Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Secure Small Business Samba File and Print Server

Troy D. Smith
August 18, 2004

GIAC Certified UNIX Security Administrator (GCUX)
Practical Assignment
Version 2.1, Option 1

Table of Contents

Tables

Table of Figures

1.0   Abstract

Large, established corporations often have a dedicated budget to create, secure, and maintain a state-of-the-art business network. Organizational charts for companies such as these often include several levels for each department, including Information Technology (IT). With the employ of an IT staff, a significant percentage of the annual budget is carved out for the acquisition of new equipment and software, as well as the maintenance and upgrade of existing resources. However, for the small independent business with modest profit margins, IT departments and technology budgets usually do not exist.

With the small independent business in mind, this paper illustrates the installation, hardening, and ongoing maintenance of a secure file and print server using Samba[1] on a Linux operating system (OS). The target audience typifies the small business entrepreneur whose monetary resources are limited and whose Linux skill set falls between elementary and intermediate. The focus is on building and maintaining a secure Samba file and print server in a small, multiplatform environment. The company and scenario represented in this paper are fictitious, although a live network has been built and configured for demonstration.

2.0   Introduction

2.1   Sample Company Existing Network Infrastructure

Hardwood Furniture Manufacturing (HFM) is a small, independently owned custom furniture manufacturer. The product line ranges from a regular catalogue of about thirty standard models to custom-built pieces designed on-site per client specifications. The staff is comprised of the owner, one shop manager, two floor managers, and fifteen shop employees. The current technology inventory consists of the following:

- 1 – Microsoft Windows desktop
- 1 – Microsoft Windows laptop
- 1 – Hewlett Packard multifunction printer

The printer, which is not network compatible, is connected locally to the Windows desktop. The two computers are connected to a Netgear RP614 router, although file sharing is not enabled. Any files created on the laptop are copied to disk, then either copied to or printed from the desktop. Internet connectivity and email are provided through a local cable ISP. The router is connected to the cable modem, providing IP addressing for the computers via Network Address Translation (NAT). By using NAT to supply IP addresses, the router also acts as a firewall, protecting the computers from direct Internet access. The owner and

---

[1] Samba

the managers share the two computers.   Data storage is unstructured and unorganized, although low level tape backups are occasionally performed using an internal tape drive on the desktop.
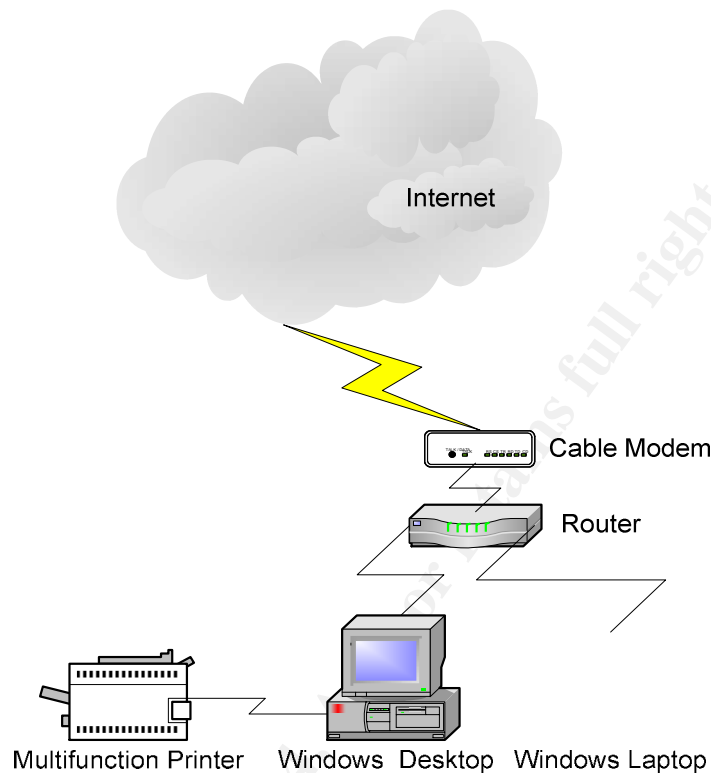
Figure 1 – Existing Company Network Infrastructure

2.2   Sample Company Proposed Network Infrastructure

HFM has decided to gradually expand the company network to facilitate an organized data structure, centralized data storage, and effortless file sharing and printing. The overall requirements are to create and maintain a functional and secure network within an extremely limited budget. The basic hardware requirements suitable for this environment include a separate file and print server, one laptop, two desktops, and a multifunction printer. Internet access and email services will continue to be provided through the existing local cable ISP. The router will remain a part of the infrastructure and continue to provide NAT and firewall services to the network. Considering the minimal budget to create and maintain the proposed network infrastructure, the hardware and software purchasing decisions will be economical and firm.

Taking into account the relatively minor amount of data that will initially be stored on the server, the preliminary build will begin with a small yet scalable desktop computer. The additional desktop that will be added to the network is a personal

As part of GIAC practical repository.

home computer that has been donated. To trim current and future costs, HFM will gradually transition the entire network to open source software. Linux will be the OS of both the server and the desktop that has been added to the network. The Linux OS will be procured directly from a vendor along with a basic support contract.
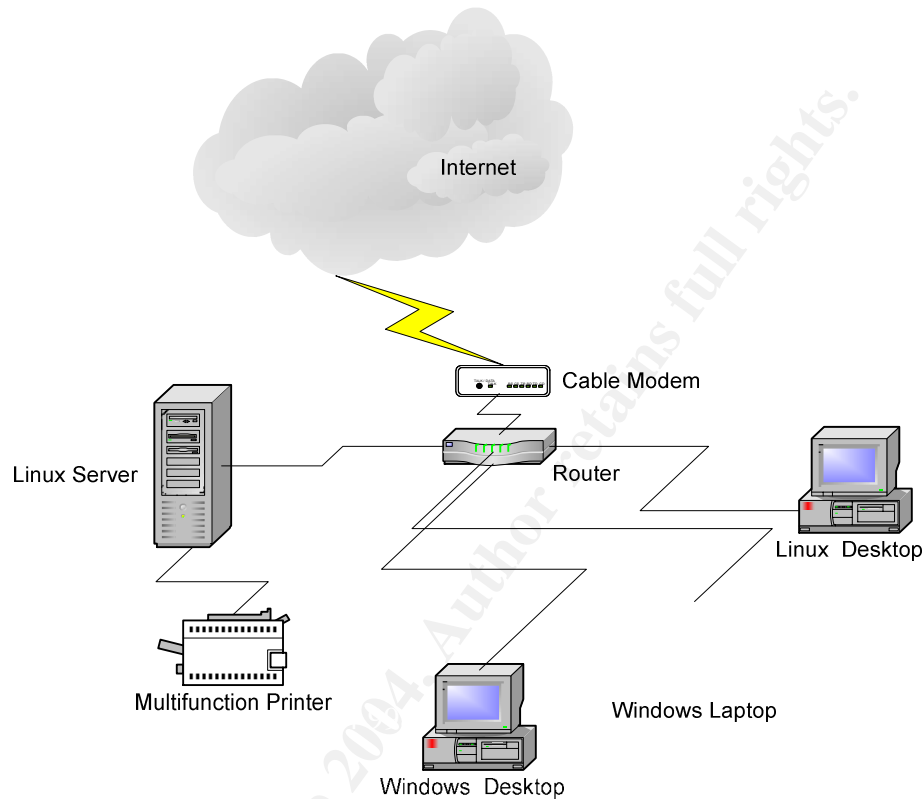
Figure 2 – Proposed Company Network Infrastructure

3.0   System Specification

3.1   *Purpose*

The purpose of this system is to provide secure file and print services to a small network. Considering the limited use the server will initially encounter, a small desktop will prove more than adequate. The server is expected to run with the specified hardware configuration for the first six months, after which the memory will be upgraded and a second drive will be added for redundancy. Additional drive space will be added as needed, and the server will be replaced upon expiration of the planned two-year life cycle.

3.2   *System Hardware Specification*

3.2.1   *Base System*

Given the [$1,000.00 budget for the server hardware], a Dell[2] Dimension 4600 has been procured.   The Dimension 4600 represents a reliable and scalable computer that may be built with durable, high-performance components while keeping the initial costs within budget. The components purchased with this budget include:

- 3.06ghz CPU, 533 front side bus, hyper threading enabled
- 512mb DDR RAM, 333mhz, dual channel
- 120gb SATA hard drive
- 1.44mb floppy drive
- Standard 40x CDROM drive
- Intel 10/100 NIC

3.2.2   Removable Media

Instead of a CDRW or DVD recorder, a standard CDROM has been purchased. A CDRW or DVD recorder raises the security concern that large files or a large amount of data can be recorded to CD or DVD media and easily removed from the premises. Even though some files are small enough to be copied to a floppy disk, the extra level of system recovery a floppy drive provides justifies its existence.

3.2.3   Projected Upgrades

The processor speed chosen is more than satisfactory for the projected level of utilization, and should prove adequate throughout the server's life cycle. A planned memory upgrade six months after the server goes into production has already been added to the projected budget. A second 120 GB hard drive will also be installed at the six-month mark to add an additional level of redundancy. Although a local backup is generally more secure than a remote backup, the data backups will be executed remotely from the Linux desktop. This is necessary because the chosen open source backup product requires services that will not be installed on the server.

3.3   System Software Specification

3.3.1   Operating System

Red Hat Enterprise Linux ES 3.0 (RHEL ES 3)[3] will be installed on the server. Red Hat was chosen based on stability, support, and overall reputation. Another contributing factor to the decision is the level of familiarity HFM has with Red Hat, compared to other distributions. To ensure the use of an authentic Red Hat OS,

---

[2] Dell
[3] Red Hat Enterprise Linux

HFM purchased a one-year basic support contract from Red Hat that includes installation media. The basic support includes access to the Red Hat Network (RHN), at www.rhn.redhat.com,[4] for online support and OS updates. HFM is primarily interested in the security updates, and although they may be downloaded from any number of Web sites, it is prudent to obtain and install updates from the OS vendor to guarantee compatibility and authenticity. Even though HFM will download the packages from the vendor Website, they should continue to verify the packages using the provided MD5 SUM. "MD5 Sums are 32 byte character strings that are the result of running the MD5 sum program against a particular file. Since any difference between two files results in two different strings, MD5's can be used to determine that the downloaded file is a bit-for-bit copy of the remote file."[5] The support contract also includes email notification of security vulnerabilities and patch availability. The cost of the authentic OS installation media and support contract is just below $400.00.

3.3.2   Samba

Building a Linux file and print server in a Windows environment necessitates installing and configuring Samba. Microsoft Windows uses the Server Message Block (SMB) protocol for file and printer sharing. SMB typifies a client-server protocol, and uses NetBIOS over TCP/IP for client connections.[6] "Samba is a suite of UNIX applications that speak the [SMB] protocol. By supporting this protocol, Samba enables computers running UNIX to get in on the action, communicating with the same networking protocol as Microsoft Windows and appearing as another Windows system on the network from the perspective of a Windows client."[7] A Samba server utilizes user-level access security by default, and may be configured as a Primary Domain Controller (PDC) in a Microsoft Windows environment. However, unlike SMB file and printer server alternatives, Samba may be obtained and used at no cost and is included with the OS distribution media. Samba 3.0.0-14.3 currently ships with RHEL ES 3.

3.3.3   Security

The server's primary function is to provide file and print services, therefore minimal amount of software will initially be installed. However, to assist with the configuration and maintenance of a secure Linux file and print server, some additional security applications will need to be installed.

An essential component to boost security is antivirus software. Although Linux does not appear to be a target platform for virus writers, preparation is the best line of defense. There are several choices available for Linux antivirus software that supports RHEL ES 3; however, none stands out above the rest. For this reason, HFM will test a select group of Linux antivirus software over the next six

---

[4] RHN
[5] MD5 SUM
[6] Sharpe
[7] Eckstein

months, and choose the best product for procurement. Using a production system to evaluate software is not typically advised. However, since HFM currently only has one Linux server and limited funds with which to acquire additional software, evaluation copies of antivirus software will be installed and tested, first on the Linux workstation, then on the server. At the six-month mark, a licensed copy of the best choice will be procured and installed.

There are several other applications that will be installed to ensure security and locate any breaches. TCP wrappers and iptables will be installed from the RHEL ES 3 media during the initial installation. Tripwire[8] and the Tiger Analytical Research Assistant (TARA)[9] will be installed on the server to help maintain a secure environment. Nessus[10] and Nmap[11] will be installed on the Linux desktop to test and verify server security through external scanning.

4.0   Risk Analysis and Mitigation

Every computer system is at risk of compromise. Whether a computer is disconnected from all peripherals and power, or secured in a locked office, the danger of physical compromise of the system and stored data always exists. For computers that are connected to a network or the Internet, the risk of local and remote compromise of the system and data integrity increases the threat. One of the primary goals in building a secure Samba server is to safeguard against numerous internal and external threats.

4.1   Internal Threats

4.1.1   Physical Damage

Numerous vulnerabilities exist inside the office where the server will be located. Physical damage to the system is often an overlooked area of concern. The system may be knocked over or kicked, possibly causing physical damage. If not properly protected, the main board or memory could be damaged by a power surge. A staff member may accidentally spill coffee on the system, potentially causing electrical problems. A more severe scenario involves the system case being opened and parts intentionally removed or violated.

