for rsync replication job.
24X CD-RW Drive	For Base Operating System Installation and Backup/Restore Operations
1.0GB SDRAM DDR	RAM
Motherboard	ASUS – A7V8X-X
CPU	Athlon XP 2400+

Operating System Details

Component	Description
Operating System	Fedora
Version	Fedora Core 1
Kernel	2.4.X
Filesystem	Ext3

Partition Details

Filesystem	Mount Point	Size(MB)	Device	Mount Options
Ext3	/	1000	/dev/sda1	rw,nosuid,nodev

Ext3	/ftp	25000	/dev/sda2	rw,nosuid,nodev,noexec
Swap	swap	1066	/dev/sda3	n/a
Ext3	/mnt/backup	35071	/dev/sdb1	rw,nosuid,nodev,noexec
Ext3	/usr	5000	/dev/sda4	ro,nosuid,nodev
Ext3	/tmp	500	/dev/sda5	rw,nosuid,nodev,noexec
Ext3	/var	2000	/dev/sda6	rw,nosuid,nodev,noexec

All of the partitions will be mounted with the nosuid, nodev mount options. This will prevent any suid programs from being created on our system. The nodev option will prevent non-root users from mounting the partition. The /var, /tmp, and /ftp partitions will be storing raw data files and execute permissions will not be needed. The noexec option will be set to enforce this. The /usr partition will be used to store and execute common programs. There will be no need to write to this partition, so the partition will be mounted read-only.

The root partition will be used primarily for storing configuration files and the base installation of various binary programs. The majority of the program files will be stored in the /usr partition, so that the root partition doesn’t need to have an inordinate amount of space allocated.

The /ftp partition will be storing the most data in relation to the other partitions, so a large chunk of the free space will be allocated to the /ftp partition. This will store all the data that the FTP server will provide anonymous access to.

The /mnt/backup partition will be used to backup a number of directories using an ‘rsync’ script should the system experience and outage and need to recover from such an event.

The /usr partition will store the majority of the daemons and application binaries for running various services. 5GB should be sufficient to address this purpose.

The /tmp partition will store temporary files created by processes and users.

Mount Options Description

Below is a table describing each of the mount options that are used in the /etc/fstab file.

rw - Read-Write. Mount the partition as read-write. This will permit users and applications to read and write to the partition.

ro – Read-Only. Users will not be able to write to the partition.

nosuid – Deny permission bits to be set suid.

noexec – Deny the ability to execute binaries on partition.

nodev – Only permit root to mount the filesystem.

Installed and Configured Services

Service Name	Purpose	Initialization
crond	Daemon for Cron	Boot Level Script
sshd	Daemon for SSH Protocol	Boot Level Script
vsftpd	Daemon for FTP Protocol	Boot Level Script

Server Architecture

Figure 1-1: High-Level Traffic Flow of FTP Architecture

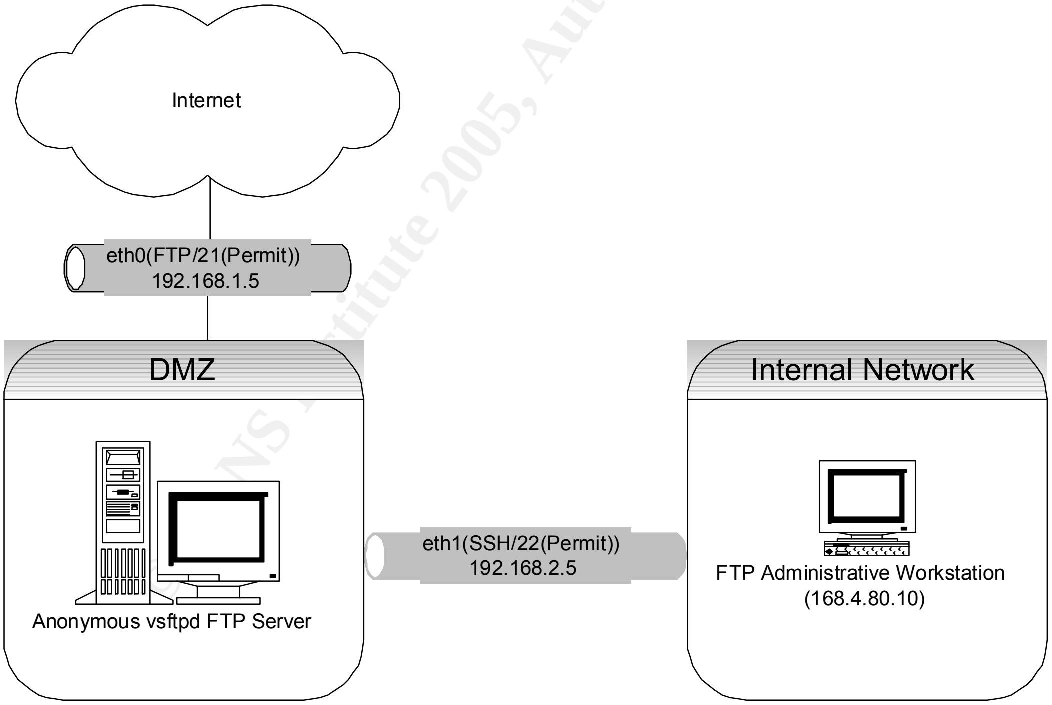
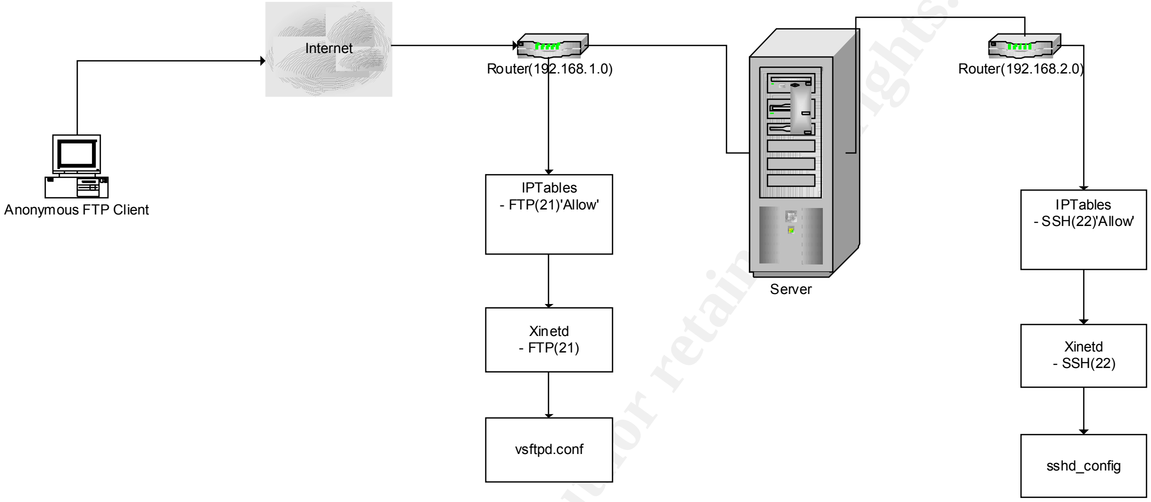


Figure 1-2: Flow of Access Controls as FTP Connection is initiated



Risk Analysis

Running an anonymous FTP server on the public Internet introduces a number of potential security risks. There's a plethora of exploit scripts targeted at various FTP daemons that can be used against the server. Once the box is 'rooted', it can then be used to store pirated software, Trojans, and other malicious data. Backdoors can also be stored on the server, so that the attackers can access the server at a later time on an alternate pathway.

To mitigate this risk we are going to configure the server with a minimal amount of network services, harden the services that we will be running, at secure the system with a 'defense in depth' philosophy.

The FTP service will be the only service available to the outside world. The sshd daemon will be restricted to the private internal network to mitigate the potential for exploitation.

Identified Risk Issues

Privilege Escalation due to compromise of Network Services

One of the risks associated with our configuration is that should a root level exploit be applied to one of our network-based services, the system would be compromised. Should this scenario occur, a layer of security mechanisms must be in place to detect this and mitigate the compromise.

Multi-Homed System

The risk associated with having a multi-homed system is that if one of the interfaces is compromised packets could be redirected. Where could the packets be redirected? They could have them routed between the two interfaces and thereby gain access to the services on the other interface.

Hosting an Anonymous FTP Server on the Internet

The risks associated with running a FTP service on the public Internet, is that should an exploit be made available for a vsftpd vulnerability, the service could be compromised. Although vsftpd has an established reputation for being a secure FTP server, there's always the possibility that a new exploit hasn't been discovered at the time of this writing.

If this were to occur additional controls need to be put in place to combat the compromise.

SSH Access

Running the SSH daemon internally also poses risk from the internal network. There have been a few vulnerabilities associated with the sshd daemon and we need to make sure that were running a patched version. Another item of concern is if the routing between the two interfaces is compromised, sshd needs to be setup to only permit traffic from a specific source.

Mitigated Risks

Risk	Mitigation Plan
Privilege Escalation due to compromise of Network Services	• Minimize the use of the root account as much as possible. • Ensure additional Access Controls are in place. • Set restrictive mount options according to the “Modifying Default Mount Options” section. .

Multi-Homed System	• Ensure IP Forwarding is disabled on our system. • IPTable rules are specific for the corresponding interface. • Ensure that the corresponding services are bound to the correct interface.
SSH Access	• Restrict root logon via sshd_config. • Restrict source address permissions with iptables. • Monitor sshd configuration files with Tripwire. • Bind SSHD to correct network interface by adding, "ListenAddress 192.168.2.5" to /etc/ssh/sshd_config. • Only allow 'ftpadmin' account SSH access to the server.
FTP Access	• Restrict access to the external interface via iptables. • Restrict application permissions in vsftpd.conf. • Monitor vsftpd configuration files with Tripwire. • Bind vsftpd to correct network interface by adding, "listen_address=192.168.1.5" to /etc/vsftpd/vsftpd.conf.

Installation and System Hardenening

Software Media

Before continuing a number of CD images and software packages will need to be obtained to install the operating system and other applications. These should be broken down as follows:

Operating System ISO Images

The ISO images and MD5SUM below can be obtained from:

http://download.fedora.redhat.com/pub/fedora/linux/core/1/i386/iso. The files to be retrieved are listed below:

- yarrow-i386-disc1.iso
- yarrow-i386-disc2.iso
- yarrow-i386-disc3.iso
- MD5SUM

Once the files have been downloaded, run:

md5sum –check MD5SUM

The output should display *iso_filename*: OK. The output from the previous command will error out on the three SRPMS files that were not downloaded.