4.1.2   Unauthorized Console Access

Unauthorized access to the server console is a primary issue to consider when securing against compromise. Data files containing personnel, accounting, client, and design information are at risk, as are system files. An unauthorized user with console access may be able to copy /etc/passwd or /etc/shadow files to floppy to run against a password-cracking utility on another system. Samba

---

[8] Tripwire
[9] TARA
[10] Deraison
[11] Nmap

configuration files--including `/etc/samba/smbpasswd`--may also be modified to an attacker's advantage. Other system files such as `/etc/fstab`, `/etc/ssh/sshd_config`, and `/etc/securetty` may be modified to allow unauthorized remote access. The system could be rebooted in an attempt to enter single-user mode. A worst-case scenario involves an open `root` shell on an unattended server console. Any of these situations, or a combination thereof, could lead to compromised data or system modification that would facilitate malicious intent to damage the local network or Internet.

4.1.3   Local Network Environment

Potential unauthorized remote access from one of the workstations on the network adds an additional risk to the local environment. Many of the same risks threatening the server console also exist from the local network. An unattended workstation that is logged onto the server could give an unauthorized user access to server data and system files. A scenario with even more dire risk is an unattended workstation with an open session to the server, possibly as `root`.

In addition, trusted, authorized users could pose a unique threat. However unlikely it may seem, a competitor could attempt to persuade a trusted user to compromise company or system data. This type of threat may be difficult to detect due to the level of confidence afforded the user. With this type of threat, any number of attacks could be executed without raising concern. Any of the server console or local network risks could be exploited by a trusted user and go unnoticed indefinitely.

4.2   Remote Threats

A seemingly insignificant server on a tiny network may be perceived as irrelevant to the malicious hacker community; then again, this may be just the type of environment that is targeted most frequently. Small, unprotected networks can easily provide invaders with systems on which to carry out harmful attacks on larger targets. The possibility of a competitor attempting unauthorized remote access through open ports also exists. Regardless of whether or not data is compromised during such an attack, any successful breach could damage system files and render the system useless, prompting a necessary rebuild. A denial of service attack that lasts long enough to bring a system down may have several adverse effects, including a loss of revenue. Packet sniffers may be executed remotely in an attempt to trap packets containing password information.

4.3   Mitigation Plan

4.3.1   Physical Security

With the exception of being in an unlocked office during business hours, the potential threats to the Samba file and print server may be alleviated by several levels of security. Physical security will be increased by securing the system in a

locked server cabinet, with the only keys in the possession of the owner and shop manager.

4.3.2 Console Access

Console access to the server will be restricted to the owner. Only the owner will have root access to the system. A primary system login account will be created for maintenance and diagnostic purposes. Only the owner will have access to this account via the console and SSH. Root login will be disabled from any console, including an SSH session. The shop manager and the two floor managers will have read and write account access to specific shared directories from the desktop or the laptops. These accounts will not be able to login directly to the server. Shop staff will be restricted from all computer access. When not in use, the console will be locked by the primary system login account.

4.3.3 Passwords

A written password policy states that all passwords must consist of at least eight characters, and include a combination of letters, numbers, and symbols. Passwords should be changed every ninety days.

4.3.4 Boot Passwords

To protect against system reboot attempts to get into single-user mode, a BIOS system password, a BIOS setup password, and a Grand Unified Boot loader (GRUB) loader password will be enabled. The passwords will not match. Only the owner and the shop manager will have this password information.

4.3.5 Package Installation

During installation, only the minimum set of packages necessary for system functionality and security will be installed. A graphical environment will not be installed, consequently the default run level will be run level 3. A limited set of additional packages will be installed, including Samba and third party security tools. Any unnecessary services installed by default will be disabled.
As the server will not have Internet access, all package updates that are not included with authorized vendor media will be downloaded to one of the workstations. All outbound server traffic will be blocked at the router. The following package update procedure will be implemented:

- All OS and primary application patches that are applicable to the system will be downloaded from www.rhn.redhat.com to a workstation.
- The packages will be copied to the server via SFTP or CDROM for verification and installation.
- The packages will be verified on the workstation using the MD5 SUM accompanying the individual packages.

- Prior to any scheduled package updates, a full backup of the system will be executed and verified
- `kernel` update packages will be installed separately from existing `kernel` packages.
- All other packages will be installed as updates.
- Any package update that is not available from Red Hat will be evaluated for necessity and tested on an alternate system prior to installation on a production server.

4.3.6 Removable Media Device Access

To guard against system files being copied to floppy disk, mounting the floppy device will be restricted to `root`. Mounting the CDROM device will also be restricted to `root` to help guard against the copying of any unwanted files or packages to the system.

4.3.7 Backup Tapes

On the Linux workstation, the owner will load backup tapes just before scheduled backups, and remove them upon completion. The tapes will be transported off-site and stored in a fireproof safe. Any tapes stored temporarily on-site will also be stored in a fireproof safe. While account information or keyed locks can readily be changed, the safe combinations cannot easily be altered if the shop manager is terminated. Therefore, only the owner will know the combination to the safe.

4.3.8 Permissions

User-level account permissions will be configured through Samba. Directory read, write, and execute access will be granted via group membership only. User accounts will be added to the necessary groups. UNIX file permissions and group access will also be configured in the same manner.

4.3.9 Third Party Applications

Select third party utilities will be implemented to help guard against unauthorized intrusion, data modification, and exploits that may leave the system vulnerable. Tripwire, F-Secure Antivirus,[12] and Tara will be installed and configured on the server. Nessus and Nmap will be executed against the server from a workstation.

4.3.10 Network

The network is protected from the Internet through a router that provides NAT functionality. All of the devices on the network will have an IP address in the

---

[12] F-Secure Linux

private 192.168.0.0 range, which is not a public Internet routable subnet.[13] All port 80 (HTTP) traffic to and from the system will be blocked at the router. This does not guarantee the integrity of the server or the network, but it does provide a credible first line of defense.

5.0   Operating System Installation and Hardening

As previously mentioned, HFM has purchased a support contract with Red Hat, and has received authentic installation media directly from the vendor. The media kit consists of nine CDs, including installation, source, documentation, and extras. For this installation, only the installation CDs--numbered one through four--are needed. Once the system is installed, HFM will proceed with the hardening process using both utilities and applications installed and configured during the base build, and packages downloaded from the Internet.

5.1   Installation

5.1.1   BIOS Passwords

The first step of the installation is to configure a system password through the BIOS utility. Using this type of password will serve as the first line of defense against system reboots attempts to gain single-user access. Please note the following instructions are for Dell BIOS version A08. Alternate BIOS versions will have the same basic premise, although the security options may be in different locations. Upon booting up the system, hit the F2 key during the initial Dell splash screen to bring up the BIOS utility. Using the arrow keys, scroll down to System Security and hit Enter. Options to configure a system password and a BIOS setup password are presented. The former will prompt for a password to continue with system startup, and the latter will protect against unwanted changes to the BIOS. Configure a unique password for both just in case one of them is compromised. Exit the utility and reboot.

5.1.2   Begin Installation

To boot from the first installation CD, hit F12 at the Dell splash screen. At the boot device menu, choose CDROM and proceed. The option to perform the installation in graphical or text mode is given. This is a preferential choice, and has little or no effect on the installation or security of the system. Additional boot options are available that are not necessary for this installation. HFM will use the graphical interface mode for this installation. At the boot options screen, hit Enter to begin the installation. Over the first few screens, choose the desired environmental variables, configure the mouse, and click through until the Disk Partition Setup screen is reached.

---

[13] Egevang

5.1.3 Partitions

A choice between automatic disk partitioning and manual disk partitioning is presented. Automatic partitioning will use all of the disk space to create the following default partitioning scheme:

```
/boot
/
swap
```

This is not a secure partitioning scheme for reasons that will be discussed in the following paragraph. The default-partitioning scheme may be edited to suit specific needs, however Disk Druid should be used to create a custom and secure configuration. Using Disk Druid will allow separate file systems to be created to aid in security and file integrity. A minimum scheme recommendation looks like this:

/boot (*kernel and bootstrap files*)
/ (*system management files*)
/home (*individual user's home directories*)
/var (*dynamic files, including log and spool files*)
/usr (*shared system files*)
/tmp (*temporary files*)
swap (*memory paging*)

This is the partitioning scheme HFM is using to help protect against denial of service (DoS) attacks. One of the reasons the default-partitioning scheme is not secure is because it does not help protect server availability from DoS attacks. An example of a DoS attack is an attack that attempts to fill up the /tmp and /var directories in order to interrupt system functionality.[14] Since the /var directory contains system logs and spool files, this type of attack proves very effective. By keeping target directories separate from the /, /var, and /home directories, HFM will help ensure that denial of service attacks do not halt all functionality of the system. An additional file system, /data, will also be added for file storage and sharing, thus providing another reason to use this type of scheme, which is to help protect against data loss in the event the system requires a rebuild.

The partitioning scheme created by HFM is as follows:

/boot	=	100mb
swap	=	1024mb
/data	=	50000mb
/var	=	5000mb
/usr	=	5000mb
/tmp	=	5000mb
/	=	5000mb

---

[14] Koconis, pg. 6

/home   =   5000mb

All file systems, with the exception of swap, are formatted using ext3. Compared
to ext2, the ext3 file system supports journaling to provide a quicker recovery
after an ungraceful shutdown, stronger data integrity, and higher throughput.[15]
Ext3 is the default file system for RHEL ES 3. 38000mb of space is left over for
file system growth as needed.

5.1.4   Boot Loader

Two boot loader options are given, GRUB and LILO. GRUB is the default RHEL
ES 3 boot loader, and should be chosen for this installation. The boot loader
configuration also offers a couple of security-based options. Configuring a
unique boot loader password provides an additional level of protection against
unwelcome system reboots by helping prevent single-user sign on and unwanted
kernel variables. Another level of protection against malicious intent may be
accomplished through the advanced boot loader options. By configuring the boot
loader record to be stored on the first sector of the boot partition instead of the
Master Boot Record, the command fdisk /mbr will not render the system
unbootable.

5.1.5   IP Address

A static IP address is configured for the system. The IP address information is
the following:

                IP Address   =   192.168.0.51
                Subnet Mask   =   255.255.255.0
                Gateway   =   192.168.0.1
                DNS Server   =   192.168.0.1
                Hostname   =   HFM101

The IP subnet 192.168.0.0 is a private IP address range, and therefore it is not
Internet routable. The NAT functionality of the router allows the creation and use
of private networking, which shields the server from remote connections
originating from outside of the network.

5.1.6   Firewall

Firewall setup follows the IP address configuration. Initially, port 22 will be open
to allow remote SSH administration from one of the workstations on the network.
The firewall is enabled during installation.

---

[15] Fuller, pg. 73

5.1.7 Root Password

After additional language support and time zone configuration, the root password is configured. For all passwords, especially the root password, a strong password scheme should be used. Weak passwords consist of only letters, or replacing a letter with a similar looking number, e.g., using "3" in place of "E", or "0" instead of "o". Other examples of weak passwords include names of family members, birthdates, and mascots of sports teams. With the proper utility, such as John the Ripper[16], or a colleague with a smart guess, weak passwords may be relatively easy to crack. Password cracking utilities use dictionaries and pre-defined word lists to decipher passwords. A good password contains a combination of upper and lower case letters, numbers, and special characters. It will also be at least eight characters in length, as the longer the password, the more difficult it is to crack. While some operating systems do not support or utilize passwords in excess of eight characters, RHEL ES 3 uses MD5 encryption by default. MD5-based encryption supports passwords of any length.[17] Since the example ac1WdT$@!3A5M has no meaning and cannot be found in a dictionary or word list, it is an example of a good password. Thirteen mixed characters make up an acronym for the sentence "a cat is walking down the street and is eating a silly mouse." By following the password policy, the root password is configured.

5.1.8 Additional Packages

While the default package configuration includes Samba, it also includes many packages that are unnecessary and may present a security risk if installed. For example, this system will not provide Web services, therefore the Web Server package group is not required. Additionally, the majority of the Server Configuration Tools will not be necessary, and thus will be removed. Always choose to customize the package selection to ensure only the necessary packages are installed.

The following table outlines the additional package groups installed on HFM101 during the initial OS installation. Unless otherwise noted, the default base and optional packages have been installed for each group.

Package Group	Removed Optional Packages	
Server Configuration Tools	redhat-config-bind redhat-config-nfs redhat-switch-mail-gnome	redhat-config-httpd redhat-switch-mail
Windows File Server		
Administration Tools	redhat-config-nfs	redhat-conifg-soundcard
Printing Support	gimp-print-cups Enscript	hpoj

Table 1 – Additional Packages

---

[16] John the Ripper
[17] Nemeth, pg. 78

5.1.9 Post Installation

Once the post-installation tasks finish, the system is rebooted. The system is logged into as root, and the primary account woodone is created by executing the command **#useradd woodone**, which automatically creates the account's primary group by the same name.   By executing the command **#passwd woodone**, a password is configured in accordance with the password policy. Log off root and re-login as woodone. Executing the command **$su -** will switch to root. Since HFM101 does not have multiple processors, and the default kernel supports symmetric multiprocessing (SMP), /etc/grub.conf is modified upon the second login to switch to the non-SMP kernel.   Prior to any file modification, a backup copy is created. For example, execute the command **#cp /etc/grub.conf /etc/grub.conf.orig** to label the copy as the original. Alternatively, the file could be copied to /etc/grub.conf.7.7.04 to reflect the date the copy is made. A preferred text editor, such as vi, is used to modify files. To change the default kernel for this system, the value of the eleventh line in /etc/grub.conf is changed from default = 0 to default = 1. The first kernel listed in /etc/grub.conf is considered "0", the second is considered "1". Also, note on line fourteen that the GRUB password configured during installation is MD5 encrypted. The /etc/grub.conf file is posted in Appendix A.

5.1.10 Boot Diskette

Before continuing, an emergency boot diskette is created by inserting a floppy disk and executing the command **#mkbootdisk *kernel version***. The kernel version may be found by executing the command **#uname -r**. This diskette can be used to boot into the system for emergency maintenance if all other boot options fail. The diskette is stored in the office fireproof safe.

5.2   Hardening

The system is now ready for hardening. Once the box is secure, HFM will proceed to create accounts and the necessary shares, configure Samba, and install the printer. The Samba post-configuration checklist includes additional hardening steps.

In general, hardening a server or workstation is defined the same regardless of platform OS. To harden a system is to secure it against known and potential vulnerabilities. There are numerous steps that may be taken to harden a system. Some of the most obvious include using TCP wrappers, a firewall, and applying patches. The steps HFM is taking to harden HFM101 are listed as follows:

- Physical security
- Block outbound traffic at the router
- Disable unnecessary services
- Update the system regularly
- Install antivirus software

- TCP Wrappers
- Configure login warning banners
- Modify /etc/securetty to restrict root access
- Disable SSH root login
- Password-protect single-user mode
- Disable ctrl-alt-del functionality
- Enable password aging
- Delete unnecessary system accounts
- Check for empty passwords on enabled accounts
- Lock unused system accounts
- Restrict floppy drive mount to root
- Restrict CDROM mount to root
- Disable booting from floppy or CDROM
- Enable BIOS boot and setup passwords
- Enable a GRUB password
- Install and configure Tripwire to create a baseline

During and after Samba configuration, two additional hardening steps will be performed. These steps are:

- Configure the firewall to allow Samba traffic
- Create a new Tripwire policy file and database and execute a new integrity check

All of these steps will be described in detail in the following sections.

5.2.1   Physical Security

Physical security is attained by placing the server in a small cabinet with sufficient ventilation and back panel holes to allow cable access. The keyboard and monitor are also stored in the cabinet. When console access is not needed, the cabinet is locked. Only the owner and shop manager have keys.

5.2.2   Firewall at the Router

Both outbound traffic from the server's IP address--192.168.0.51--to the Internet, and inbound traffic addressed to the server, are filtered. This is accomplished by using the router configuration utility's Web interface.
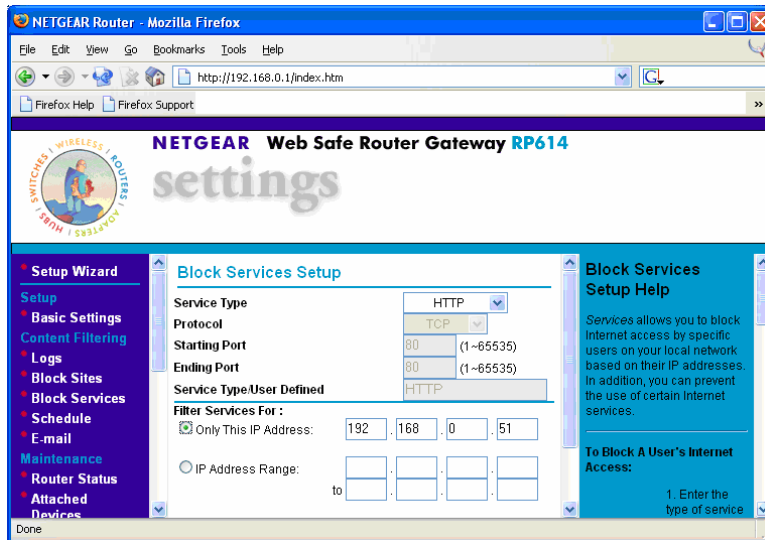
Figure 3 – Filter HTTP Traffic

5.2.3   *Disable Services*

To avoid patching known unnecessary services, they will be disabled prior to applying updates. The `chkconfig` utility will determine the services that will be disabled and removed. The `chkconfig` command is able to list, by run level, enabled services, including those running through `xinetd`. By executing the command `#chkconfig --list | more`, the current list of services is presented:
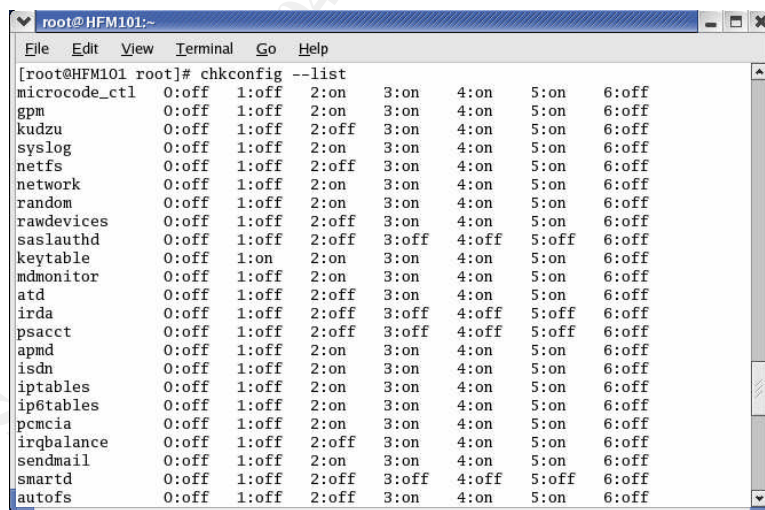

Figure 4.1 – `chkconfig` List Example

Figure 4.2 – `chkconfig` List Example Continued

The list includes nine unnecessary services that may be disabled. The following table lists and describes each service that will be disabled.

Service	Description
isdn	For use with isdn cards
ip6tables	Firewall utility for IPv6
pcmcia	For use with pcmcia cards
sendmail	Internet mail server
autofs	Used for auto mounting network shares
portmap	Security tool for RPC calls, usually with NIS and NFS
nfslock	Control script for NFS server
rhnsd	Query program for RHN updates
xfs	X font server

Table 2 – Disabled Services Description[18] [19]

To disable these services, the `chkconfig` command is again utilized. For example, to disable `isdn`, execute the command **`#chkconfig --level 2345 isdn off`**. Once the specified services are disabled, execute **`#chkconfig --list`** to verify. Reboot the server to end any leftover processes. Upon reboot, the command **`#ps -ef`** is executed to verify there are not any unnecessary processes running.
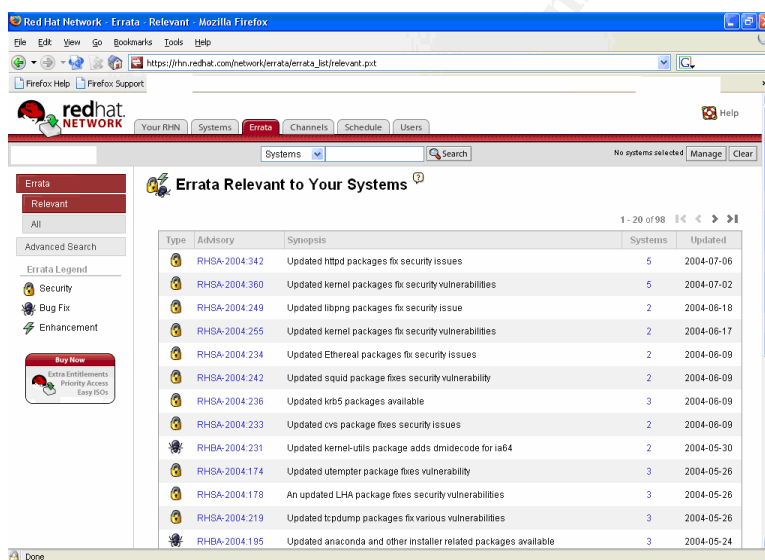
---

[18] Berger
[19] Rhnsd

5.2.4 Package Updates

Considering the OS has just been installed, a system backup is not necessary before initial package updates. Since HFM101 is not connected to the Internet, HFM's RHN subscription will need to be used manually. This is not a security requirement, as the command `up2date` is an acceptable means of updating a system. If the subscribed system is connected to the Internet, checking for and applying package updates is easily done by executing the command **#up2date**. However, HFM prefers to restrict Internet access to and from the server. In this situation, the Red Hat Errata on www.rhn.redhat.com will need to be searched manually and checked against existing packages. Once the necessary packages are determined, they will be downloaded along with the MD5 SUM to a workstation, and then copied to HFM101 via SFTP or burned to CDROM.

To begin, the Errata section of RHN is accessed.

Figure 5 – Errata List

Start with the most recent advisory at the top of the list. RHSA-2004:342 is not relevant to HFM101, as a Web server is not installed. Next on the list is RHSA-2004:360, which addresses a vulnerability in the `kernel` NFS server. HFM101 is not running NFS, and consequently this package is not needed. The third advisory potentially applies to the system being built. RHSA-2004:249 describes a vulnerability in `libpng`. Checking the advisory details for affected channels verifies that RHEL ES 3 is at risk. Whether this package should be installed on HFM101 may be determined by first clicking on the advisory link, and then the packages tab to check available package names. [20]

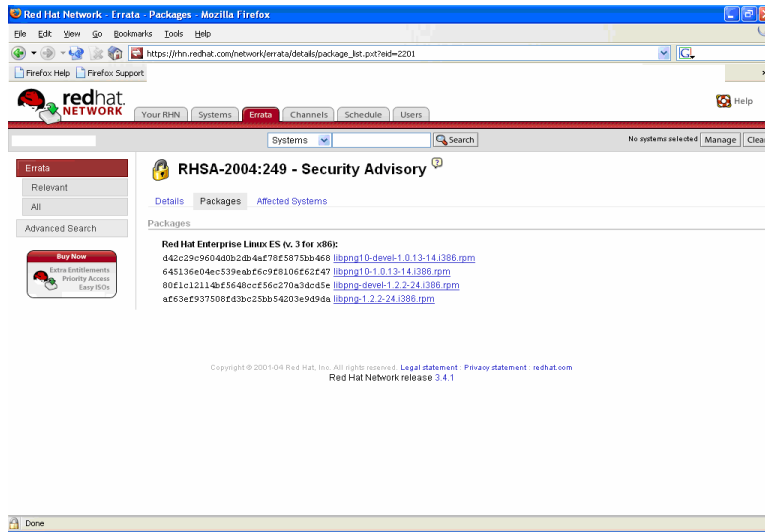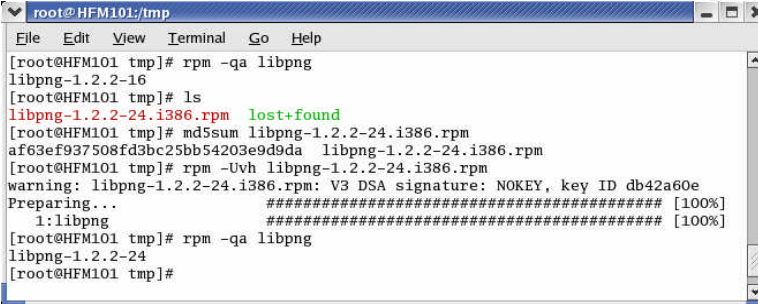[20] Errata

Figure 6 – libpng Package Updates

Once the available package update names are checked, the command **#rpm -qa libpng** is executed to verify if the vulnerable packages are currently installed. HFM101 is currently running libpng-1.2.2-16. The package update version is libpng-1.2.2-24, and therefore this update must be downloaded and applied. Along with the package download, the MD5 SUM information provided is documented for later verification.

A thorough check and comparison of the advisories and existing packages has produced a list of twelve packages that require an update:

- glibc-common-2.3.2-95.6.i386.rpm
- ipsec-tools-0.2.5-0.4.i386.rpm
- kernel-2.4.21-15.0.2.EL.i686.rpm
- krb5-libs-1.2.7-24.i386.rpm
- krb5-workstation-1.2.7-24.i386.rpm
- lha-1.14i-10.2.i386.rpm
- libpng-1.2.2-24.i386.rpm
- libxml2-2.5.10-6.i386.rpm
- rsync-2.5.7-4.3E.i386.rpm
- slocate-2.7-3.i386.rpm
- tcpdump-3.7.2-7.E3.2.i386.rpm
- glibc-2.3.2-95.6.i386.rpm

The RPMs and accompanying MD5 SUM are downloaded to a workstation and transferred to the /tmp directory on the server using SFTP. Using the libpng package as an example, the RPM is verified and applied. With the exception of the kernel updates, the command **#rpm -Uvh *packagename*.rpm** is generally used for RPM updates. Kernel updates should be installed separately from the existing kernel for redundancy purposes. If upon reboot after the kernel upgrade the system does not boot properly, the system may be booted to the previous kernel version. If the kernel version is upgraded directly and the

system does not boot properly, a much more involved method of repair may be required. To verify the `libpng` package, execute the command **#md5sum libpng-1.2.2-24.i386.rpm**. The output af63ef937508fd3bc25bb54203e9d9da libpng-1.2.2-24.i386.rpm is checked against the MD5 SUM downloaded with the RPM or posted on the download page (af63ef937508fd3bc25bb54203e9d9da).   The package file integrity verifies and may be installed. The command **#rpm -Uvh libpng-1.2.2-24.i386.rpm** is executed to update the package. Executing the command **#rpm -q libpng** verifies the package update to `libpng-1.2.2-24`.
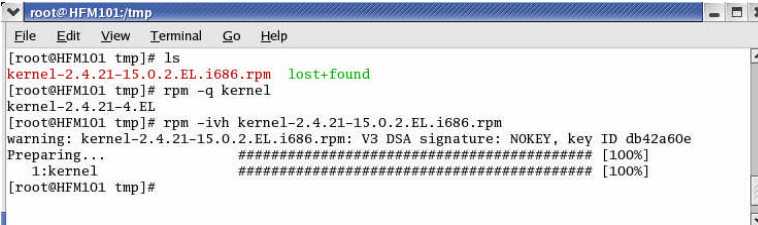
```
root@HFM101:/tmp
File  Edit  View  Terminal  Go  Help
[root@HFM101 tmp]# rpm -qa libpng
libpng-1.2.2-16
[root@HFM101 tmp]# ls
libpng-1.2.2-24.i386.rpm  lost+found
[root@HFM101 tmp]# md5sum libpng-1.2.2-24.i386.rpm
af63ef937508fd3bc25bb54203e9d9da  libpng-1.2.2-24.i386.rpm
[root@HFM101 tmp]# rpm -Uvh libpng-1.2.2-24.i386.rpm
warning: libpng-1.2.2-24.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
   1:libpng                 ########################################### [100%]
[root@HFM101 tmp]# rpm -qa libpng
libpng-1.2.2-24
[root@HFM101 tmp]#
```

Figure 7 – `libpng` Update

While proceeding with the remaining updates, a dependency failure is encountered. Executing the update for `ipsec-tools-0.2.5-0.4` advises a dependency failure in `initscripts`. Package `initscripts-7.31.11.EL-1` or later is required. The current version is `initscripts-7.31.6.EL-1`, and as a result, an update of this package needs to be completed before proceeding.