Miscellaneous Software Packages

These should be burned to a single CD-R:

Tripwire : http://download.fedora.us/fedora/fedora/1/i386/SRPMS.testing/tripwire-2.3.1-18.fdr.3.1.src.rpm

CIS-Benchmark for Linux: http://cisecurity.org/tools2/linux/cis-linux.tar.gz
MD5 Checksum for CIS-Benchmark Tool: http://cisecurity.org/tools2/linux/cis-linux_tgz_md5.txt.

Note: Make sure you run a version of md5sum against the cis-linux.tar.gz to make sure the hash that's extracted from the binary matches the cis-linux_tgz_md5.txt file before burning the CD-R.

Fedora RPM Patches

Ensure that the procedure below is performed from a secured Unix based host.

Perform the procedure below to download the Fedora security patches from the FTP site below:

1. su – to gain root access.
2. mkdir /home/updates
3. mkdir /home/updates/kernel
4. cd /home/updates
5. wget ftp://rpmfind.net/linux/fedora/core/updates/1/i386/
6. mv kernel*.* /home/updates/kernel

Create an ISO image to burn the /home/updates filesystem to a CD-R. Two different installation methods need to be performed. When the kernel updates are applied, they need to be applied in such a way as to not break our system and to revert to the previous kernel if necessary.

Base Operating System Installation

Obtaining the installation media

You will need to obtain the installation media by retrieving the files below from one of the Fedora mirror sites. One you can reference is http://download.fedora.redhat.com/pub/fedora/linux/core/1/i386/iso/:

Directory: /linux/6/fedora/core/1/i386/iso

Files:

- yarrow-i386-disc1.iso
- yarrow-i386-disc2.iso
- yarrow-i386-disc3.iso

You will need to burn these ISOs to CDs to install the operating system.

Note: It's vital that none of the network interfaces are attached to either the public or private network prior to installation. Doing so could provide an attacker an opportunity to exploit our system. The time to attach the network interfaces to the public and private networks will be specified once the system is secured.

Booting the Installation Media

Insert the Fedora Core 1 CD 1 disc into the CD-ROM and boot the system.
At the 'boot:' prompt hit the <Enter> key.
Hit <Enter> to have the system validate your CD media.
Hit <Enter> to initiate the test.
You should receive a 'Pass' and you can hit <Enter> to continue.
Insert the remaining discs and repeat the procedure above.
Select 'Continue' and hit <Enter> when your last disc has been tested.

Welcome Screen

Click **Next**

Language Selection

Click **Next** to select **English** as the language to use.

Keyboard Configuration

Click **Next** to select **U.S. English** for the keyboard type.

Mouse Configuration

Select the **Microsoft/Intellimouse Optical(USB)**.
Click **Emulate 3 buttons**.
Click **Next**.

Installation Type

Click **Custom**.
Click **Next**.

Partitioning Scheme

Click **Manually partition with Disk Druid**.
Click **Next**.
Highlight the partition labeled: **Free Space** on **/dev/sda1**.
Click **New.**
Select **/** for the mount point.
Type: **1000** for the size.
Click on: **Force to be primary partition**.
Click **Ok**.
Select **Add Anyway** to the warning message.
Highlight the partition labeled: **Free Space** on **/dev/sda1**.
Click **New.**
Type: **/usr** for the mount point.
Type: **5000** for the size.
Click on: **Force to be primary partition**.
Click **Ok**.
Highlight the partition labeled: **Free Space** on **/dev/sda1**.
Click **New.**
Type: **/var** for the mount point.
Type: **2000** for the size.
Click on: **Force to be primary partition**.
Click **Ok**.
Highlight the partition labeled: **Free Space** on **/dev/sda1**.
Click **New.**
Type: **/tmp** for the mount point.
Type: **500** for the size.
Click **Ok**.
Highlight the partition labeled: **Free Space** on **/dev/sda1**.

Click **New**.
Change the **Filesystem Type:** to **swap**.

Type: **1066** for the size.
Click **Ok**.
Highlight the partition labeled: **Free Space** on **/dev/sdb1**.
Click **New**.
Type: **/mnt/backup** for the mount point.
Change the **Filesystem Type:** to **ext3**.
Click **Fill to maximum allowable space**.
Click **Ok**.
Click **Next** to commit partition changes.

Bootloader Configuration

Click **Next** to select Grub as the bootloader.
Boot Loader Password Configuration
Click **Next** to disable bootloader password. An MD5 encrypted password will be added to the /etc/grub.conf file later in the document.

Network Configuration

Highlight the **eth0** device.
Click **Edit**.
Uncheck **Configure using DHCP**.
Make sure **Activate on boot** is checked.
Specify: **192.168.1.5** for the IP address.
Specify: **255.255.255.0** for the Netmask.
Specify: 192.168.1.0 for the Network.
Specify: 192.168.1.255 for the Broadcast.
Specify: **abcftps01.myftp.com** for the hostname.
Specify: 192.168.1.1 for the gateway.
Specify: The IP Address for your Primary DNS Server.
Specify: The IP address for the Secondary DNS Server.
Click on **eth1**.
Click **Edit**.
Uncheck **Configure using DHCP**.
Make sure **Activate on boot** is checked.
Specify: **192.168.2.5** for the IP address.
Specify: **255.255.255.0** for the Netmask.
Specify: **192.168.2.0** for the Network.
Specify: **192.168.2.255** for the Broadcast.
Click **NEXT**.

Firewall Configuration

Ensure that **Enable Firewall** is enabled.

Click on:

- FTP
- SSH

Click **Next**.

Language Selection

Click **Next** to select **English(USA)** as the default language.

Time zone Selection

Select your time zone and click **Next**.

Set Root Password

Select a strong **root** password and type it in the two textboxes. A strong password would meet the criteria below:

- Consists of at least one uppercase and one lowercase character.
- Have a length of at least 7 characters.
- Contain at least one numeric digit.
- Contain at least one special character such as: #, $, or @.

Click **Next**.

Package Group Selection

Uncheck *All* packages. Only the required packages should be installed. The reasoning behind this is that the fewer applications that are on the system, the fewer potential vulnerabilities that could arise from the use of the system.

Click on **FTP Server**
Click on **System Tools.**
Click on the **Details** link next to **System Tools**.
Uncheck all options except **nmap**.
Click **Ok**.
Click on **Development Tools**.
Click **Details**.
Uncheck *all* optional packages except **rpm-build**.
Click **Ok**.
Click **Next**.

About to Install

Click **Next** to begin installation.
Click **Continue** to the **Required Install Media** prompt.
When prompted, Insert disc 2 and click **Ok**.
When prompted, insert disc 3 and click **Ok**.

Boot Diskette Creation

Click on **No, I do not want to create a boot diskette**.
Click **Next**.
Click **Reboot**.

Post-Installation Setup

Logon to the console as the root account..
Type: adduser ftpadmin and press <Enter>.
Type: passwd ftpadmin and press <Enter>.
Type a strong password and press <Enter>.
A strong password would meet the criteria below:

- Consists of at least one uppercase and one lowercase character.
- Have a length of at least 7 characters.
- Contain at least one numeric digit.
- Contain at least one special character such as: #, $, or @.

Re-type the password and press <Enter>.

Updating RPM Packages

The system will need to be patched following the installation. Insert the CD-R that you created when you pulled the updated RPM files from the *Software Media* section.

1. Logon as the ftpadmin account.
2. su – to obtain root access.
3. Change to the root directory of the CD-R filesystem.
4. Type: rpm –F *.rpm. This will install all of the non-kernel updates.
5. Type: cd kernel
6. Type: rpm –I *.rpm. This will install the kernel updates without breaking the system.

Once the updates are applied, schedule a reboot during off-hours to test the functionality of the new kernel. This will allow you to revert to the previous kernel version if the new kernel breaks the functionality of the system.

Post Installation Hardening and Configuration

Remove User Accounts

The majority of the accounts that are installed are needed in most scenarios. To further secure our environment, we'll disable user accounts that won't be needed. To accomplish this we'll implement the shell script below(Make sure you are root):

1. Logon as the 'ftpadmin' account.
2. Type: su –
3. Enter the root account password.
4. cd ~/bin
5. vi acctclean.sh
6. Add the text below to the acctclean.sh file:

```
#!/bin/sh
for user in `awk –F: '($3 < 500 && $3 > 0) {print $1 }' /etc/passwd`
do
        usermod –L –s /dev/null $user
done
usermod –L –s /dev/null nfsnobody
```

7. Run the acctclean.sh, which will disable the unused accounts.

Password Policy Enforcement

The table below is a matrix of our password policy for the system to protect the root and ftpadmin accounts:

Description	**Variable**	**Value**
Maximum days Password may be used	PASS_MAX_DAYS	90
Minimum days allowed between password changes	PASS_MIN_DAYS	7
Minimum acceptable password length	PASS_MIN_LENGTH	8
Number of Days warning about password expiration	PASS_WARN_AGE	7

Change the variables above with the corresponding values referenced in the table above in the /etc/login.defs file to enforce our password policy.

Existing accounts will need to be modified with the 'chage' command to reflect this policy change. Execute the shell script below to apply the change to existing accounts:

```
for name in `cut -d: -f1 /etc/passwd`; do
```

```
uid=`id -u $name`
if [ $uid -ge 500 -a $uid != 65534 ]; then
/usr/bin/chage -m 7 -M 90 -W 28 $name
fi
done
```

Disable Anonymous Shutdowns

Limit Cron Usage

To limit who can run the crontab program on our system, we'll need to create the /etc/cron.allow file and place the root account in this file. If another system account was compromised, the attacker could utilize one of these accounts to execute cron jobs.

Restrict Cron File Permissions

Since the crontab command is setuid to root, we will restrict cron file permissions to the root account only. Execute the commands below to accomplish this:

```
chown –R root:root /etc/cron* /var/spool/cron
chmod –R go-rwx /etc/cron* /var/spool/cron
```

Boot Level Security

One thing most people overlook when securing a system is boot level access to the box. There are a couple of items that we will want to modify to harden the boot level security of our system.

Require root password when booting into Single User Mode

Fedora Core 1 doesn't by default require the root password when booting into Single User Mode. This is difficult to understand, considering it's a one-liner to enable this feature. Anyone with physical access to the machine could boot into single-user mode and reset the root password to compromise the system and the data. To have the system prompt for the root password when entering single user mode, add the line below to the /etc/inittab file:

```
sum:S:wait:/sbin/sulogin
```

Password Protect the GRUB Boot Loader

As an added security measure an md5 encrypted password is going to be placed in our /etc/grub.conf. This will prevent someone with physical access to the server to pass parameters to the boot process without supplying the md5 password.

1. Type grub in the shell prompt.
2. Type: md5crypt
3. Enter a strong password.
4. Copy the md5 encryption string to the /etc/grub.conf similar to the line below:

   password –md5 *encrypted string*

Disabling Anonymous Shutdowns

To prevent someone with physical access to the server to enter the 'ctrl+alt+del' command sequence to reboot the server, the key sequence will be trapped to authpriv.info.

1. Edit the /etc/inittab.
2. Find the line that contains the string:
   ca::ctrlaltdel:/sbin/shutdown –t3 –r now
3. Change this entry to prevent anonymous users from rebooting the system with the Ctrl+Alt+Del key sequence by replacing the string with the entry below:
   ca::ctrlaltdel:/usr/bin/logger –p authpriv.info 'ctrl-alt-del trapped'

Hardening Operating System Services

Hardening Network Connectivity

Turning Off Services

There are a number of services that will need to be disabled. The less services that are running the less exposure there is to an exploit. We can disable these services by a simple shell script:

```
#!/bin/sh

for a in atd gpm sendmail pcmcia apmd ipchains anacron xinetd
do

        chkconfig –level 12345 $a off
done
```

Kernel Tuning

There are two classifications of parameters we can enable for increasing the security of our system:

- ‘Soft’ – These parameters can be modified by users with the ‘ulimit’ command.
- ‘Hard’ – These parameters cannot be modified by users.

Enable these by editing the /etc/security/limits.conf file with the attributes below[II]:

```
# Prevent Global Core Dumps

*        hard   core    0

# Set Per-User Based Limits

*        soft   nproc  64

*        hard   nproc 128

*        soft   nofile  256

*        hard   nofile  1024
```

In our configuration above, we are preventing ‘core’ files from being generated on our system. We are also limiting the number of processes per user and for the system has a whole. The last two entries limit the number of open files on both the user and system level. The ‘*’ above includes all groups and users.

“soft” entries can be overridden by users on the system with the ‘ulimit’, whereas “hard” entries cannot be modified.

Hardening Kernel Parameters

Edit the /etc/sysctl.conf and add the entries per the table below:

```
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0

# Need to include net.ipv4.conf.default.* as well.
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

Description of Kernel Parmeters[6]

tcp_max_syn_backlog: Maximal number of remembered connection requests, which still didn't receive an acknowledgement from connecting client. This is set on the high side to account for the possibility of a large number of FTP client connections.

log_martians: Log packets with no known source route.

accept_source_route: Disable source routing. This could allow an attacker to forward packets through a trusted interface to bypass security.

send_redirects, accept_redirects, and secure_redirects: The "redirects" settings will disable ICMP redirects which generates additional traffic to and from the client, which is not needed.

Additional System Tuning

There are a number of non console or tty entries in the /etc/securetty file. Delete the lines below from /etc/securetty:

- vc/7
- vc/8
- vc/9
- vc/10
- vc/11
- tty7
- tty8
- tty9
- tty10
- tty11

This should be done to limit the number of consoles that can be used to logon to the server. Permitting these to stay open could allow an attacker with physical access to the system to use a serial based connection to access the server. This will disable anonymous root logons, which we don't want to enable on our system. For administration purposes, the ftpadmin account will be used and will 'su –' to the root account as needed.

Hardening UMask Settings

To further harden our system we are going to set restrictive umask settings in the files below by setting the umask to 077. Add 'umask 077' to each of the files below:

- /etc/profile
- /etc/cshrc
- /etc/tcshrc
- /etc/bashrc
- /root/.bashrc
- /root/.bash_profile

With a umask of 077 files and directories will be not be readable by other users on the system. Should a non-privileged account be compromised, that account wouldn't be permitted to view other users files.

Restrict /etc/crontab Permissions

Execute the command below to prevent non-root accounts from being able to modify /etc/crontab. This could allow a remote user to issue a denial service attack to subvert cron jobs that run on the server.

Type: chmod go= -R /etc/crontab

Hardening SSH Protocol

SSH(Secure Shell) is a low-cost, software-based solution for keeping prying eyes away from the data on a network. SSH encrypts the data on the network from prying eyes and offers a variety of authentication methods, such as: Password, Public Key, Kerberos, and PAM[3].

SSH will be used to permit remote administration of the FTP server. Our configuration parameters will be set in the /etc/ssh/sshd_config file, which can be referenced in Appendix B.

Restricting Mount Options to Non-Root Accounts

By default non-root users can mount a variety of removable storage devices including: Floppy, CD-ROMs, USB Flash Cards, and Jazz and Zip drives. To prevent non-root accounts from being able to mount these devices, edit the /etc/security/console.perms as root and comment out the lines below:

```
# <cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
#<pilot>=/dev/pilot
#<jaz>=/mnt/jaz*
#<zip>=/mnt/pocketzip* /mnt/zip*
#<ls120>=/dev/ls120 /mnt/ls120*
#<scanner>=/dev/scanner /dev/usb/scanner*
#<rio500>=/dev/usb/rio500
```

```
#<camera>=/mnt/camera* /dev/usb/dc2xx* /dev/usb/mdc800*
#<memstick>=/mnt/memstick*
#<flash>=/mnt/flash*
#<diskonkey>=/mnt/diskonkey*

# permission definitions
# <console>  0660 <floppy>     0660 root.floppy
# <console>  0600 <sound>      0600 root
# <console>  0600 <cdrom>      0660 root.disk
# <console>  0600 <pilot>      0660 root.uucp
# <console>  0600 <jaz>        0660 root.disk
# <console>  0600 <zip>        0660 root.disk
# <console>  0600 <ls120>      0660 root.disk
# <console>  0600 <scanner>    0600 root
# <console>  0600 <camera>     0600 root
# <console>  0600 <memstick>   0600 root
# <console>  0600 <flash>      0600 root
# <console>  0600 <diskonkey>  0660 root.disk
# <console>  0600 <rem_ide>    0660 root.disk
# <console>  0600 <fb>         0600 root
# <console>  0600 <kbd>        0600 root
# <console>  0600 <joystick>   0600 root
# <console>  0600 <v4l>        0600 root
# <console>  0700 <gpm>        0700 root
# <console>  0600 <mainboard>  0600 root
# <console>  0600 <rio500>     0600 root
```

Defining IP Table Rules

IPTables is a software firewall that will permit us to setup rules for accessing our system. It provides support for stateful firewalling.

SSH connections will be permitted to only the internal interface. Outsiders will not be given the opportunity to login. FTP connections will be permitted to only the external interface.

IPtables will also be used to prevent DoS(Denial of Service) attacks against our system.

To accomplish this our /etc/sysconfig/iptables.conf file will be as follows:

```
#Define Interface Variables

EXT_IFACE=”eth0”
INT_IFACE=”eth1”
```

```
#Set default policies to DROP
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

# Permit Incoming SSH connections on device eth1
iptables –i $INT_IFACE  –dport 22 –j ACCEPT

# Permit External FTP Connections on device eth0
iptables –i $EXT_IFACE –dport 21 –j ACCEPT
iptables –i $EXT_IFACE –dport 20 –j ACCEPT

# Create syn-flood chain from detecting Denial of Service attacks
iptables –t nat –N syn-flood[1]

# Limit 12 Connections per second(burst to 24)
iptables –t nat –A syn-flood –m limit --limit 12/s –limit-burst 24 \
        -j RETURN[1]
iptables –t nat –A syn-flood –j DROP[1]


# Drop Xmas & Null Tcp Packets
iptables –t nat –A PREROUTING –p tcp –tcp-flags ALL –j DROP[1]
Iptables –t nat –A PREROUTING –p tcp –tcp-flags ALL NONE –j DROP[1]
```

Third Party Applications

Tripwire Installation

Tripwire is a tool that checks to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc[5]. By scanning the current system and comparing that information with the data stored in the database, Tripwire detects and reports any additions, deletions, or changes to the system outside of the specified boundaries[2].

At first this may seem like overkill, but when you expose a system to the Internet and a week later you have a system compromised, you realize the value of this tool.

Installing Tripwire

Logon as the 'ftpadmin' account.
Type: cd /tmp
Type:
wget http://download.fedora.us/fedora/fedora/1/i386/SRPMS.testing/tripwire-2.3.1-18.fdr.3.1.src.rpm
Type: su –
Type the root password.
Type: rpmbuild –rebuild tripwire-2.3.1-18.fdr.3.1.src.rpm and press <Enter>.
Type: rpm –Uvh /usr/src/redhat/RPMS/i386/tripwire-2.3.1-18.fdr.3.1.i386.rpm

Configuring Tripwire

1. Login as the **ftpadmin**.
2. Type: **su –** su to root.
3. Type: **/etc/tripwire/twinstall.sh**.
4. Enter a passphrase for the site and hit <enter>.
5. Enter the passphrase again and hit <enter>
6. Enter the local keyfile passphrase and hit<enter>.
7. Enter the local keyfile passphrase again and hit <enter>.
8. Enter site passphrase and hit <enter>.
9. Enter site passphrase and hit <enter>.
10. We will need to modify our Policy file to exclude files that are in the default Tripwire installation, but that are not present on Fedora Core 1 installation. Our policy file can found in Appendix A.

11. Once we have the Tripwire policy file configured as defined in Appendix A, we need to run: **/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt** to update the Policy File. You'll need to supply the local passphrase for the command to run.
12. Next we initialize the database with: **tripwire –init**.
13. Enter the local passphrase.
14. Create cronjob under **root** to run an integrity check every hour:

    0 * * * * /usr/sbin/tripwire –check

The question that arises with Tripwire is: What if our Tripwire is compromised? If that happens any Tripwire related reports could not be trusted. To address this scenario, we are going to:

1. Rename the Tripwire binary from /usr/tripwire to /usr/kts. We could name this to any arbitrary name. The reason we want to do this is to make it more difficult for the attacker to compromise our Tripwire binary.
2. Mount the /usr partition as read-only. To do this – modify the /etc/fstab file to change the options for /usr from **defaults** to **defaults,ro** to mount the **/usr** partition as read-only. Again all the attacker would have to do is remount the partition as read-write. The goal of implementing these changes is to deter the attacker.

VSFTPD Configuration

The good thing about using vsftpd is that there's very little configuration that needs to be done to vsftpd.conf out of the box. There are a few configuration options we'll want to change though.

The settings that we are concerned with in regards to security are:

- Enable Anonymous Access: Since the main purpose of deploying a vsftpd server for anonymous FTP access, we want to enable this setting.
- Disable local users to login: We don't want to enable this as this would subvert our purpose of an *anonymous* FTP server.
- Disable Write Access: Enabling this feature would be a very bad idea.
- Local Umask: The majority of FTP clients use a umask of 022 and we'll do the same.
- Disable Uploads for Anonymous: This would permit anyone to upload malicious type content. This will be disabled.
- Disable anonymous user to create directories: Again, we don't want to enable the anonymous account the ability to *create* any items on our FTP server.

Change the home directory for the 'ftp' id in /etc/passwd to point to the '/ftp' directory. The complete vsftpd.conf can be found in Appendix C.

Design and Implement Ongoing Maintenance Procedures

Maintenance Strategy

The advantage of installing a system with a minimal set of packages and services is that only a few items need to be patched. Our strategy is going to be to monitor a variety of security related bulletins and determine if any affect our system and patch according to the threat.

An example of this philosophy would be taking a look at the SSH protocol. There have been vulnerabilities that have affected the use of version 1 of the protocol. Since we have setup our sshd_config file to only accept SSH version 2 connections there's no need for us to patch for the vulnerability.

Maintenance Procedures

Backup/Recovery

The FTP server is offered as an anonymous FTP Server. Anonymous users are not permitted to create objects in the FTP filesystem. The FTP administrator will be uploading the data to the pub FTP directory.

We will mirror the first hard drive with the second, so that in the event of a disaster, we have a working copy that can be switched to be the primary drive, while the damaged drive is replaced or repaired.

As of this writing, a Host-Raid driver doesn't exist for the Adaptec 29320 on Fedora Core 1. Due to this limitation we will implore a software based mirroring process using the rsync program.

The benefits of using the rsync program is that it will only synchronize the differences between the filesystem. We will not be synchronizing the entire hard drive, but only the portions of the filesystem that we have decided are critical to recover. We will be synchronizing the areas below:

- /etc
- /var/spool
- /root
- /home/ftpadmin
- /ftp

To accomplish this proposition, the ‘rsync’ program will be used in a shell script to mirror the data to the secondary hard drive. Below is a copy of our shell script:

```
#!/bin/sh

RSYNC="/usr/bin/rsync"
RSYNC_ARGS="--archive --one-file-system"
LOG="/root/logs/mirror.`date +%d%m%y.log`"
DESTPART="/mnt/synchro"

date>${LOG}

for x in /etc /root /ftp /var/spool /home/ftpadmin
do
  ${RSYNC} ${RSYNC_ARGS} $x ${DESTPART} 2>/dev/null>>${LOG}
done

date>>${LOG}
```

Disaster Recovery Considerations

For disaster recovery purposes we’ll be backing up our main configuration files and data, so that in the event of a disaster to our FTP server, we will re-install the base operating system and restore the configuration files from our last successful backup.

The data will be mirrored to another server using the ‘rsync program.

Log File Review Plan and Procedures

Obviously, with our logfiles constantly changing as our system changes, we need a process of tracking these changes should they become critical. This could include scenarios such as the ones described below:

- Hardware Related Errors
- Network Congestion or Errors
- Storage Thresholds Being Reached
- System being compromised by a remote attacker

LogCheck Configuration

Our chosen tool for this job is Logwatch. Logwatch is a PERL script that will parse through our SYSLOG for certain anomalies.

Logcheck installs a daily cron job in **/etc/cron.daily** that will e-mail the results to the root account, which can then be reviewed for further analysis. For one we want to have e-mails sent to the ftpadmin account instead of to root. To accomplish this we need to edit the /etc/logs.d/conf/logwatch.conf file. Change the line labeled: **MailTo** from root to ftpadmin.

Next we want to configure which services we want to monitor. The default installation utilizes a number of services that we don't need. To disable the unneeded services rename all the files in /etc/log.d/conf/services to *filename.ext.orig* except sshd.conf, vsftpd.conf, yum.conf, syslogd.conf, kernel.conf, and cron.conf.

Now we want to perform a similar function in /etc/log.d/conf/logfiles. There are only a few logfiles that will be needed. They are:

- cron.conf
- messages.conf
- secure.conf
- vsftpd.conf
- xferlog.conf – For vsftpd transfers
- yum.conf

All other files under /etc/log.d/conf/logfiles can be renamed or deleted.

Baseline Violations Plan and Procedures

For our purposes we'll be using Tripwire to establish a baseline plan and procedure if specific files are modified or deleted. See Appendix A for the Tripwire configuration file, which documents our filesystem baseline.

The Tripwire report will be reviewed by the FTP administrator on a daily basis. If violations are discovered they will be acted up according to the risk that they impose on the system.

For example, if we find that our /etc/passwd file has been modified, but no other violations have occurred, it's probable that a password was changed on a specified account. It's also noteworthy to note that our password policy requires password changes periodically, so changes to this file should be expected in relation to our password policy.

If on the other hand, /etc/passwd, /etc/vsftpd.conf, and /bin/ls, changes we have a rootkit installed on our system. In this scenario, further forensics would need to be performed on the host and a remediation plan executed.

Test and Verify the Setup

Test and Verification Plan and Procedure

In order to verify and validate our proposition that only the services accessed from the chosen interface work a test plan has been established. A series of seven tests will be performed to validate our network access policy.

Test One: Logon as Anonymous to download a file

Our first test will be to logon to the FTP server as anonymous and download a file from the pub directory.

1. Using your preferred FTP client, logon to **myftp.com**.

2. Type: anonymous for the username.

3. Enter: user@domain.com for the password.

4. Type: cd pub

5. Type: get *filename*.

Test Two: Logon as Anonymous to create a directory

Next we'll attempt to create a directory logged on as the anonymous user.

1. Using your preferred FTP client, logon to **myftp.com**.
2. Type: anonymous for the username.
3. Enter: user@domain.com for the password.
4. Type: mkdir *testdir*.
5. You'll receive a permission denied error.

Test Three: SSH into the system from the internal network

The next test we'll verify that we can logon to the FTP server via the SSH protocol from an internal host.

1. Using your preferred SSH client, logon to **abcftps01.myftp.com**.
2. Type: ftpadmin for the username.
3. Enter: the password for the 'ftpadmin' account.

Test Four: SSH into the system from the Internet

The last test will be to verify that a host *cannot* login via SSH from the Internet. You'll need to perform this procedure on an external host with Internet access.

1. Telnet to myftp.com over port 22.
2. You should receive a 'Connection Failed' error message.

Test Five: Ensuring Firewall is Operating on External Interface

To verify that the only available service to outside hosts is FTP on port 21, a nmap scan will be run against the Internet facing interface.

1. Bring up a shell prompt.
2. Type: nmap –v abc.com
3. The only output should be FTP running on port 21.

Test 6: Ensure that firewall is Operating on Internal Interface

To verify that the only available service to internal hosts is SSH on port 22, a nmap scan will be run against the internal interface.

1. Bring up a shell prompt.
2. Type: nmap –v 192.168.1.5.
3. The only output should be SSH running on port 22.

Test 7: Using CIS-Benchmark to Test Security of System

Installing CIS-Benchmark Tool[4]

1. Run the script below as the 'ftpadmin' id.
2. Type: 'su –' to gain root privileges.
3. Type: 'cd cis' and press <enter>.
4. Type: 'rpm –hiv CISscan-1.4.2-1.0.i386.rpm
5. Edit the /usr/local/CIS/tester.sub file.
6. Add the code excerpt below to the section on line 213 :

```
elsif ($release_line =~ /Fedora/) {
  $DISTRIBUTION = "RH";
  $DISTRIBUTION_VERSION = $1;
}
```

7. Type: /usr/local/CIS/tester.sub from a command shell.

Below are the results from the CIS Benchmark scan:

```
*** CIS Ruler Run ***
Starting at time 20041202-21:00:43

Positive: 1.1 System appears to have been patched within the last month.
Positive: 1.2 System is running sshd and it's configured well.
Positive: 2.1 inetd/xinetd is not listening on any of the miscellaneous ports
checked in this item.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 imap is deactivated.
Positive: 2.7 POP server is deactivated.
Positive: 3.1 Found a good daemon umask of 022 in
/etc/rc.d/init.d/functions.
Positive: 3.2 inetd has been deactivated.
Positive: 3.3 Mail daemon is not listening on TCP 25.
Positive: 3.4 Graphical login is deactivated.
Positive: 3.5 X Font Server (xfs) script has been deactivated
Positive: 3.6 Miscellaneous scripts are all turned off.
Positive: 3.7 Windows compatibility servers (samba) have been
deactivated.
Positive: 3.8 NFS Server script nfs is deactivated.
Positive: 3.9 This machine isn't being used as an NFS client.
Positive: 3.10 NIS Client processes are deactivated.
Positive: 3.11 NIS Server processes are deactivated.
Positive: 3.12 RPC rc-script has been deactivated.
Positive: 3.13 netfs rc script is deactivated.
Positive: 3.14 printing daemon is deactivated.
Positive: 3.15 Web server is deactivated.
Positive: 3.16 SNMP daemon is deactivated.
Positive: 3.17 DNS server is deactivated.
Positive: 3.18 SQL database server is deactivated.
Positive: 3.19 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.20 Squid web cache daemon deactivated.
Positive: 3.21 Kudzu hardware detection program has been deactivated.
Positive: 4.1 Network parameters for item 4.1 are set well.
Positive: 4.2 All 'additional' network parameters set correctly.
Positive: 5.1 syslog captures authpriv messages.
Positive: 5.2 FTP server is configured to do full logging.
Positive: 5.3 All logfile permissions and owners match benchmark
recommendations.
Positive: 6.1 All appropriate partitions are mounted nodev.
```

```
Positive: 6.2 /etc/fstab mounts all removable filesystems nosuid and nodev.
Positive: 6.3 Users cannot mount removable media.
Positive: 6.4 password and group files have right permissions and owners.
Positive: 6.5 all temporary directories have sticky bits set.
Positive: 7.1 rhosts authentication totally deactivated in PAM.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either don't
exist, are zero size or are links to /dev/null.
Positive: 7.3 FTP daemons do not permit system users to use FTP.
Positive: 7.4 X11 Server is blocked from listening on TCP port 6000.
Positive: 7.5 cron.allow and at.allow are configured correctly.
Positive: 7.6 crontabs all have good ownerships and modes
Positive: 7.7 All authorized-use-only warning banners are in place.
Positive: 7.8 All authorized-use-only warning banners are in place.
Positive: 7.9 System is set to only allow root login on console.
Positive: 7.10 GRUB is password-protected.
Positive: 7.10 GRUB is password-protected.
Positive: 7.11 Single user mode requires a root password.
Positive: 7.12 /etc/exports is empty or doesn't exist, so it doesn't need to be
tuned for privports.
Positive: 8.1 All system accounts are locked/deleted
Positive: 8.2 All users have passwords
Positive: 8.3 User passwords expire within reasonable timeframes.
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.6 root's PATH is clean of group/world writable directories or the
current-directory link.
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles in user home directories!
Positive: 8.9 No user has a .netrc file.
Positive: 8.10 Umasks in all global shell configuration files appear to be
good.
Positive: 8.11 Coredumps are deactivated.
Preliminary rating given at time: Thu Dec  2 21:00:44 2004