`Initscripts-7.31.13.EL-1` is downloaded, verified against the accompanying MD5 SUM, and applied. Following this update, the `ipsec-tools` package is successfully updated. With the exception of the `kernel` update, all other packages are successfully updated.

As previously mentioned, the `kernel` update should not be applied using the **#rpm -Uvh** command. The reason behind this is that the availability of a known good `kernel` for backup is highly recommended. For the `kernel` update, the command **#rpm -ivh kernel-2.4.21-15.0.2.EL.i686.rpm** is used to install a separate `kernel`. Once installed, the system is rebooted to verify the installation. If the installation is successful, `/etc/grub.conf` is modified to reflect the changes.

```
root@HFM101:/tmp
File  Edit  View  Terminal  Go  Help
[root@HFM101 tmp]# ls
kernel-2.4.21-15.0.2.EL.i686.rpm  lost+found
[root@HFM101 tmp]# rpm -q kernel
kernel-2.4.21-4.EL
[root@HFM101 tmp]# rpm -ivh kernel-2.4.21-15.0.2.EL.i686.rpm
warning: kernel-2.4.21-15.0.2.EL.i686.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
   1:kernel                 ########################################### [100%]
[root@HFM101 tmp]#
```

Figure 8 – `Kernel` Update

After a successful reboot, verify the new kernel is running using the **#uname -r** command. Once verified, two entries in the /etc/grub.conf file are modified. First, make a new backup copy of /etc/grub.conf. Next, comment out any kernel version that is not necessary. For redundancy, the two latest kernel versions should be available for selection during boot. In the case of HFM101, kernel 2.4.21-4.ELsmp is not necessary since this system has only one processor. This entry is commented out. The new kernel is then configured as the default by changing default = 1 back to default = 0. The emergency boot diskette is updated to reflect the new kernel. An example of the modified /etc/grub.conf is posted in Appendix B.

5.2.5   Antivirus Software

A permanent antivirus solution has not yet been determined, and as part of the previously discussed plan to determine the best antivirus software, select evaluation copies will be installed and tested over a six-month period. Initially, an evaluation copy of F-Secure Antivirus for Linux Servers 4.61[21] is installed and configured for use. During installation, a daily virus scan of all file systems is scheduled to execute at 5:00 AM. This time is chosen to prevent interference with normal business use and nightly backups.

5.2.6   TCP Wrappers

TCP wrappers is installed by default with RHEL ES 3 and provides host-based access control to network services. It references the /etc/hosts.allow and /etc/hosts.deny files--in that order--to determine if a client is granted access. Once the connection is granted, TCP wrappers allows access to the wrapped service. Most network services on RHEL ES 3, including xinetd, are linked to TCP wrappers.[22]

5.2.7   Login Banners

The next step on HFM101 is to create login banners to advise users of the rules of authorized use. Another benefit of login banners is that information important to potential hackers can be hidden. Examples of this information are the OS type and version. Three files may be edited to post a message upon local and remote login.

- /etc/motd – This is the message of the day, and is displayed after a successful login.
- /etc/issue – This message is displayed to any user logging in locally.
- /etc/issue.net – This message is displayed to any user logging in remotely.

---

[21] F-Secure Antivirus
[22] Fuller, pg. 240

Warning banners may also be of use--as evidence--in the legal prosecution of alleged system trespassers in a court of law.[23]

Per standard procedure, prior to modifying `/etc/motd`, `/etc/issue`, and `/etc/issue.net`, a backup copy is made of each file. The following login warning message is configured on HFM101.

> "Access to this system is for authorized personnel only. Unauthorized access is prohibited. All actions may be monitored and documented."
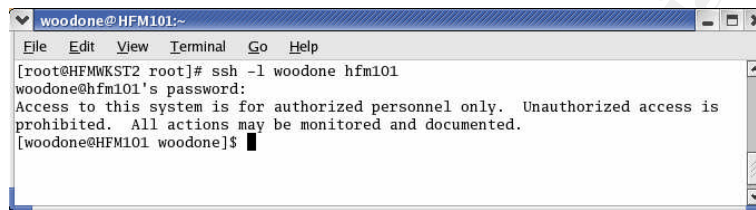

Figure 9 – Sample SSH Login With Warning Banner

5.2.8 Disable `Root` Login

Disabling `root` login both locally and remotely is especially important. A `root` password compromise could prove devastating if a thief or attacker with malicious intent is able to login directly with the compromised account information. HFM is taking two steps to disable `root` logins from any console. First, the `/etc/securetty` file is modified to disable `root` logins from any console. For security purposes, a copy of this file is not created. To disable `root` logins at the console, the command **`#echo > /etc/securetty`** is executed to empty the file. However, this will not disable `root` logins via SSH since the console is not opened until after authentication occurs.[24] For this reason, step two is to modify `/etc/ssh/sshd_config`. Line 37 of `/etc/ssh/sshd_config`, `PermitRootLogin yes`, is commented out by default. To disable `root` login via SSH, the comment is removed, and the value is changed to "`no`". The `/etc/ssh/sshd_config` file is posted in Appendix C.

5.2.9 Modify Inittab File

Password-protecting single-user mode and disabling ctrl-alt-del are both accomplished by modifying `/etc/inittab`. To password-protect single-user mode, modify `/etc/inittab` by adding `~~:S:wait:/sbin/sulogin` after the eighteenth line.[25] To disable ctrl-alt-del functionality, comment out line thirty-two

---

[23] Koconis, pg. 11
[24] Ha, pg. 30
[25] Koconis, pg. 12

of `/etc/inittab`, `ca::ctrlaltdel:/sbin/shutdown -t3 -r now`.[26] The `/etc/inittab` file is posted in Appendix D.

5.2.10   Linux Accounts

The following four steps are all related to securing system accounts. Password aging, deleting unused user and group accounts, verifying there are not any active accounts with empty passwords, and locking system accounts that do not require interactive login are vital account-management tactics that reduce the risk of password compromise and uninhibited access.

Since HFM101 does not have an X server installed, the command `chage` is used to modify password expiration. To configure password expiration on the user account `woodone` to occur every ninety days, the command **#chage -M 90 woodone** is executed. [27] To ensure that all subsequent accounts will be created with the ninety-day password aging setting, `/etc/login.defs` is backed up and modified. The value for the seventeenth line, `PASS_MAX_DAYS` is changed from `99999` to `90`. This is also a good time to modify the minimum characters required for passwords on line nineteen. The `/etc/login.defs` file is posted in Appendix E.

Removing unused system accounts that are installed by default will reduce the risk of account compromise. Searching through the `/etc/passwd` file, several accounts are found that are no longer necessary since their corresponding services have been disabled. The default `/etc/passwd` file is posted in Appendix F.

After creating a backup copy of `/etc/passwd`, the following accounts are removed from HFM101 using the `userdel` command.   For example, the account `mail` is removed by executing the command **#userdel mail**.

- `mail`
- `news`
- `uucp`
- `games`
- `operator`
- `gopher`
- `ftp`
- `rpc`
- `rpcuser`
- `nfsnobody`
- `mailnull`
- `smmsp`
- `xfs`
- `ntp`

---

[26] Fox, pg. 227
[27] Ha, pg. 26

The corresponding groups are deleted by executing the command #groupdel *groupname*.

System accounts that do not have a valid shell cannot be used to login, however it is still prudent to verify these accounts do not have empty passwords and are locked. To verify system accounts do not have empty passwords, the command #awk -F: '($2 == "") { print $1 }' /etc/shadow is executed. If the output is blank, then there are no accounts with empty passwords. An alternative method is to manually verify that the second field of the /etc/shadow file entries is not blank.[28]

Browsing the /etc/shadow file will also verify if a system account is locked. If the account is locked, the character string of the password field is preceded by an "!" symbol. In addition, when a password field contains only "!!", the account is locked and unable to login, and does not have a password.[29] To lock an account, execute the #usermod -L *username* command. Appendix G exhibits two examples of the /etc/shadow file. The first example displays the /etc/shadow file prior to locking any accounts, and the second example shows the results of the execution of the usermod command.

5.2.11 Removable Media Device Access

To provide additional protection against unwanted file and application installations, mounting of the floppy drive and CDROM drive are restricted to root. After creating a backup of /etc/fstab, this file's mount options may be modified to restrict the mounting of /dev/fd0 and /dev/cdrom.

The nouser option for the mount command restricts mounting the file system to root. Examples of the /etc/fstab file before and after the mount options are changed are posted in Appendix H.

5.2.12 Disable Bootable Devices

Disabling the floppy and CDROM drives as boot devices is completed by rebooting the server and entering the BIOS configuration. On Dell BIOS version A08, this is done by choosing Boot Sequence and using the space bar to disable the floppy drive and CDROM drive as boot devices. If BIOS and BIOS setup passwords have not yet been configured, this is a good time to do so. The BIOS and GRUB passwords for HFM101 are already enabled. To verify a GRUB password has been enabled, hit the P key when the GRUB screen appears.

5.2.13 Tripwire

The final step before the configuration of Samba is to install and configure Tripwire.   "Tripwire is a tool that checks to see what has changed on your

---

[28] Koconis, pg. 14
[29] Murdoch, page 43

system. The program monitors key attributes of files that should not change."[30]
Available both commercially and as open source, Tripwire is an essential
ingredient in creating and maintaining a secure server. The commercial version
may be purchased from http://www.tripwire.com,[31] while open source versions in
the form of tarballs or RPMs may be downloaded from http://www.tripwire.org,[32]
http://rpmfind.net,[33] and http://sourceforge.net.[34] An open source version created
specifically for RHEL ES 3 is not currently available. HFM has download and
successfully tested an RPM from http://rpmfind.net that was written for a previous
version of Red Hat Linux. This RPM is copied to HFM101, and then verified,
installed, and configured.

By executing the command **#rpm –ivh tripwire-2.3.1-17.i386.rpm**, Tripwire
version 2.3.1-17 is installed. To setup Tripwire, execute the script
#/etc/tripwire/twinstall.sh and follow the prompts.[35] Customizing the default
policy file to match the server's file configuration requires a manual edit of the
/etc/tripwire/twpol.txt file. The first modification adds the following files to
the Critical Configuration Files section of the policy file:

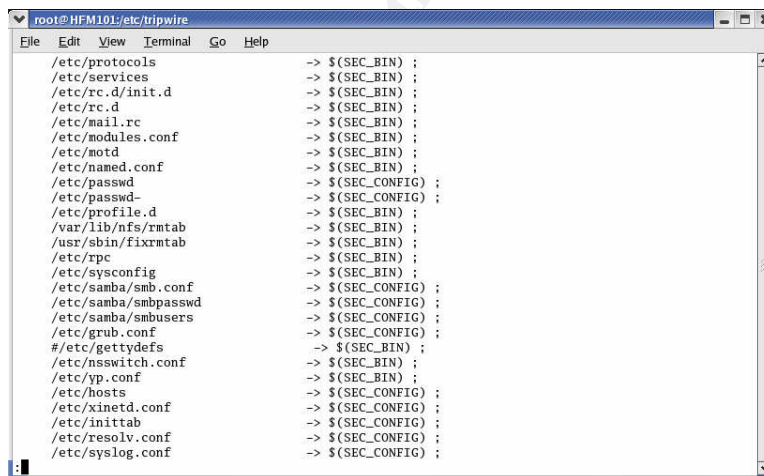- /etc/samba/smbpasswd
- /etc/samba/smbusers
- /etc/grub.conf

Figure 10 – Excerpt From Critical Configuration Files Section of /etc/tripwire/twpol.txt

Execute the command **#twadmin --create-polfile twpol.txt** to update the
policy file /etc/tripwire/tw.pol. Once the policy file is updated, execute the
command **#tripwire --init** to initialize the Tripwire database. Several file

---

[30] What is Tripwire
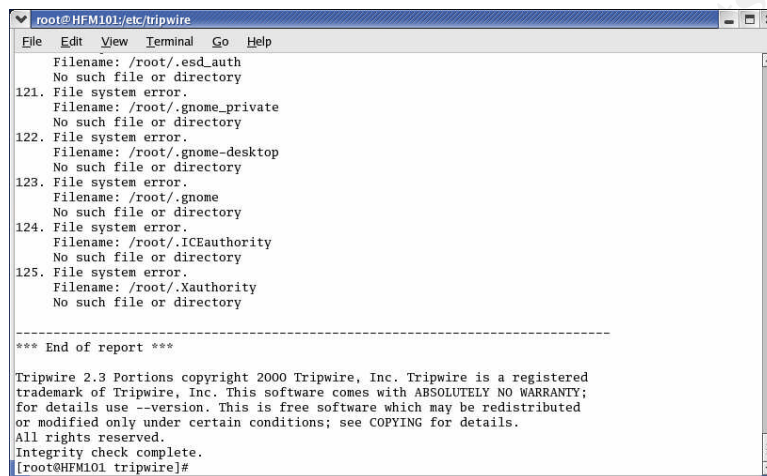[31] Tripwire.com
[32] Tripwire Download
[33] Veillard
[34] Sourceforge
[35] Armstrong, pg. 26

system errors may appear during the database initialization, indicating files that have an entry in /etc/tripwire/twpol.txt, but do not exist on the system. To verify which files do not exist on the system, execute the command #tripwire --check to check the integrity of the system.[36]

Viewing the Integrity Check Report determines that 125 files that are listed in /etc/tripwire/twpol.txt do not exist on the system. A second manual edit of /etc/tripwire/twpol.txt removes the entries for these files.