        Preliminary rating = 9.69 / 10.00

Ending run at time: Thu Dec  2 21:00:44 2004

        Final rating = 9.69 / 10.00
```

References

[1] Flickenger, Rob. Linux Server Hacks Sebastopol: O'Reilly, 2003. 91.

[2] Gerhard Mourani. Securing and Optimizing Linux:RedHat Edition Portland: OpenDocs, 2000. 204.

[3] Daniel J. Barrett and Richard E. Silverman. SSH, the Secure Shell: The Definitive Guide USA: O'Reilly, 2001.

[4] http://www.cisecurity.org/bench_linux.html including LinuxBenchmark.pdf and README found under CIS Security Benchmarks and Scoring Tools for Linux Level 1. (Authors: CIS Security, Title: CIS Security Benchmarks and Scoring Tools for Linux Level 1, Last Updated: Unknown, Date Accessed: Nov 2003)

[5] http://www.tripwire.org/qanda/index.php#1. (Authors: Tripwire.Org, Title: Tripwire Open Source, Linux Edition FAQ, Last Updated: Unknown, Date Accessed: Dec 2004)

[6] http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt. (Authors: linux.no, Title: Cross-Referencing Linux, Last Updated: 12/13/2001, Date Accessed: Dec 2004)

Appendix A: tripwire Policy File

```
##################################################################
##################################################################
################ #
#
#
#
#                  Policy file for Red Hat Linux
#
#                           V1.2.0rh
#
#                         August 9, 2001
#
#
#
##################################################################
#######

@@section GLOBAL
TWROOT=/usr/sbin;
TWBIN=/usr/sbin;
TWPOL="/etc/tripwire";
TWDB="/var/lib/tripwire";
TWSKEY="/etc/tripwire";
TWLKEY="/etc/tripwire";
TWREPORT="/var/lib/tripwire/report";
HOSTNAME=localhost;

@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;    # Critical files that cannot change
SEC_SUID      = $(IgnoreNone)-SHa ;    # Binaries with the SUID or SGID flags
set
SEC_BIN       = $(ReadOnly) ;                 # Binaries that should not change
SEC_CONFIG    = $(Dynamic) ;           # Config files that are changed
infrequently
SEC_LOG       = $(Growing) ;                  # Files that grow, but that should
never
                                       # change ownership.
SEC_INVARIANT = +tpug ;                # Directories that should never change
SIG_LOW       = 33 ;                   # Non-critical files with low security
impact
```

```
SIG_MED      = 66 ;                          # Non-critical files that are of significant
SIG_HI       = 100 ;

# Tripwire Binaries
(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
)
{
  $(TWBIN)/siggen                     -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                   -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                     -> $(SEC_BIN) ;
  $(TWBIN)/twprint                     -> $(SEC_BIN) ;
}

# Tripwire Data Files - Configuration Files, Policy Files, Keys, Reports,
Databases
(
  rulename = "Tripwire Data Files",
  severity = $(SIG_HI)
)
{

######################################################################
#####
  # NOTE: We remove the inode attribute because when Tripwire creates a
backup,
  # it does so by renaming the old file and creating a new one (which will
  # have a new inode number).  Inode is left turned on for keys, which shouldn't
  # ever change.

  # NOTE: The first integrity check triggers this rule and each integrity check
  # afterward triggers this rule until a database update is run, since the
  # database file does not exist before that point.

######################################################################
######

  $(TWDB)                                  -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol                          -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg                          -> $(SEC_BIN) -i ;
  # $(TWLKEY)/$(HOSTNAME)-local.key  -> $(SEC_BIN) ;
  $(TWSKEY)/site.key                       -> $(SEC_BIN) ;

  #don't scan the individual reports
  $(TWREPORT)                              -> $(SEC_CONFIG) (recurse=0) ;
```

```
}

# Tripwire HQ Connector Binaries
#(
#  rulename = "Tripwire HQ Connector Binaries",
#  severity = $(SIG_HI)
#)
#{
#  $(TWBIN)/hqagent                    -> $(SEC_BIN) ;
#}
#
# Tripwire HQ Connector - Configuration Files, Keys, and Logs

######################################################################
#########
# Note: File locations here are different than in a stock HQ Connector
# installation.  This is because Tripwire 2.3 uses a different path
# structure than Tripwire 2.2.1.
#
# You may need to update your HQ Agent configuation file (or this policy
# file) to correct the paths.  We have attempted to support the FHS standard
# here by placing the HQ Agent files similarly to the way Tripwire 2.3
# places them.
######################################################################
########
#(
#  rulename = "Tripwire HQ Connector Data Files",
#  severity = $(SIG_HI)
#)
#{
#
######################################################################
########

######################################################################
########
#  # NOTE: Removing the inode attribute because when Tripwire creates a
backup
#  # it does so by renaming the old file and creating a new one (which will
#  # have a new inode number).  Leaving inode turned on for keys, which
#  # shouldn't ever change.
######################################################################
########
#  $(TWBIN)/agent.cfg                  -> $(SEC_BIN) -i ;
#  $(TWLKEY)/authentication.key        -> $(SEC_BIN) ;
#  $(TWDB)/tasks.dat                   -> $(SEC_CONFIG) ;
#  $(TWDB)/schedule.dat                -> $(SEC_CONFIG) ;
#
#  # Uncomment if you have agent logging enabled.
#  #/var/log/tripwire/agent.log      -> $(SEC_LOG) ;
#}



# Commonly accessed directories that should remain static with regards to owner
and group
(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
)
{
  /                                -> $(SEC_INVARIANT) (recurse = 0) ;
  /home                               -> $(SEC_INVARIANT) (recurse = 0) ;
  /etc                              -> $(SEC_INVARIANT) (recurse = 0) ;
}

################################################
# File System and Disk Administration Programs
################################################

(
  rulename = "File System and Disk Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/badblocks                  -> $(SEC_CRIT) ;
  /sbin/convertquota                -> $(SEC_CRIT) ;
  /sbin/dosfsck                   -> $(SEC_CRIT) ;
  /sbin/debugfs                   -> $(SEC_CRIT) ;
  /sbin/debugreiserfs               -> $(SEC_CRIT) ;
  /sbin/dumpe2fs                   -> $(SEC_CRIT) ;
  # /sbin/e2fsadm                   -> $(SEC_CRIT) ; tune2fs?
  /sbin/e2fsck                   -> $(SEC_CRIT) ;
  /sbin/e2label                  -> $(SEC_CRIT) ;
  /sbin/fdisk                   -> $(SEC_CRIT) ;
  /sbin/fsck                    -> $(SEC_CRIT) ;
  /sbin/fsck.ext2                 -> $(SEC_CRIT) ;
  /sbin/fsck.ext3                 -> $(SEC_CRIT) ;
  /sbin/fsck.minix                -> $(SEC_CRIT) ;
  /sbin/fsck.msdos                  -> $(SEC_CRIT) ;
  /sbin/fsck.vfat                -> $(SEC_CRIT) ;
  /sbin/ftl_check                 -> $(SEC_CRIT) ;
```

```
/sbin/ftl_format                    -> $(SEC_CRIT) ;
/sbin/hdparm                        -> $(SEC_CRIT) ;
#/sbin/lvchange                     -> $(SEC_CRIT) ;
#/sbin/lvcreate                     -> $(SEC_CRIT) ;
#/sbin/lvdisplay                    -> $(SEC_CRIT) ;
#/sbin/lvextend                     -> $(SEC_CRIT) ;
#/sbin/lvmchange                    -> $(SEC_CRIT) ;
#/sbin/lvmcreate_initrd             -> $(SEC_CRIT) ;
#/sbin/lvmdiskscan                  -> $(SEC_CRIT) ;
#/sbin/lvmsadc                      -> $(SEC_CRIT) ;
#/sbin/lvmsar                       -> $(SEC_CRIT) ;
#/sbin/lvreduce                     -> $(SEC_CRIT) ;
#/sbin/lvremove                     -> $(SEC_CRIT) ;
#/sbin/lvrename                     -> $(SEC_CRIT) ;
#/sbin/lvscan                       -> $(SEC_CRIT) ;
/sbin/mkbootdisk                    -> $(SEC_CRIT) ;
/sbin/mkdosfs                       -> $(SEC_CRIT) ;
/sbin/mke2fs                        -> $(SEC_CRIT) ;
/sbin/mkfs                          -> $(SEC_CRIT) ;
/sbin/mkfs.bfs                      -> $(SEC_CRIT) ;
/sbin/mkfs.ext2                     -> $(SEC_CRIT) ;
/sbin/mkfs.minix                    -> $(SEC_CRIT) ;
/sbin/mkfs.msdos                    -> $(SEC_CRIT) ;
/sbin/mkfs.vfat                     -> $(SEC_CRIT) ;
/sbin/mkinitrd                      -> $(SEC_CRIT) ;
/sbin/mkraid                        -> $(SEC_CRIT) ;
/sbin/mkreiserfs                    -> $(SEC_CRIT) ;
/sbin/mkswap                        -> $(SEC_CRIT) ;
#/sbin/mtx                          -> $(SEC_CRIT) ;
/sbin/pam_console_apply             -> $(SEC_CRIT) ;
/sbin/parted                        -> $(SEC_CRIT) ;
/sbin/pcinitrd                      -> $(SEC_CRIT) ;
#/sbin/pvchange                     -> $(SEC_CRIT) ;
#/sbin/pvcreate                     -> $(SEC_CRIT) ;
#/sbin/pvdata                       -> $(SEC_CRIT) ;
#/sbin/pvdisplay                    -> $(SEC_CRIT) ;
#/sbin/pvmove                       -> $(SEC_CRIT) ;
#/sbin/pvscan                       -> $(SEC_CRIT) ;
/sbin/quotacheck                    -> $(SEC_CRIT) ;
/sbin/quotaon                       -> $(SEC_CRIT) ;
/sbin/raidstart                     -> $(SEC_CRIT) ;
/sbin/reiserfsck                    -> $(SEC_CRIT) ;
/sbin/resize2fs                     -> $(SEC_CRIT) ;
/sbin/resize_reiserfs               -> $(SEC_CRIT) ;
/sbin/scsi_info                     -> $(SEC_CRIT) ;
/sbin/sfdisk                        -> $(SEC_CRIT) ;
```