Figure 11 – Tripwire Integrity Check Report With File Errors

After /etc/tripwire/twpol.txt is modified, the process of updating the policy file and initializing the database begins again with the execution of #twadmin --create-polfile, #twpol.txt, #tripwire --init, and #tripwire --check.   The Integrity Check Report is printed following the check, although checking the twprint man pages shows that executing #twprint -m r will also print a copy of the report. An entry for a daily integrity check has already been added to /etc/cron.daily by the Tripwire setup program. A copy of the Integrity Check Report from this example is printed in Appendix I.

Figure 12 – Sample Tripwire Execution

---

[36] Armstrong, pg. 26

6.0   Accounts and Samba

6.1   Accounts

6.1.1   Linux Users and Groups

The next step in the server build is to define and create necessary user accounts, groups, and shared directories. The user account woodtwo is created for the shop manager by executing the command **#useradd woodtwo -s /bin/false**, and accounts woodthree and woodfour are created for the floor managers using the same command syntax. The -s options specifies the shell /bin/false, which is used to deny access to an interactive shell, thereby denying direct or SSH logins to the server. The frontoffice and shop groups are also created by executing the **#groupadd** *groupname* command. An existing group--woodone--will be used for restricted group access for the owner's user account.

The account woodone is a member of all three groups. Since the account is already a member of the woodone group, it is not necessary to add this group to the command string. To add woodone to the necessary groups, execute the command **#usermod -G frontoffice,shop woodone**. To verify group membership for woodone, execute the command **#groups woodone** and review. The output should contain all groups of which the account is a member. The woodtwo user account is added to the frontoffice and shop groups. woodthree and woodfour are added to the shop group.

6.1.2   Shared Directories

The following directory listing exhibits the Samba shared directories created under /data, the associated group ownership, and the assigned permissions to the directories. To create a directory, the command **#mkdir** *directory name* is executed. Group ownership is assigned by executing the command **#chgrp** *groupname directory*. Recursive read, write, and execute access is granted through group permissions. An example of this is the execution of the command **#chmod -r 770 personnel**. The account root retains recursive ownership on all groups.

```
drwx------    2 root      root              16384Jul  5 12:12 lost+found
drwxr-xr-x   21 root      root              4096 Jul 11 13:26 ..
drwxrwx---    2 root      woodone           4096 Jul 11 13:50 personnel
drwxrwx---    2 root      frontoffice       4096 Jul 11 13:50 advertising
drwxrwx---    2 root      frontoffice       4096 Jul 11 13:50 purchasing
drwxr-xr-x   11 root      root              4096 Jul 11 13:50 .
drwxrwx---    5 root      shop              4096 Jul 11 13:51 inventory
drwxrwx---    4 root      shop              4096 Jul 11 13:51 maintenance
drwxrwx---    2 root      frontoffice       4096 Jul 11 14:02 design
drwxrwx---    2 root      woodone           4096 Jul 11 14:06 acct
drwxrwx---    2 root      frontoffice       4096 Jul 11 14:17 sales
```

Figure 13 - /data Group Ownership and Permissions

6.2   Samba

6.2.1   Configuration File

In a text-only environment running Samba, one option for configuration is
manually editing the `/etc/samba/smb.conf` file. Using the command
`#chkconfig --level 3 smb on`, Samba is configured to start when the system is
booted. After creating a backup copy of the original, `/etc/samba/smb.conf` is
deleted and a new `/etc/samba/smb.conf` file is created and modified to reflect
HFM's requirements. The `[global]` section is added to `/etc/samba/smb.conf`
first. This section is used to configure server-wide options.[37]

```
[global]
        workgroup = HFM
        server string = hfm101
        wins support = yes
        wins server = 192.168.0.51
        hosts allow = 192.168.0/24 127.
        security = user
        encrypt passwords = yes
        smb passwd file = /etc/samba/smbpasswd
```

figure 14 – `[global]` Section of `/etc/samba/smb.conf`

The HFM network is setup as a workgroup, although using a domain
configuration is an option. For Microsoft Windows computers to communicate
with the Samba server, WINS support must be enabled, as the Samba server is
configured as the WINS server. The `hosts.allow` entry defines the subnets
allowed to connect. User-level security is the Samba default, and authenticates
users against the server.   Samba must be configured for encrypted passwords
because Windows default behavior is to encrypt passwords. Finally, the path to
the `/etc/samba/smbpasswd` file is configured to provide Samba with the
passwords it should use for authentication.[38]

6.2.2   Samba User Accounts

To create the Samba user `woodone`, the command `#smbpasswd -a woodone` is
executed. This will create entries in `/etc/samba/smbusers` and
`/etc/samba/smbpasswd`.[39] The Samba user accounts and the local workstation
accounts are identical, although they do not need to be. The
`/etc/samba/smbusers` file may be modified to create different usernames. The
`/etc/samba/smbpasswd` file is similar to the `/etc/passwd` and `/etc/shadow` files.
Examples of the `/etc/samba/smbusers` and the `/etc/samba/smbpasswd` are printed
in Appendix J.

---

[37] Yuen, pg. 45
[38] Yuen, pg. 47
[39] Yuen, pg. 47

6.2.3   Share Configuration

The remaining sections of the `/etc/samba/smb.conf` file are configured to share directories and the printer. The following example exhibits the `[homes]` and `[acct]` sections. The `[homes]` section defines access to the home directories, while the `[acct]` section is an example of a data directory share. Notice in the `[homes]` section that the valid users are listed individually. In addition, notice that a path to the directories is not specified. In contrast, the `[acct]` section lists the share path, and identifies valid users by group. The remaining directories are configured for access by group following the `[acct]` example below.

```
[homes]
        comment = Home directories
        valid users = woodone,woodtwo,woodthree,woodfour
        browseable = no
        writable = yes

[acct]
        comment = Accounting data
        path = /data/acct
        valid users = @woodone
        writable = yes
```

Figure 15 – Sample from `/etc/samba/smb.conf`

6.2.4   Firewall

Before the Samba shares may be accessed from any workstation, the firewall must be configured to allow the necessary port access. Samba uses the following ports:

- UDP port 137
- UDP port 138
- TCP port 139
- TCP port 145

To allow access to UDP port 137, the following line is added to `/etc/sysconfig/iptables` before any REJECT entries:

```
-A RH-FIREWALL-1-INPUT –m –state --state NEW –m udp –p udp --
dport 137 –j ACCEPT
```

Entries for the remaining ports are added, and the firewall is restarted by executing the command **#service iptables restart**. Following the firewall restart, Samba is restarted by executing the command **#service smb restart**. The `/etc/sysconfig/iptables` file is exhibited in Appendix K.

6.2.5   Share Access

The shares are tested from the Windows and Linux workstations. From Windows, the shares are accessed by opening My Network Places and browsing

to the HFM workgroup.
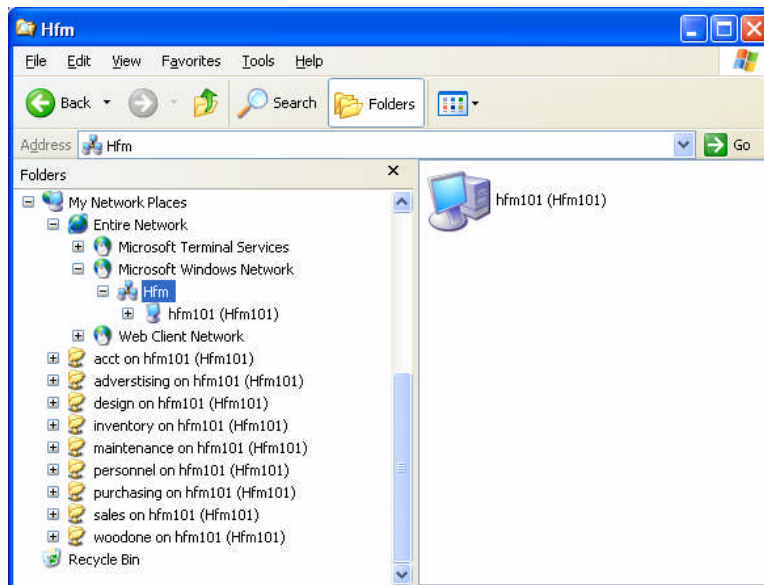
Figure 16 – Windows Access

From a Linux workstation, open Nautilus and enter smb://HFM101 in the location
field to access the shares.
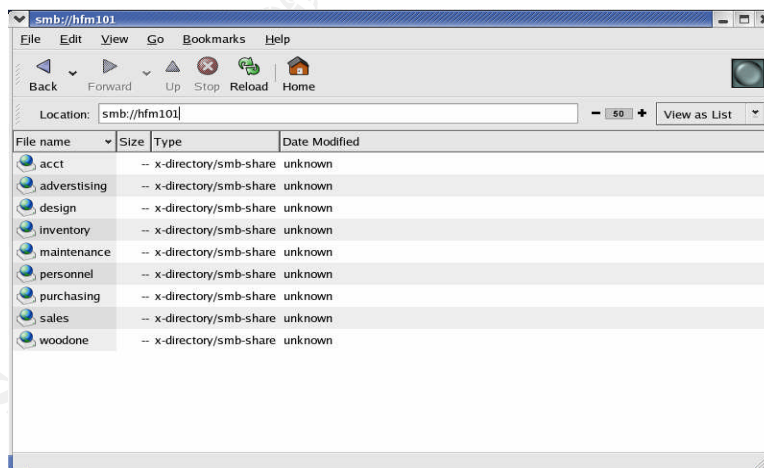
Figure 17 – Linux Access

6.2.6   Printer Configuration

The final steps of the Samba configuration on HFM101 involve setting up and
sharing an HP PSC 2110 inkjet printer. To open up the printer configuration
utility, execute the command **#redhat-config-printer**.
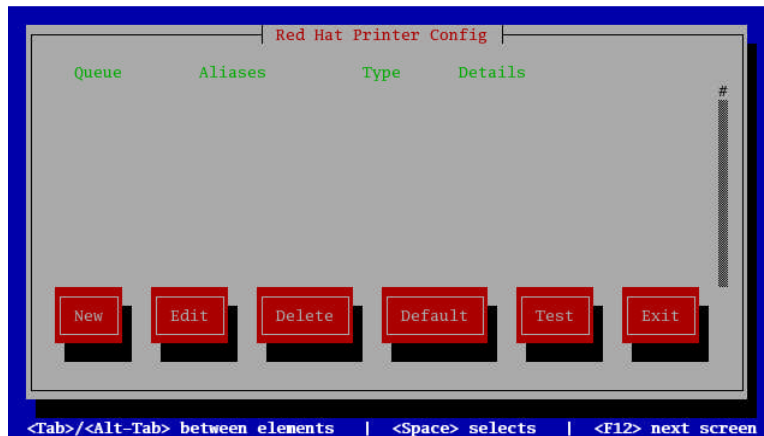
Figure 18 – Red Hat Printer Configuration Utility

The Local Printer Device Queue name is configured as PQ-HFM-2110.
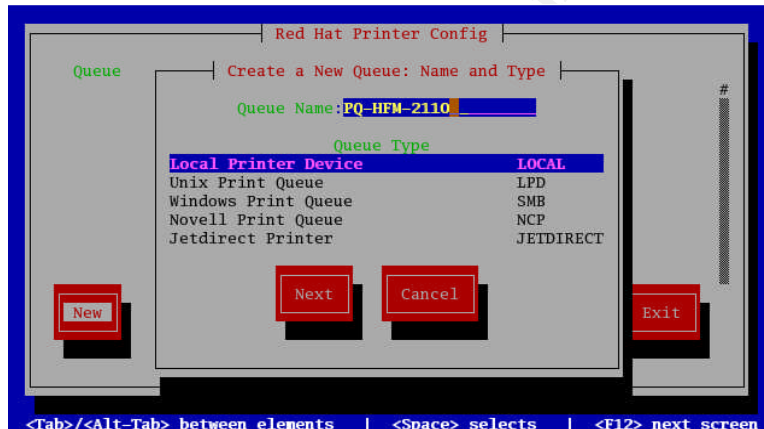
Figure 19 – New Printer Queue

The printer is attached to the server via USB, and therefore the Local Printer Device requires customization. The device is changed to /dev/usb/lp0.
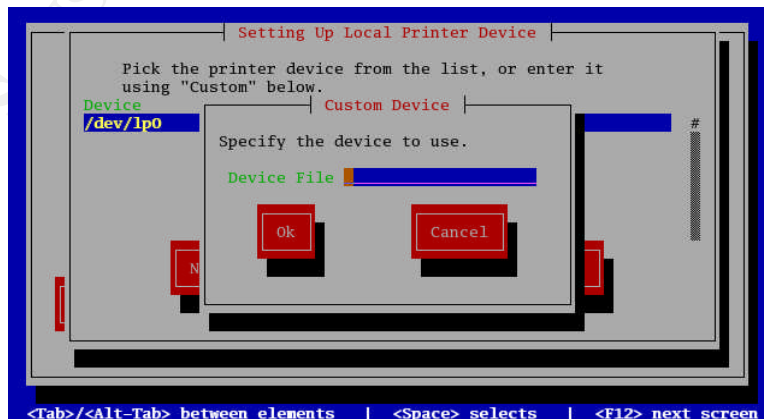
Figure 20 – Local Printer Device

The PSC 2110 hpijs Queue Driver is selected.

Figure 21 – Queue Driver

The printer installation is completed and a test job is executed from the server.
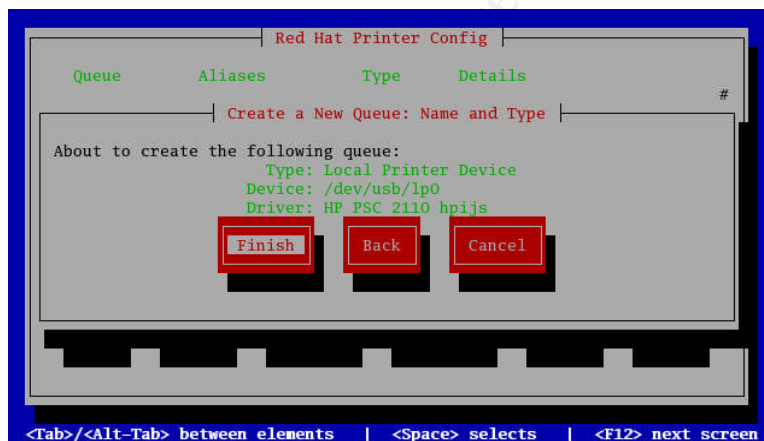
Figure 22 – Queue Creation
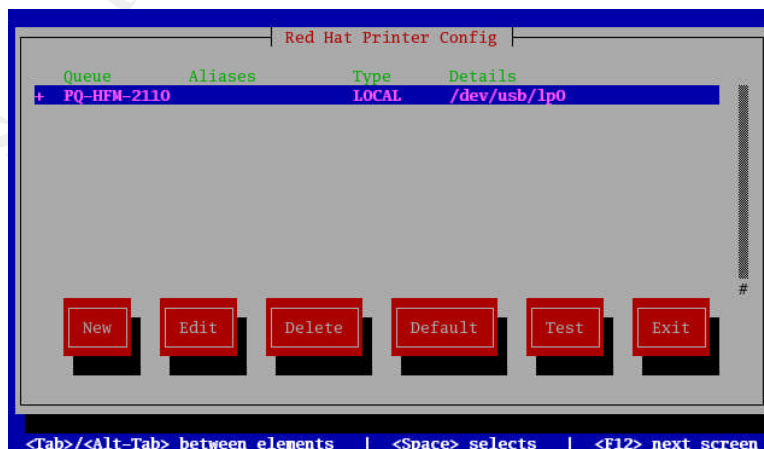
Figure 23- Printer Installation Complete

As the final step in configuring the printer for network use, the
`/etc/samba/smb.conf` file is modified. The following lines are appended to the
`[global]` section.[40]

```
        printcap name = /etc/printcap
        load printers = yes
        printing = cups
```

Figure 24 – [global] Printer Append

Next, the `[printers]` section is added to `/etc/samba/smb.conf` to instruct Samba
to share the printer.[41]

```
        [printers]
                comment = Printers
                path = /var/spool/samba
                browseable = no
                public = yes
                guest = yes
                writable = no
                printable = yes
                use client driver = yes
```

Figure 25 – [printers] Section of /etc/samba/smb.conf

Since authenticating to the server is required to access any resources, including
the printer, HFM has decided that an additional level of authentication is not
necessary to access the printer. A complete example of `/etc/samba/smb.conf` is
posted in Appendix L.
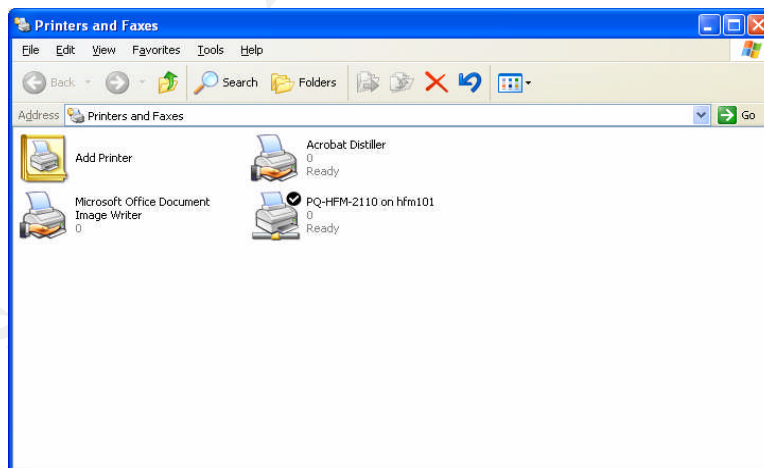
Figure 26 – Windows Printer List

---

[40] Yuen, pg. 51
[41] Yuen, pg. 51
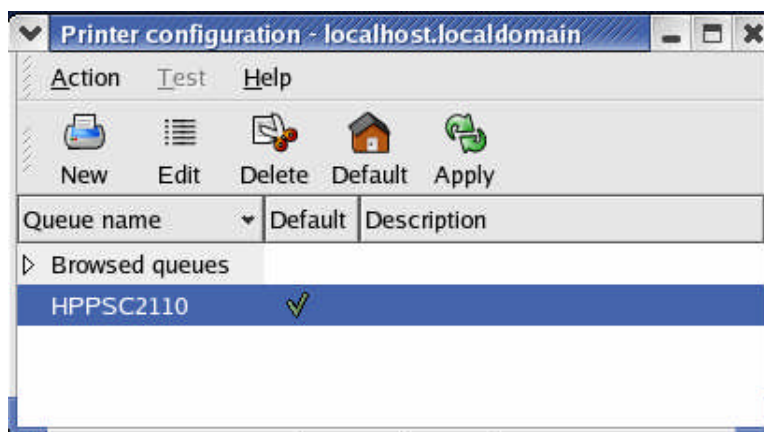
Figure 27- Linux Printer List

6.3   Tripwire Revisited

Once the Samba services configuration is complete and functioning properly, the Tripwire policy file and database are recreated and an integrity check is executed to create a new baseline by following the steps outlined in section 5.2.14.

7.0   Design and Implementation of Ongoing Maintenance Procedures

After initial setup, ongoing maintenance on HFM101 consists of several tasks. The list of tasks follows.

- Regular backups
- Regular updates to the OS and primary application
- System integrity verification
- Regular antivirus scans
- Checking log files
- Regular port scans to verify additional ports have not been opened
- Regular TARA scans

7.1   Data Backups

As previously mentioned, data backups are executed remotely from the Linux desktop. There are two reasons for this. The first is that the chosen software--BackupPC[42]--which is an open source backup application available from http://backuppc.sourceforge.net/, requires HTTPD and PERL.[43] These two services are not installed on HFM101, and the current projected plan for this system does not include their installation. The second reason is that client-side software is not necessary to perform a backup. This allows HFM to continue with

---

[42] Barratt
[43] Perl

a minimal set of services running on the server. The installation, configuration, and use of BackupPC is outlined in detail in the online documentation on their Website.

BackupPC has been chosen for several reasons. Primarily, BackupPC is open source software that is available for download at no cost. This supports the HFM directive to move in the direction of open source to minimize the costs associated with building and maintaining a business network. Another reason is that BackupPC utilizes SMB to backup data from remote hosts.[44] Since the ports used for SMB communication are already open at the firewall, additional ports will not need to be opened. In addition, an SMB user account and a system account are necessary to access the target host. As these accounts already exist, the risk of server compromise is not increased at this level by using this software.

The HFM backup plan is relatively simple. A full backup of the entire system is performed on a monthly basis. A full backup of the following is executed weekly:

- /data
- /etc/passwd
- /etc/shadow
- /etc/samba
- /var/log
- /home

An incremental backup of /data and /home is executed nightly. The backup tapes are stored off-site in a fireproof safe. Tapes on-site for use are stored in the company safe until loaded into the workstation at the close of business each day. The owner is always the last to leave the shop, and loads the tape prior to leaving. Since this is not the most reliable method of maintaining backups, a revised solution is being worked on and will be put into effect at the six-month mark.

7.2   Updates
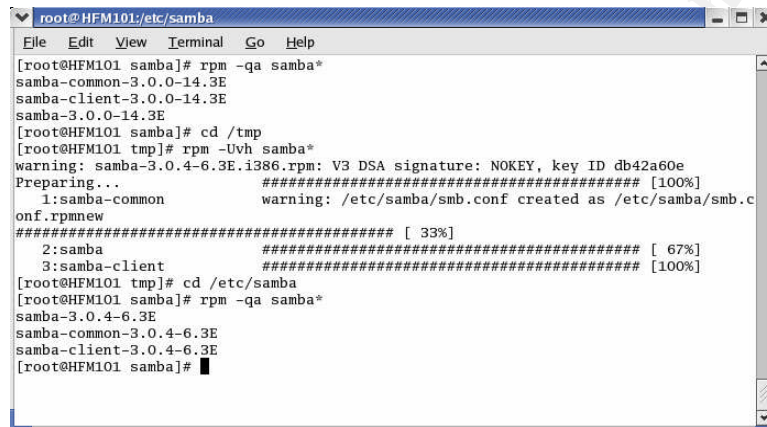
The primary purpose for procuring the RHN support contract is to allow easy access to patches and updates as necessary. Since HTTP traffic from HFM101 is blocked, the up2date command cannot be used for maintaining current patch levels. The two methods that are utilized for communicating update information are the RHN Errata email notifications that will be sent to the primary RHN account email address, and weekly manual checks of the Errata listed on www.rhn.redhat.com. Additional information regarding vulnerabilities may be researched at the Common Vulnerabilities and Exposures Website at http://cve.mitre.org.[45] When necessary patches are identified, they will be downloaded and applied following the package update procedure. An example

---

[44] Barratt, Overview
[45] CVE

of a recent RHN Errata advisory that addressed a Samba vulnerability is RHSA-2004:259-23, which was brought to HFM's attention via an email update. This email example is posted in Appendix M.[46]

By following the update procedure, the packages `samba-common-3.0.0-14.3E`, `samba-client-3.0.0-14.3E`, and `samba-3.0.0-14.3E` are updated simultaneously by executing the command **#rpm –Uvh samba***, followed by the command **#rpm –qa samba*** to verify the updates are successful. The SMB service is restarted, and access to the shares is successfully tested from the workstations.

Figure 28 – Samba Update

7.3   System Integrity Checks

An entry in `/etc/cron.daily` ensures a Tripwire integrity check occurs daily. The Integrity Check Reports are stored in `/var/lib/tripwire/report,` and are manually viewed daily using the command **#twprint –m r –r *filename***. The report names are saved in a *hostname-date-time.twr* format.
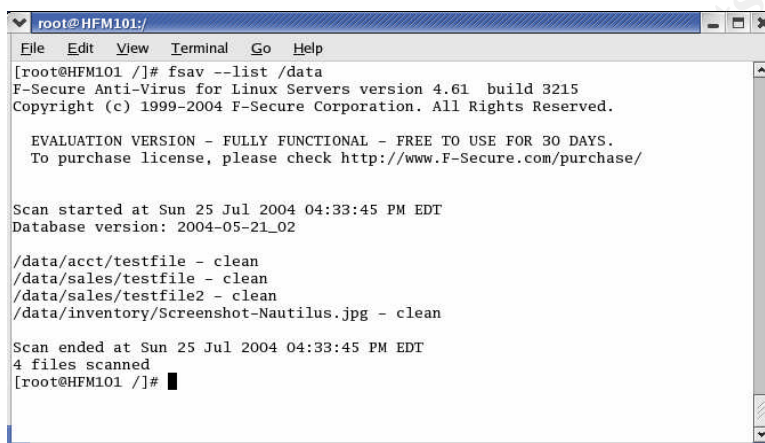
Figure 29 – Tripwire Report Example

---

[46] Red Hat Network Alert

7.4 Antivirus

Since a daily scan has already been configured, additional antivirus updates will be completed manually as necessary. The configuration file, `/etc/opt/f-secure/fsav/fsav.conf` is modified to log to the system log. To execute a manual scan on `/data` for example, the command **#fsav /data** is executed. Additional options for manual or automatic use are available in the `fsav` man pages, or by executing **#fsav -help**.

Figure 30– Manual Execution of F-Secure Antivirus for Linux Servers Evaluation Copy

7.5 Log Files

Log files are manually viewed on a routine basis using the commands `more`, `less`, or `tail`.   Since an X server is not installed on HFM101, a utility such as `redhat-logviewer` is not accessible. The log files are located in the `/var/log` directory, and include the system log, which is located in the `/var/log/messages` file. To view the last 15 lines of the security log, execute the command **#tail -n 15 /var/log/secure**. To view entries as they are logged, execute the command **#tail -f /var/log/secure**.

Figure 31 – Review Security Log Example

7.6   *Port Scans*

7.6.1   *Nmap*

Two separate utilities will be used to scan for open ports on HFM101: Nmap and
Nessus. "Nmap is a free open source utility for network exploration or security
auditing. It was designed to rapidly scan large networks, even though it works
fine against single hosts."[47]   Nmap is freely available for download from
http://www.insecure.org/nmap/, although it is also installed by default on Red Hat
Enterprise Workstation 3. A typical scan using Nmap is executed with the
command `#nmap -sS -O -v` *ip address*. Checking the Nmap man pages, the -
sS option invokes a TCP SYN ACK scan. The -O option creates an OS
fingerprint and compares it to a list of known OS fingerprints, and the - v option
is for verbose mode. According to the man pages, using the -v option twice
produces greater output. The output from `#nmap -sS -O -v -v 192.168.0.51` is
posted in Appendix N.