```
  /sbin/stinit           -> $(SEC_CRIT) ;
  #/sbin/tapeinfo           -> $(SEC_CRIT) ;
  /sbin/tune2fs            -> $(SEC_CRIT) ;
  /sbin/unpack             -> $(SEC_CRIT) ;
  /sbin/update             -> $(SEC_CRIT) ;
  #/sbin/vgcfgbackup          -> $(SEC_CRIT) ;
  #/sbin/vgcfgrestore         -> $(SEC_CRIT) ;
  #/sbin/vgchange            -> $(SEC_CRIT) ;
  #/sbin/vgck              -> $(SEC_CRIT) ;
  #/sbin/vgcreate           -> $(SEC_CRIT) ;
  #/sbin/vgdisplay          -> $(SEC_CRIT) ;
  #/sbin/vgexport           -> $(SEC_CRIT) ;
  #/sbin/vgextend            -> $(SEC_CRIT) ;
  #/sbin/vgimport           -> $(SEC_CRIT) ;
  #/sbin/vgmerge             -> $(SEC_CRIT) ;
  #/sbin/vgmknodes            -> $(SEC_CRIT) ;
  #/sbin/vgreduce            -> $(SEC_CRIT) ;
  #/sbin/vgremove            -> $(SEC_CRIT) ;
  #/sbin/vgrename             -> $(SEC_CRIT) ;
  #/sbin/vgscan             -> $(SEC_CRIT) ;
  #/sbin/vgsplit           -> $(SEC_CRIT) ;
  /bin/chgrp              -> $(SEC_CRIT) ;
  /bin/chmod               -> $(SEC_CRIT) ;
  /bin/chown               -> $(SEC_CRIT) ;
  /bin/cp              -> $(SEC_CRIT) ;
  /bin/cpio             -> $(SEC_CRIT) ;
  /bin/mount            -> $(SEC_CRIT) ;
  /bin/umount              -> $(SEC_CRIT) ;
  /bin/mkdir              -> $(SEC_CRIT) ;
  /bin/mknod               -> $(SEC_CRIT) ;
  /bin/mktemp              -> $(SEC_CRIT) ;
  /bin/rm                -> $(SEC_CRIT) ;
  /bin/rmdir             -> $(SEC_CRIT) ;
  /bin/touch              -> $(SEC_CRIT) ;
}
######################################
#  Kernel Administration Programs
####################################

(
  rulename = "Kernel Administration Programs",
  severity = $(SIG_HI)
)
{
  /sbin/ctrlaltdel        -> $(SEC_CRIT) ;
  /sbin/depmod              -> $(SEC_CRIT) ;
  /sbin/insmod                          -> $(SEC_CRIT) ;
  /sbin/insmod.static                   -> $(SEC_CRIT) ;
  /sbin/insmod_ksymoops_clean           -> $(SEC_CRIT) ;
  /sbin/klogd                           -> $(SEC_CRIT) ;
  /sbin/ldconfig                        -> $(SEC_CRIT) ;
  /sbin/minilogd                        -> $(SEC_CRIT) ;
  /sbin/modinfo                         -> $(SEC_CRIT) ;
  /sbin/pivot_root                      -> $(SEC_CRIT) ;
  /sbin/sndconfig                       -> $(SEC_CRIT) ;
  /sbin/sysctl                          -> $(SEC_CRIT) ;
}

################################################
# Networking Programs
################################################

(
  rulename = "Networking Programs",
  severity = $(SIG_HI)
)
{
  /etc/sysconfig/network-scripts/ifdown                 -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-cipcb           -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ippp            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ipv6            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-isdn            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-post            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-ppp             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-sit             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifdown-sl              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup                   -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-aliases           -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-cipcb             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ippp              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ipv6              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-isdn              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-plip              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-plusb             -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-post              -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-ppp               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-routes            -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-sit               -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-sl                -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/ifup-wireless          -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/network-functions      -> $(SEC_CRIT) ;
  /etc/sysconfig/network-scripts/network-functions-ipv6  -> $(SEC_CRIT) ;
  /bin/ping                    -> $(SEC_CRIT) ;
  /sbin/agetty                 -> $(SEC_CRIT) ;
  /sbin/arp                    -> $(SEC_CRIT) ;
  /sbin/arping                 -> $(SEC_CRIT) ;
  /sbin/dhcpcd                 -> $(SEC_CRIT) ;
  /sbin/ether-wake             -> $(SEC_CRIT) ;
  #/sbin/getty                 -> $(SEC_CRIT) ;
  /sbin/ifcfg                  -> $(SEC_CRIT) ;
  /sbin/ifconfig               -> $(SEC_CRIT) ;
  /sbin/ifdown                 -> $(SEC_CRIT) ;
  /sbin/ifenslave              -> $(SEC_CRIT) ;
  /sbin/ifport                 -> $(SEC_CRIT) ;
  /sbin/ifup                   -> $(SEC_CRIT) ;
  /sbin/ifuser                 -> $(SEC_CRIT) ;
  /sbin/ip                     -> $(SEC_CRIT) ;
  /sbin/ipchains               -> $(SEC_CRIT) ;
  /sbin/ipchains-restore       -> $(SEC_CRIT) ;
  /sbin/ipchains-save          -> $(SEC_CRIT) ;
  /sbin/ipfwadm                -> $(SEC_CRIT) ;
  /sbin/ipmaddr                -> $(SEC_CRIT) ;
  /sbin/iptables               -> $(SEC_CRIT) ;
  /sbin/iptables-restore       -> $(SEC_CRIT) ;
  /sbin/iptables-save          -> $(SEC_CRIT) ;
  /sbin/iptunnel               -> $(SEC_CRIT) ;
  /sbin/nameif                 -> $(SEC_CRIT) ;
  /sbin/netreport              -> $(SEC_CRIT) ;
  /sbin/plipconfig             -> $(SEC_CRIT) ;
  /sbin/portmap                -> $(SEC_CRIT) ;
  /sbin/ppp-watch              -> $(SEC_CRIT) ;
  #/sbin/rarp                  -> $(SEC_CRIT) ;
  /sbin/route                  -> $(SEC_CRIT) ;
  /sbin/slattach               -> $(SEC_CRIT) ;
  /sbin/tc                     -> $(SEC_CRIT) ;
  #/sbin/uugetty               -> $(SEC_CRIT) ;
  /sbin/ypbind                 -> $(SEC_CRIT) ;
}


######################################
#  System Administration Programs
#
######################################


(
  rulename = "System Administration Programs",
  severity = $(SIG_HI)
```

```
)
{
  /sbin/chkconfig                    -> $(SEC_CRIT) ;
  /sbin/fuser                      -> $(SEC_CRIT) ;
  /sbin/halt                      -> $(SEC_CRIT) ;
  /sbin/init                     -> $(SEC_CRIT) ;
  /sbin/initlog                    -> $(SEC_CRIT) ;
  /sbin/install-info                -> $(SEC_CRIT) ;
  /sbin/killall5                  -> $(SEC_CRIT) ;
  /sbin/pam_tally                    -> $(SEC_CRIT) ;
  /sbin/pwdb_chkpwd                     -> $(SEC_CRIT) ;
  /sbin/rescuept                    -> $(SEC_CRIT) ;
  /sbin/rmt                       -> $(SEC_CRIT) ;
  /sbin/rpc.lockd                   -> $(SEC_CRIT) ;
  /sbin/rpc.statd                  -> $(SEC_CRIT) ;
  /sbin/rpcdebug                     -> $(SEC_CRIT) ;
  /sbin/service                    -> $(SEC_CRIT) ;
  /sbin/setsysfont                   -> $(SEC_CRIT) ;
  /sbin/shutdown                     -> $(SEC_CRIT) ;
  /sbin/sulogin                    -> $(SEC_CRIT) ;
  /sbin/swapon                      -> $(SEC_CRIT) ;
  /sbin/syslogd                    -> $(SEC_CRIT) ;
  /sbin/unix_chkpwd                    -> $(SEC_CRIT) ;
  /bin/pwd                       -> $(SEC_CRIT) ;
  /bin/uname                       -> $(SEC_CRIT) ;
}

##############################################
# Hardware and Device Control Programs
##############################################
(
  rulename = "Hardware and Device Control Programs",
  severity = $(SIG_HI)
)
{
  /bin/setserial                   -> $(SEC_CRIT) ;
  /bin/sfxload                     -> $(SEC_CRIT) ;
  /sbin/blockdev                     -> $(SEC_CRIT) ;
  /sbin/cardctl                    -> $(SEC_CRIT) ;
  /sbin/cardmgr                      -> $(SEC_CRIT) ;
  /sbin/dump_cis                      -> $(SEC_CRIT) ;
  /sbin/elvtune                     -> $(SEC_CRIT) ;
  /sbin/hotplug                     -> $(SEC_CRIT) ;
  /sbin/hwclock                      -> $(SEC_CRIT) ;
  /sbin/ide_info                    -> $(SEC_CRIT) ;
  /sbin/kbdrate                     -> $(SEC_CRIT) ;
  /sbin/losetup                        -> $(SEC_CRIT) ;
  /sbin/lspci                        -> $(SEC_CRIT) ;
  /sbin/lspnp                        -> $(SEC_CRIT) ;
  /sbin/mii-tool                     -> $(SEC_CRIT) ;
  /sbin/pack_cis                       -> $(SEC_CRIT) ;
  /sbin/probe                         -> $(SEC_CRIT) ;
  /sbin/setpci                       -> $(SEC_CRIT) ;
}

###################################
#  System Information Programs
###################################
(
  rulename = "System Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/consoletype                   -> $(SEC_CRIT) ;
  /sbin/kernelversion                 -> $(SEC_CRIT) ;
  /sbin/runlevel                    -> $(SEC_CRIT) ;
}


#######################################
# Application Information Programs
#######################################

(
  rulename = "Application Information Programs",
  severity = $(SIG_HI)
)
{
  /sbin/genksyms                      -> $(SEC_CRIT) ;
  /sbin/rtmon                        -> $(SEC_CRIT) ;
}

#############################
#  Shell Related Programs
#############################
(
  rulename = "Shell Related Programs",
  severity = $(SIG_HI)
)
{
  /sbin/getkey                       -> $(SEC_CRIT) ;
  /sbin/nash                         -> $(SEC_CRIT) ;
```

```
}


##########################
#  OS Utilities
##########################
(
  rulename = "Operating System Utilities",
  severity = $(SIG_HI)
)
{
  /bin/arch                        -> $(SEC_CRIT) ;
  /bin/ash                         -> $(SEC_CRIT) ;
  /bin/ash.static                  -> $(SEC_CRIT) ;
  /bin/aumix-minimal               -> $(SEC_CRIT) ;
  /bin/basename                    -> $(SEC_CRIT) ;
  /bin/cat                         -> $(SEC_CRIT) ;
  /bin/consolechars                -> $(SEC_CRIT) ;
  /bin/cut                         -> $(SEC_CRIT) ;
  /bin/date                        -> $(SEC_CRIT) ;
  /bin/dd                          -> $(SEC_CRIT) ;
  /bin/df                          -> $(SEC_CRIT) ;
  /bin/dmesg                       -> $(SEC_CRIT) ;
  /bin/doexec                      -> $(SEC_CRIT) ;
  /bin/echo                        -> $(SEC_CRIT) ;
  /bin/ed                          -> $(SEC_CRIT) ;
  /bin/egrep                       -> $(SEC_CRIT) ;
  /bin/false                       -> $(SEC_CRIT) ;
  /bin/fgrep                       -> $(SEC_CRIT) ;
  /bin/gawk                        -> $(SEC_CRIT) ;
  /bin/gawk-3.1.0                  -> $(SEC_CRIT) ;
  /bin/grep                        -> $(SEC_CRIT) ;
  /bin/gunzip                      -> $(SEC_CRIT) ;
  /bin/gzip                        -> $(SEC_CRIT) ;
  /bin/hostname                    -> $(SEC_CRIT) ;
  /bin/igawk                       -> $(SEC_CRIT) ;
  /bin/ipcalc                      -> $(SEC_CRIT) ;
  /bin/kill                        -> $(SEC_CRIT) ;
  /bin/ln                          -> $(SEC_CRIT) ;
  /bin/loadkeys                    -> $(SEC_CRIT) ;
  /bin/login                       -> $(SEC_CRIT) ;
  /bin/ls                          -> $(SEC_CRIT) ;
  /bin/mail                        -> $(SEC_CRIT) ;
  /bin/more                        -> $(SEC_CRIT) ;
  /bin/mt                          -> $(SEC_CRIT) ;
  /bin/mv                          -> $(SEC_CRIT) ;
  /bin/netstat                        -> $(SEC_CRIT) ;
  /bin/nice                           -> $(SEC_CRIT) ;
  /bin/pgawk                          -> $(SEC_CRIT) ;
  /bin/ps                             -> $(SEC_CRIT) ;
  /bin/rpm                            -> $(SEC_CRIT) ;
  /bin/sed                            -> $(SEC_CRIT) ;
  /bin/sleep                          -> $(SEC_CRIT) ;
  /bin/sort                           -> $(SEC_CRIT) ;
  /bin/stty                           -> $(SEC_CRIT) ;
  /bin/su                             -> $(SEC_CRIT) ;
  /bin/sync                           -> $(SEC_CRIT) ;
  /bin/tar                            -> $(SEC_CRIT) ;
  /bin/true                           -> $(SEC_CRIT) ;
  /bin/usleep                         -> $(SEC_CRIT) ;
  /bin/vi                             -> $(SEC_CRIT) ;
  /bin/zcat                           -> $(SEC_CRIT) ;
  /sbin/sln                           -> $(SEC_CRIT) ;
}

##################################
#  Critical Utility Sym-Links
##################################
(
  rulename = "Critical Utility Sym-Links",
  severity = $(SIG_HI)
)
{
  /sbin/clock                         -> $(SEC_CRIT) ;
  /sbin/fsck.reiserfs                 -> $(SEC_CRIT) ;
  /sbin/ipfwadm-wrapper               -> $(SEC_CRIT) ;
  /sbin/kallsyms                      -> $(SEC_CRIT) ;
  /sbin/ksyms                         -> $(SEC_CRIT) ;
  /sbin/lsmod                         -> $(SEC_CRIT) ;
  /sbin/mkfs.reiserfs                 -> $(SEC_CRIT) ;
  /sbin/modprobe                      -> $(SEC_CRIT) ;
  /sbin/pidof                         -> $(SEC_CRIT) ;
  /sbin/poweroff                      -> $(SEC_CRIT) ;
  /sbin/quotaoff                      -> $(SEC_CRIT) ;
  /sbin/raid0run                      -> $(SEC_CRIT) ;
  /sbin/raidhotadd                    -> $(SEC_CRIT) ;
  /sbin/raidhotgenerateerror          -> $(SEC_CRIT) ;
  /sbin/raidhotremove                 -> $(SEC_CRIT) ;
  /sbin/raidstop                      -> $(SEC_CRIT) ;
  /sbin/reboot                        -> $(SEC_CRIT) ;
  /sbin/rmmod                         -> $(SEC_CRIT) ;
  /sbin/swapoff                       -> $(SEC_CRIT) ;
  /sbin/telinit                    -> $(SEC_CRIT) ;
  /bin/awk                          -> $(SEC_CRIT) ;
  /bin/bash2                         -> $(SEC_CRIT) ;
  /bin/bsh                          -> $(SEC_CRIT) ;
  /bin/csh                          -> $(SEC_CRIT) ;
  /bin/dnsdomainname                     -> $(SEC_CRIT) ;
  /bin/domainname                      -> $(SEC_CRIT) ;
  /bin/ex                          -> $(SEC_CRIT) ;
  /bin/gtar                        -> $(SEC_CRIT) ;
  /bin/nisdomainname                     -> $(SEC_CRIT) ;
  /bin/red                         -> $(SEC_CRIT) ;
  /bin/rvi                        -> $(SEC_CRIT) ;
  /bin/rview                        -> $(SEC_CRIT) ;
  /bin/view                         -> $(SEC_CRIT) ;
  /bin/ypdomainname                     -> $(SEC_CRIT) ;
}


##############################
#  Temporary directories
##############################
(
  rulename = "Temporary directories",
  recurse = false,
  severity = $(SIG_LOW)
)
{
  /usr/tmp                          -> $(SEC_INVARIANT) ;
  /var/tmp                          -> $(SEC_INVARIANT) ;
  /tmp                            -> $(SEC_INVARIANT) ;
}

#################
#  Local files
#################
(
  rulename = "User binaries",
  severity = $(SIG_MED)
)
{
  /sbin                           -> $(SEC_BIN) (recurse = 1) ;
  /usr/bin                         -> $(SEC_BIN) (recurse = 1) ;
  /usr/sbin                         -> $(SEC_BIN) (recurse = 1) ;
  /usr/local/bin                      -> $(SEC_BIN) (recurse = 1) ;
}
```

```
(
  rulename = "Shell Binaries",
  severity = $(SIG_HI)
)
{
  /bin/bash                          -> $(SEC_BIN) ;
  # /bin/psh                          -> $(SEC_BIN) ; # No longer used?
  # /bin/Rsh                          -> $(SEC_BIN) ; # No longer used?
  /bin/sh                            -> $(SEC_BIN) ;
  # /bin/shell                        -> $(SEC_SUID) ; # No longer used?
  # /bin/tsh                          -> $(SEC_BIN) ; # No longer used?
  /bin/tcsh                          -> $(SEC_BIN) ;
  /sbin/nologin                       -> $(SEC_BIN) ;
}

(
  rulename = "Security Control",
  severity = $(SIG_HI)
)
{
  /etc/group                         -> $(SEC_CRIT) ;
  /etc/security                      -> $(SEC_CRIT) ;
  #/var/spool/cron/crontabs              -> $(SEC_CRIT) ; # Uncomment when this file
exists
}

#(
#  rulename = "Boot Scripts",
#  severity = $(SIG_HI)
#)
#{
#  /etc/rc                           -> $(SEC_CONFIG) ;
#  /etc/rc.bsdnet                     -> $(SEC_CONFIG) ;
#  /etc/rc.dt                         -> $(SEC_CONFIG) ;
#  /etc/rc.net                        -> $(SEC_CONFIG) ;
#  /etc/rc.net.serial                  -> $(SEC_CONFIG) ;
#  /etc/rc.nfs                        -> $(SEC_CONFIG) ;
#  /etc/rc.powerfail                   -> $(SEC_CONFIG) ;
#  /etc/rc.tcpip                      -> $(SEC_CONFIG) ;
#  /etc/trcfmt.Z                      -> $(SEC_CONFIG) ;
#}

(
  rulename = "Login Scripts",
  severity = $(SIG_HI)
)
```

```
{
  /etc/bashrc                          -> $(SEC_CONFIG) ;
  /etc/csh.cshrc                        -> $(SEC_CONFIG) ;
  /etc/csh.login                       -> $(SEC_CONFIG) ;
  /etc/inputrc                        -> $(SEC_CONFIG) ;
  # /etc/tsh_profile                        -> $(SEC_CONFIG) ; #Uncomment when this file
exists
  /etc/profile                        -> $(SEC_CONFIG) ;
}

# Libraries
(
  rulename = "Libraries",
  severity = $(SIG_MED)
)
{
  /usr/lib                          -> $(SEC_BIN) ;
  /usr/local/lib                      -> $(SEC_BIN) ;
}


##############################################################
#  Critical System Boot Files
#  These files are critical to a correct system boot.
##############################################################

(
  rulename = "Critical system boot files",
  severity = $(SIG_HI)
)
{
     /boot                         -> $(SEC_CRIT) ;
     #/sbin/devfsd                        -> $(SEC_CRIT) ;
     /sbin/grub                       -> $(SEC_CRIT) ;
     /sbin/grub-install                 -> $(SEC_CRIT) ;
     /sbin/grub-md5-crypt                   -> $(SEC_CRIT) ;
     /sbin/installkernel                 -> $(SEC_CRIT) ;
     /sbin/lilo                    -> $(SEC_CRIT) ;
     /sbin/mkkerneldoth                   -> $(SEC_CRIT) ;
     !/boot/System.map ;
     !/boot/module-info ;
}

  #########################################################
  # These files change every time the system boots
  ########################################################
```