7.6.2   *Nessus*

Nessus is a security scanner that may remotely audit a system and determine
whether the system is vulnerable to compromise by scanning the available ports
and the corresponding running services.[48]   Nessus is downloaded for free from
http://www.nessus.org/download.html and installed on the Linux workstation.
Updates to configure Nessus for recent vulnerabilities are obtained by executing
the command `#nessus-update-plugins`. To use Nessus, and access the GUI
utility, execute the command `#nessus`. To minimize scan time for frequent scans,
execute Nmap first, and then execute Nessus against the ports identified in
Nmap. Nessus may also be configured to execute an Nmap scan. Detailed
information regarding the use of Nessus is available at www.nessus.org.   A
complete scan of all ports on the system should be executed once a month. A
scan on HFM101 is executed with all installed plug-ins enabled.

7.7   *TARA*

TARA has been installed under `/etc/opt/tara-3.0.3` and is executed from this
directory by executing the command `#./tara`. According to the README file under
`/etc/opt/tara-3.0.3`, "TARA is a set of scripts that scan a UNIX based file
system for security problems."[49] This is a good utility to use to during the
hardening process to locate and secure any missed items. It is also a good utility
to use after executing updates or installing applications to verify the new
packages have not created any potential security hazards. Sample output from a
TARA scan is posted in Appendix O.

---

[47] What is Nmap
[48] Deraison
[49] TARA README

8.0 Test and Verify the Setup

Prior to putting the system into production, the system--and measures taken to protect it--must be tested. Almost two dozen separate steps have been implemented to secure HFM101, and all have been tested. For demonstration purposes, the following five tests are described:

- Enabled GRUB password
- Disabled root login from the console and SSH
- Disabled woodtwo, woodthree, woodfour login from the console and SSH
- Restricted floppy and CDROM device mount
- Tested Samba account access

8.1 GRUB Password

A GRUB password was configured during the initial OS installation to prevent compromise to the GRUB loader utilities. Unwanted access to the GRUB utilities poses a threat because single-user mode is entered from GRUB, along with the ability to pass additional kernel arguments. To test this configuration, the server is powered up. Upon reaching the GRUB screen, enter the P key to prompt for a password. Enter the incorrect password for demonstration, and the message "Failed! Press any key to continue…" is produced. This is cleared, and the correct password is entered to grant access to the utility.
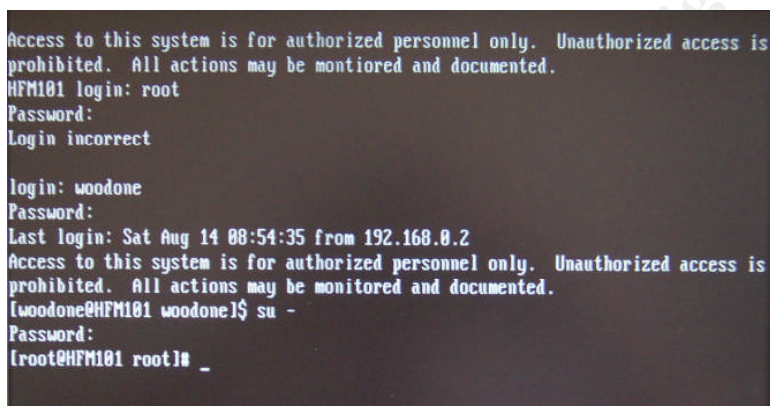
Figure 32 – Failed GRUB Login Example

8.2   *Root Login*

Root login from any console or SSH session has been disabled in
/etc/securetty and /etc/ssh/sshd_config. There are two simple tests to verify
this; from both a console and an SSH session.

8.2.1   From the Console

Power up HFM101 and attempt to login as root at the login prompt. "Login
incorrect" is the message produced.
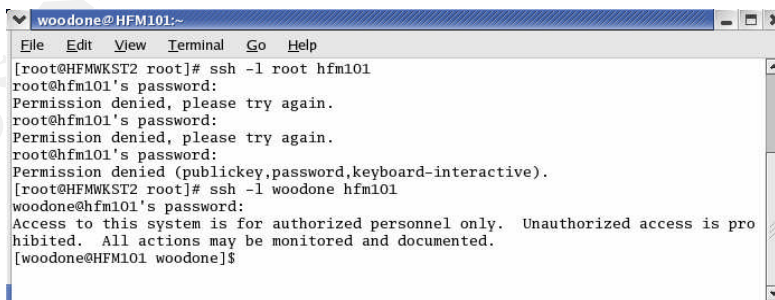
Figure 33 – Failed Root Console Login

8.2.2   From SSH

For the SSH test, open up a terminal from the Linux workstation. Use an SSH
utility such the OS default or F-Secure SSH.[50] PuTTY,[51] a free utility that is
downloadable from the Internet may be used from a Windows workstation.
Execute the command #ssh –l root hfm101. The message "Permission denied,
please try again" is produced. To verify SSH is functioning properly, and that the
denied access was the proper response to an attempt to login as root, a
successful login using woodone is executed.

Figure 34 – Denied Root Login via SSH

---

[50] F-Secure
[51] PuTTY

8.3 User Account Login

The same two tests may also be used to test direct or SSH login for the accounts woodtwo, woodthree, and woodfour, all of which have been restricted from console access. This was done by configuring the local $SHELL variable for each account to /bin/false. This prevents the accounts from gaining access to an interactive shell, and thereby prevents login. For example, if woodtwo attempts to login via SSH, the following entries in /var/log/messages are produced:

> "HFM101 sshd(pam_unix)[4945] session opened for user woodtwo by (uid=501)"
> "HFM101 sshd(pam_unix)[4945] session closed for user woodtwo"
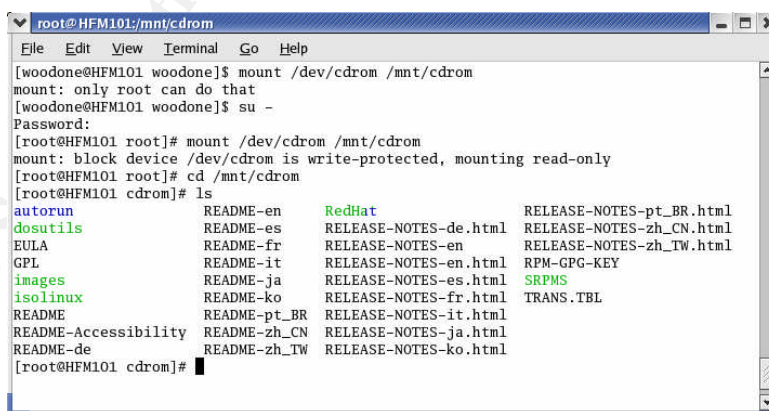
A denied attempt by woodfour to login directly from the server console will produce the following entries in /var/log/messages:

> "HFM101 login(pam_unix)[846]: authentication failure;
> logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=woodfour"
>
> "HFM101 login[846]: FAILED LOGIN 1 FROM (null) FOR woodfour,
> Authentication failure"

8.4 Removable Media Device Mount

One of the additional levels of security implemented to protect against installation of unwanted files on the physical box is the restriction of the mounting of the floppy and CDROM devices. Since the options set in /etc/fstab for the floppy and CDROM state –nouser, only root is able to mount either device. To verify only root may mount either device, the primary system account is used to test the restriction by executing the commands $mount /mnt/floppy and $mount /mnt/cdrom. The message "mount: only root can do that" is posted. Once denied, $su and attempt the mounts again; they should be successful.

Figure 35 – CDROM Mount Test

8.5   Test Samba Account Access

A major configuration for Samba is share access permissions. On HFM101, access to the `/data` subdirectories is granted by group membership.   A good test of this is to attempt access to restricted directories. As an example, `woodfour` is logged into the Samba server from a Linux workstation. Since `woodfour` is a member of the `shop` group, access to `smb://hfm101/maintenance` is successful. However, attempts to access `smb://hfm101/purchasing` produces the following message:

> "You do not have the permissions necessary to view the contents of 'purchasing'."
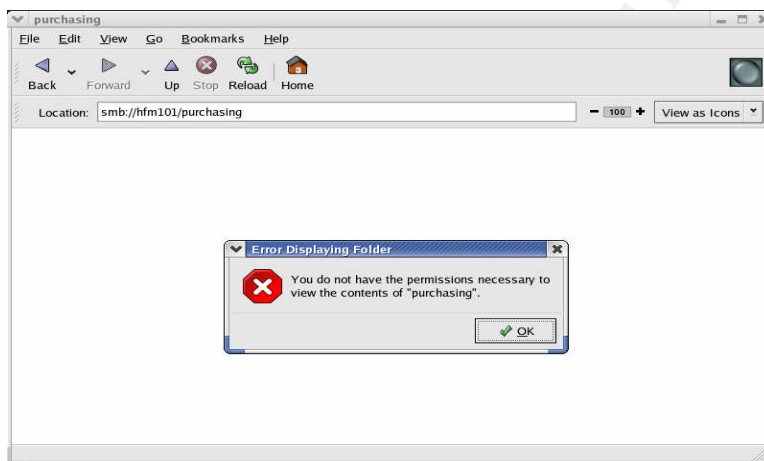
Figure 36 – Samba Share Access

9.0   Conclusion

This paper was written to provide an educational guide for small, independent business entrepreneurs who may believe they do not have the resources to build a network, much less one that is secure.   Many of these owners may have migrated to electronic office management without foreseeing the potential of creating a more robust electronic environment, or realizing the probable risks involved in having all company data accessible from one system. The intent of this guide has been to provide basic instruction and to foster ideas on how to build and maintain a small, secure network through demonstration and the presentation of several potential security configurations. Other ideas presented illustrate that not all requirements may be available immediately, however through careful planning the desired specifications may be realized over a period of time.

Considering the diminutive size of HFM101 and the fictitious HFM network, applying all of the security configurations presented may seem overstated. This may be the case, however not all of the potential configurations may suit the requirements of all networks, therefore it was necessary to demonstrate several

possibilities. There are numerous possible security configurations and utilities available that were not mentioned in this paper, yet that does not indicate they should not be utilized if suitable to the environment being secured. In addition, using Samba for file and print services may not suit the requirements for a particular environment. With these thoughts in mind, this paper should be utilized as a guideline for starting a small business network on a limited budget, and securing the network to the level of necessity required.

Online References

Samba "Samba: Welcome to the Samba Web Pages." 10 June 2004.
http://us2.samba.org/samba/samba.html.

MD5 SUM. "How to Check MD5 Sums on a Linux ISO Image." Linux ISO.org.
2002. 10 June 2004. http://www.linuxiso.org/viewdoc.php/verifyiso.html.

Eckstein, Robert, David Collier-Brown, and Jay Ts. "Learning the Samba."
Using Samba. 2nd ed. Ed. Andy Oram. Sebastopol: O'Reilly & Associates, 2003.
10 June 2004
http://www.faqs.org/docs/samba/ch01.html.

Red Hat Enterprise Linux "Red Hat Enterprise Linux ES: For Small/mid-range
Servers." Red Hat, Inc. 2004. 10 June 2004.
http://www.redaht.com/software/rhel/es/.

RHN "Red Hat Network: Welcome to Red Hat Network." Red Hat, Inc. 2004. 10
June 2004. www.rhn.redhat.com.

Sharpe, Richard. "Just What is SMB: What is SMB." 8 Oct. 2002. 10 June
2004. http://www.samba.org/cifs/docs/what-is-smb.html.

Tripwire "Home Tripwire.org: Welcome to Tripwire.org." Tripwire, Inc. 10 June
2004. www.tripwire.org.

TARA "Tiger Analytical Research Assistant." Advanced Research Corporation.
15 Aug. 2002. 10 June 2004. http://www-arc.com/tara/index.shtml.

Deraison, Renaud. "Nessus: Introduction." 2004. 10 June 2004.
http://www.nessus.org/intro.html.

Nmap. "Nmap: Introduction." Insecure.org. 10 June 2004.
www.insecure.org/nmap.

Egevang, Kjeld, and Paul Francis. RFC 1631: The IP Network Address
Translator (NAT). May 1994. www.faqs.org. 10 June 2004.
www.faqs.org/rfcs/rfc1631.html.

John the Ripper. "John the Ripper Password Cracker." DataForce, ISP. 10
June 2004 www.openwall.com/john.

Berger, Tom. System Services. MandrakeSoft. 2002. Start Linux. 10 June
2004. http://www.start-linux.com/articles/article_164.php.

Rhnsd. "rhnsd." Red Hat. 2000. 4th Berkeley Distribution. February 9, 2001. 10 June 2004. http://gd.tuwien.ac.at/linuxcommand.org/man_pages/rhnsd8.html.

Errata. "Red Hat Network: Errata Relevant to Your Systems." Red Hat, Inc. 2004. 10 June 2004. https://rhn.redhat.com/network/errata/errata_list/relevant.pxt.

What is Tripwire. "Tripwire Open Source, Linux Edition FAQ: What is Tripwire." Tripwire, Inc. 10 June 2004. http://www.tripwire.org/qanda/index.php#1.

Veillard, Daniel. "RPM Resource Tripwire." 10 June 2004. http://rpmfind.net/linux/rpm2html/search.php?query=tripwire&submit=Search.

Tripwire.com. "Tripwire: Tripwire Products." Tripwire, Inc. 2004. 10 June 2004. http://www.tripwire.com/products/purchase/index.cfm.

Tripwire Download. "Downloads Tripwire.org: Downloads." Tripwire, Inc. 10 June 2004. http://www.tripwire.org/downloads/index.php.

Sourceforge. "Project:Tripwire:Summary." Open Source Technology Group. 2004. 10 June 2004. http://sourceforge.net/projects/tripwire/.

CVE. "Common Vulnerabilities and Exposures: The Key to Information Sharing." The MITRE Corporation. 4 Aug. 2004. 7 Aug. 2004. http://cve.mitre.org/.