```
(
  rulename = "System boot changes",
  severity = $(SIG_HI)
)
{
    !/var/run/ftp.pids-all ; # Comes and goes on reboot.
    !/root/.enlightenment ;
    /dev/log                      -> $(SEC_CONFIG) ;
    /dev/cua0                      -> $(SEC_CONFIG) ;
    # /dev/printer                  -> $(SEC_CONFIG) ; # Uncomment if you have a
printer device
    /dev/console                   -> $(SEC_CONFIG) -u ; # User ID may change on
console login/logout.
    /dev/tty1                     -> $(SEC_CONFIG) ; # tty devices
    /dev/tty2                     -> $(SEC_CONFIG) ; # tty devices
    /dev/tty3                     -> $(SEC_CONFIG) ; # are extremely
    /dev/tty4                     -> $(SEC_CONFIG) ; # variable
    /dev/tty5                     -> $(SEC_CONFIG) ;
    /dev/tty6                     -> $(SEC_CONFIG) ;
    /dev/urandom                    -> $(SEC_CONFIG) ;
    /dev/initctl                  -> $(SEC_CONFIG) ;
    /var/lock/subsys                -> $(SEC_CONFIG) ;
    /var/lock/subsys/anacron         -> $(SEC_CONFIG) ;
    /var/lock/subsys/apmd           -> $(SEC_CONFIG) ;
    /var/lock/subsys/atd           -> $(SEC_CONFIG) ;
    /var/lock/subsys/crond          -> $(SEC_CONFIG) ;
    /var/lock/subsys/gpm            -> $(SEC_CONFIG) ;
    /var/lock/subsys/keytable       -> $(SEC_CONFIG) ;
    /var/lock/subsys/kudzu          -> $(SEC_CONFIG) ;
    /var/lock/subsys/netfs         -> $(SEC_CONFIG) ;
    /var/lock/subsys/network         -> $(SEC_CONFIG) ;
    /var/lock/subsys/nfslock        -> $(SEC_CONFIG) ;
    /var/lock/subsys/pcmcia          -> $(SEC_CONFIG) ;
    /var/lock/subsys/portmap         -> $(SEC_CONFIG) ;
    /var/lock/subsys/random          -> $(SEC_CONFIG) ;
    /var/lock/subsys/sendmail        -> $(SEC_CONFIG) ;
    /var/lock/subsys/sshd           -> $(SEC_CONFIG) ;
    /var/lock/subsys/syslog          -> $(SEC_CONFIG) ;
    /var/lock/subsys/xfs           -> $(SEC_CONFIG) ;
    /var/run                      -> $(SEC_CONFIG) ;
    /var/log                      -> $(SEC_CONFIG) ;
    /etc/ioctl.save                -> $(SEC_CONFIG) ;
    /etc/issue.net                  -> $(SEC_CONFIG) -i ; # Inode number changes
    /etc/issue                    -> $(SEC_CONFIG) ;
    /etc/mtab                      -> $(SEC_CONFIG) -i ; # Inode number changes on
any mount/unmount
```

```
    /lib/modules                    -> $(SEC_CONFIG) ;
    /etc/.pwd.lock                  -> $(SEC_CONFIG) ;
    # /lib/modules/preferred              -> $(SEC_CONFIG) ; #Uncomment when this
file exists
}

# These files change the behavior of the root account
(
  rulename = "Root config files",
  severity = 100
)
{
    /root                          -> $(SEC_CRIT) ; # Catch all additions to /root
    /root/.Xresources                   -> $(SEC_CONFIG) ;
    /root/.bashrc                   -> $(SEC_CONFIG) ;
    /root/.bash_profile                 -> $(SEC_CONFIG) ;
    /root/.bash_logout                  -> $(SEC_CONFIG) ;
    /root/.cshrc                   -> $(SEC_CONFIG) ;
    /root/.tcshrc                  -> $(SEC_CONFIG) ;
    /root/.bash_history                 -> $(SEC_CONFIG) ;
    /root/.esd_auth                    -> $(SEC_CONFIG) ;
    /root/.gnome_private                  -> $(SEC_CONFIG) ;
    /root/.gnome                    -> $(SEC_CONFIG) ;
}

################################
# Critical configuration files
################################
(
  rulename = "Critical configuration files",
  severity = $(SIG_HI)
)
{
    /etc/crontab                   -> $(SEC_BIN) ;
    /etc/cron.hourly                  -> $(SEC_BIN) ;
    /etc/cron.daily                  -> $(SEC_BIN) ;
    /etc/cron.weekly                    -> $(SEC_BIN) ;
    /etc/cron.monthly                   -> $(SEC_BIN) ;
    /etc/default                   -> $(SEC_BIN) ;
    /etc/fstab                    -> $(SEC_BIN) ;
    /etc/exports                   -> $(SEC_BIN) ;
    /etc/group-                   -> $(SEC_BIN) ;  # changes should be infrequent
    /etc/host.conf                   -> $(SEC_BIN) ;
    /etc/hosts.allow                   -> $(SEC_BIN) ;
    /etc/hosts.deny                    -> $(SEC_BIN) ;
    /etc/protocols                   -> $(SEC_BIN) ;
    /etc/services                    -> $(SEC_BIN) ;
    /etc/rc.d/init.d                -> $(SEC_BIN) ;
    /etc/rc.d                      -> $(SEC_BIN) ;
    /etc/mail.rc                    -> $(SEC_BIN) ;
    /etc/modules.conf                  -> $(SEC_BIN) ;
    /etc/motd                       -> $(SEC_BIN) ;
    /etc/passwd                       -> $(SEC_CONFIG) ;
    /etc/passwd-                      -> $(SEC_CONFIG) ;
    /etc/profile.d                  -> $(SEC_BIN) ;
    /var/lib/nfs/rmtab                -> $(SEC_BIN) ;
    /etc/rpc                       -> $(SEC_BIN) ;
    /etc/sysconfig                    -> $(SEC_BIN) ;
    #/etc/gettydefs                    -> $(SEC_BIN) ;
    /etc/nsswitch.conf                 -> $(SEC_BIN) ;
    /etc/yp.conf                     -> $(SEC_BIN) ;
    /etc/hosts                      -> $(SEC_CONFIG) ;
    /etc/inittab                   -> $(SEC_CONFIG) ;
    /etc/resolv.conf                  -> $(SEC_CONFIG) ;
    /etc/syslog.conf                   -> $(SEC_CONFIG) ;
}

######################
# Critical devices
######################
(
  rulename = "Critical devices",
  severity = $(SIG_HI),
  recurse = false
)
{
    /dev/kmem                         -> $(Device) ;
    /dev/mem                         -> $(Device) ;
    /dev/null                      -> $(Device) ;
    /dev/zero                       -> $(Device) ;
    /proc/devices                     -> $(Device) ;
    /proc/net                       -> $(Device) ;
    /proc/sys                       -> $(Device) ;
    /proc/cpuinfo                    -> $(Device) ;
    /proc/modules                      -> $(Device) ;
    /proc/mounts                      -> $(Device) ;
    /proc/dma                        -> $(Device) ;
    /proc/filesystems                  -> $(Device) ;
    /proc/pci                      -> $(Device) ;
    /proc/interrupts                  -> $(Device) ;
    /proc/driver/rtc                -> $(Device) ;
    /proc/ioports                   -> $(Device) ;
    /proc/kcore                    -> $(Device) ;
    /proc/self                   -> $(Device) ;
    /proc/kmsg                     -> $(Device) ;
    /proc/stat                   -> $(Device) ;
    /proc/ksyms                    -> $(Device) ;
    /proc/loadavg                  -> $(Device) ;
    /proc/uptime                   -> $(Device) ;
    /proc/locks                   -> $(Device) ;
    /proc/version                  -> $(Device) ;
    /proc/mdstat                   -> $(Device) ;
    /proc/meminfo                    -> $(Device) ;
    /proc/cmdline                  -> $(Device) ;
    /proc/misc                    -> $(Device) ;
}

# Rest of critical system binaries
(
  rulename = "OS executables and libraries",
  severity = $(SIG_HI)
)
{
    /bin                          -> $(SEC_BIN) ;
    /lib                         -> $(SEC_BIN) ;
}

# vsftpd critical system files
(
        rulename = "vsftpd executables and conf files",
        severity = $(SIG_HI)
)
{
        /etc/logrotate.d/vsftpd.log   -> $(SEC_BIN) ;



        /etc/pam.d/vsftpd             -> $(SEC_BIN) ;
        /etc/vsftpd.conf              -> $(SEC_BIN) ;
        /etc/vsftpd.ftpusers          -> $(SEC_BIN) ;
        /etc/vsftpd.user_list         -> $(SEC_BIN) ;
        /usr/sbin/vsftpd              -> $(SEC_BIN) ;
}
```

Appendix B: SSHD Configuration Options

Setting	Value	Comments
Protocol	2	Don't fallback to Protocol 1. Version 1 has a number of security related vulnerabilities.
SysLogFacility	Auth	Enable AuthPriv for Linux
PermitRootLogin	No	Don't allow root account to login remotely via SSH.
AllowEmptyPasswords	no	This will require a password for access to the system.
IgnoreRhosts	yes	Don't allow rhost compatibility.
RHostsAuthentication	no	Don't permit RHosts based Authentication
RhostsRSAAuthentication	no	Don't permit RhostsRSA authentication
HostBasedAuthentication	no	Don't permit HostBased Authentication
AllowUsers	ftpadmin	Only permit the ftpadmin account SSH access to the server.
AllowHosts	168.4.80.10	Only permit 168.4.80.10 workstation to connect to our SSH Server.

Appendix C: vsftpd Configuration File

```
# vsftpd.conf
#
# Allow anonymous FTP?
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=NO
#
# Uncomment this to enable any form of FTP write command.
write_enable=NO
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=NO
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=NO
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=NO
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
log_ftp_protocol = yes
pam_service_name=vsftpd
listen=no
# Our FTP Banner
ftpd_banner=Welcome to ABC Corporations FTP service. Authorized Access Only!
```

Appendix D: CIS-Benchmark Install Script

```
#!/bin/sh
########################################################
# Shell Script to download the CIS-Benchmark Toolkit                ##
# For Linux and to verify MD5 checksum                               ##
#######################################################
cd /tmp
URLPATH="http://cisecurity.org/tools2/linux/"
CIS_PACKAGE="cis-linux.tar.gz"
MD5FILE="cis-linux_tgz_md5.txt"

wget ${URLPATH}${CIS_PACKAGE}
wget ${URLPATH}${MD5FILE}

MD5HASH=`cat /tmp/cis-linux_tgz_md5.txt | awk '{print $1}'`
CISHASH=`md5sum /tmp/cis-linux.tar.gz | awk '{print $1}'`

if [ $MD5HASH == $CISHASH ]; then
  echo "Package Validated with Md5sum..."
  tar -xvzf $CIS_PACKAGE
  if [ -d cis ]; then
     cd cis
  else
     echo "Package didn't extract."
  fi
fi
```