Red Hat Network Alert. "RHN Errata Alert: Updated Samba Packages Fix Vulnerabilities." Email to xxxxxxxx@xxxxxxxxxxxx.xxx. 22 July 2004.

Perl. "The Perl Directory: About Perl." The Perl Foundation. 2004. 1 Aug. 2004. http://www.perl.org/about.html.

Barratt, Craig. "BackupPC: BackupPC Documentation." Sourceforge. 2004. 1 Aug. 2004. http://backuppc.sourceforge.net/faq/BackupPC.html.

Barratt, Craig. "BackupPC: BackupPC Documentation: Overview." 2004. Sourceforge. 1 Aug. 2004. http://backuppc.sourceforge.net/faq/BackupPC.html.

What is Nmap. "Nmap: Introduction." Insecure.org. 10 June 2004. www.insecure.org/nmap.

F-Secure. "F-Secure: F-Secure SSH 5.3 Client for Windows." 1 Aug. 2004. http://www.f-secure.com/estore/sshclientwin.shtml.

Dell. "Easy As Dell." Dell. 2004. 10 June 2004. http://www.dell.com.

F-Secure Linux. "F-Secure Anti-Virus for Linux." 1 Aug. 2004.
http://www.f-secure.com/products/anti-virus/linux/.

Putty. "Putty Download Page." 3 Aug. 2004. 7 Aug 2004.
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Openwall. "John the Ripper Password Cracker." DataForce, ISP. 10 June
2004. www.openwall.com/john.

Murdoch, Don. "Building a Secured OS for a Root Certificate Authority." Feb.
2004. 10 June 2004.
http://www.giac.org/practical/GCUX/Don_Murdoch_GCUX.pdf. Page 43.

Armstrong, Mike. "Red Hat Java Applications Server Step-by-Step." March
2004. 10 June 2004.
http://www.giac.org/practical/GCUX/Michael_Armstrong_GCUX.pdf. Page 26.

F-Secure Antivirus. "F-Secure Anti-Virus Download." 10 June 2004.
https://www.europe.f-secure.com/download-purchase/download-forms/anti-virus-
linux-srv.shtml.

TARA README. "Tiger Analytical Research Assistant." Advanced Research
Corporation. 15 Aug. 2002. 10 June 2004. http://www-arc.com/tara/index.shtml.

References in Print

Koconis, David, Jim Murray, Jos Purvis, and Darrin Wassom. "Securing Linux."
Securing Linux A Survival Guide for Linux Security Version 1.0. Ed. Mitch Baker,
Guy Bruneau, John Moore, and Bill Stearns. Sans Press, 2003. 6-14.

Fuller, Johnray. "The proc File System." Red Hat Enterprise Linux: Reference
Guide. Raleigh: Red Hat, Inc. Page 73.

Nemeth, Evi, et al. "Adding New Users." UNIX System Administration Handbook.
3rd ed. Upper Saddle River: Prentice Hall, 2001. Page 78.

Fuller, Johnray. "TCP Wrappers and xinetd." Red Hat Enterprise Linux:
Reference Guide. Raleigh: Red Hat, Inc. 2003. Page 240.

Ha, John, and Johnray Fuller. "Workstation Security." Red Hat Enterprise Linux:
Security Guide. Raleigh: Red Hat, Inc. 2003. 26-30.

Fox, Tammy. "Console Access." Red Hat Enterprise Linux: System
Administration Guide. Raleigh: Red Hat, Inc. 2003. Page 227.

Yuen, Rosanna. "Setting Up Samba." Wide Open 1 (2004): 44-52.

Appendix A - /etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda8
#          initrd /initrd-version.img
#boot=/dev/sda1
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
password --md5 $1$vNgmbL/4$dwoAOrB2DJ7xay20Vuase0
title Red Hat Enterprise Linux ES (2.4.21-4.ELsmp)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-4.ELsmp ro root=LABEL=/ hdc=ide-scsi
        initrd /initrd-2.4.21-4.ELsmp.img
title Red Hat Enterprise Linux ES-up (2.4.21-4.EL)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-4.EL ro root=LABEL=/ hdc=ide-scsi
        initrd /initrd-2.4.21-4.EL.img
```

Appendix B – Modified `/etc/grub.conf`

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this
file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda8
#          initrd /initrd-version.img
#boot=/dev/sda1
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
password --md5 $1$6z7azdXM$WaNWx6ayDBlGZsa8wRPNm0
title Red Hat Enterprise Linux ES (2.4.21-15.0.2.EL)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-15.0.2.EL ro root=LABEL=/ hdc=ide-scsi
        initrd /initrd-2.4.21-15.0.2.EL.img
#title Red Hat Enterprise Linux ES (2.4.21-4.ELsmp)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-4.ELsmp ro root=LABEL=/ hdc=ide-scsi
        initrd /initrd-2.4.21-4.ELsmp.img
title Red Hat Enterprise Linux ES-up (2.4.21-4.EL)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-4.EL ro root=LABEL=/ hdc=ide-scsi
        initrd /initrd-2.4.21-4.EL.img
```

Appendix C – /etc/ssh/sshd_config

```
#         $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
PermitRootLogin no
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in
/etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
```

```
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of
'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
#Banner /some/path
#VerifyReverseMapping no

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Appendix D - /etc/inittab

```
#
# inittab        This file describes how the INIT process should set up
#                the system in a certain run-level.
#
# Author:        Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#                Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#    0 - halt (Do NOT set initdefault to this)
#    1 - Single user mode
#    2 - Multiuser, without NFS (The same as 3, if you do not have
networking)
#    3 - Full multiuser mode
#    4 - unused
#    5 - X11
#    6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
~~:s:wait:/sbin/sulogin
# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

[root@HFM101 root]# cp /etc/inittab /etc/inittab.orig
[root@HFM101 root]# vi /etc/inittab.orig
[root@HFM101 root]# more /etc/inittab
#
# inittab        This file describes how the INIT process should set up
#                the system in a certain run-level.
#
# Author:        Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#                Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#    0 - halt (Do NOT set initdefault to this)
#    1 - Single user mode
#    2 - Multiuser, without NFS (The same as 3, if you do not have
networking)
#    3 - Full multiuser mode
#    4 - unused
#    5 - X11
#    6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
```

52

```
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting
Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown
Cancelled"


# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm –nodaemon
```

Appendix E - /etc/login.defs

```
# *REQUIRED*
#    Directory where mailboxes reside, _or_ name of file, relative to
the
#    home directory.  If you _do_ define both, MAIL_DIR takes
precedence.
#    QMAIL_DIR is for Qmail
#
#QMAIL_DIR       Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE       .mail

# Password aging controls:
#
#        PASS_MAX_DAYS   Maximum number of days a password may be used.
#        PASS_MIN_DAYS   Minimum number of days allowed between password
changes.
#        PASS_MIN_LEN    Minimum acceptable password length.
#        PASS_WARN_AGE   Number of days warning given before a password
expires.
#
PASS_MAX_DAYS   90
PASS_MIN_DAYS   2
PASS_MIN_LEN    8
PASS_WARN_AGE   7


#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                         500
UID_MAX                         60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                         500
GID_MAX                         60000

#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD    /usr/sbin/userdel_local

#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is ORed with the -m flag on
# useradd command line.
#
CREATE_HOME     yes
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
woodone:x:500:500::/home/woodone:/bin/bash
```

Appendix G - /etc/shadow

With unlocked accounts:

```
root:$1$XnZOWgd7$l1MmTyzwGkgDZS3to2OnC.:12604:0:99999:7:::
bin:!*:12604:0:99999:7:::
daemon:*:12604:0:99999:7:::
adm:*:12604:0:99999:7:::
lp:*:12604:0:99999:7:::
sync:!*:12604:0:99999:7:::
shutdown:*:12604:0:99999:7:::
halt:*:12604:0:99999:7:::
nobody:*:12604:0:99999:7:::
rpm:!:12604:0:99999:7:::
vcsa:!!:12604:0:99999:7:::
nscd:!!:12604:0:99999:7:::
sshd:!!:12604:0:99999:7:::
pcap:!!:12604:0:99999:7:::
woodone:$1$ktbRYxQV$OQJN64jj86eSUsr1hRUnU.:12605:0:90:7:::
```


With locked accounts:

```
bin:!*:12604:0:99999:7:::
daemon:!*:12604:0:99999:7:::
adm:!*:12604:0:99999:7:::
lp:!*:12604:0:99999:7:::
sync:!*:12604:0:99999:7:::
shutdown:!*:12604:0:99999:7:::
halt:!*:12604:0:99999:7:::
nobody:!*:12604:0:99999:7:::
rpm:!!:12604:0:99999:7:::
vcsa:!!:12604:0:99999:7:::
nscd:!!:12604:0:99999:7:::
sshd:!!:12604:0:99999:7:::
pcap:!!:12604:0:99999:7:::
woodone:$1$ktbRYxQV$OQJN64jj86eSUsr1hRUnU.:12605:0:90:7:::
```

Appendix H - /etc/fstab

Default file

```
LABEL=/            /                      ext3    defaults        1 1
LABEL=/boot        /boot                  ext3    defaults        1 2
LABEL=/data        /data                  ext3    defaults        1 2
none               /dev/pts               devpts  gid=5,mode=620  0 0
LABEL=/home        /home                  ext3    defaults        1 2
none               /proc                  proc    defaults        0 0
none               /dev/shm               tmpfs   defaults        0 0
LABEL=/tmp         /tmp                   ext3    defaults        1 2
LABEL=/usr         /usr                   ext3    defaults        1 2
LABEL=/var         /var                   ext3    defaults        1 2
/dev/sda9          swap                   swap    defaults        0 0
/dev/cdrom         /mnt/cdrom             udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0           /mnt/floppy            auto    noauto,owner,kudzu 0 0
```

Modified file

```
LABEL=/            /                      ext3    defaults        1 1
LABEL=/boot        /boot                  ext3    defaults        1 2
LABEL=/data        /data                  ext3    defaults        1 2
none               /dev/pts               devpts  gid=5,mode=620  0 0
LABEL=/home        /home                  ext3    defaults        1 2
none               /proc                  proc    defaults        0 0
none               /dev/shm               tmpfs   defaults        0 0
LABEL=/tmp         /tmp                   ext3    defaults        1 2
LABEL=/usr         /usr                   ext3    defaults        1 2
LABEL=/var         /var                   ext3    defaults        1 2
/dev/sda9          swap                   swap    defaults        0 0
/dev/cdrom         /mnt/cdrom             udf,iso9660 noauto,nouser,kudzu,ro 0 0
/dev/fd0           /mnt/floppy            auto    noauto,nouser,kudzu 0 0
```

Appendix I – Tripwire Integrity Check Report

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:        root
Report created on:          Sat 24 Jul 2004 02:50:14 PM EDT
Database last updated on:   Never

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

Host name:                  HFM101
Host IP address:            127.0.0.1
Host ID:                    None
Policy file used:           /etc/tripwire/tw.pol
Configuration file used:    /etc/tripwire/tw.cfg
Database file used:         /var/lib/tripwire/HFM101.twd
Command line used:          tripwire --check

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

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

Rule Name	Severity Level	Added	Removed	M odified
Invariant Directories	66	0	0	0
Temporary directories	33	0	0	0
Tripwire Data Files	100	0	0	0
Critical devices	100	0	0	0
User binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Libraries	66	0	0	0
Critical system boot files	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	100	0	0	0
Application Information Programs				
	100	0	0	0
Shell Related Programs	100	0	0	0
Operating System Utilities	100	0	0	0
Critical Utility Sym-Links	100	0	0	0
Shell Binaries	100	0	0	0
Critical configuration files	100	0	0	0
System boot changes	100	0	0	0
OS executables and libraries	100	0	0	0
Security Control	100	0	0	0

```
   Login Scripts                        100           0          0          0
   Root config files                    100           0          0          0

Total objects scanned:  14355
Total violations found:   0

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

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

No violations.

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

No Errors

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

Appendix J - `/etc/samba/smbusers` & `/etc/samba/smbpasswd`

`/etc/samba/smbusers`

```
# Unix_name = SMB_name1 SMB_name2 ...
woodone = woodone
woodtwo = woodtwo
woodthree = woodthree
woodfour = woodfour
```

`/etc/samba/smbpasswd`

```
woodone:500:CACC6077A11950C1AAD3B435B51404EE:9B65B92F989A29BD589FD0BED4
A69031:[U          ]:LCT-40F5BB41:
woodtwo:502:CACC6077A11950C1AAD3B435B51404EE:9B65B92F989A29BD589FD0BED4
A69031:[U          ]:LCT-40F1E1D9:
woodthree:503:CACC6077A11950C1AAD3B435B51404EE:9B65B92F989A29BD589FD0BE
D4A69031:[U          ]:LCT-40F1E1DF:
woodfour:504:CACC6077A11950C1AAD3B435B51404EE:9B65B92F989A29BD589FD0BED
4A69031:[U          ]:LCT-40F1E1E7:
```

Appendix K - /etc/sysconfig/iptables

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 137 -
j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 138 -
j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 139 -
j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 145 -
j ACCE
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Appendix L - `/etc/samba/smb.conf`

```
[global]
        workgroup = HFM
        server string = hfm101
        wins support = yes
        wins server = 192.168.0.51
        hosts allow = 192.168.0/24 127.
        security = user
        encrypt passwords = yes
        smb passwd file = /etc/samba/smbpasswd
        printcap name = /etc/printcap
        load printers = yes
        printing = cups

[homes]
        comment = Home directories
        valid users = woodone,woodtwo,woothree,woodfour
        browseable = no
        writable = yes

[acct]
        comment = Accounting data
        path = /data/acct
        valid users = @woodone
        writable = yes

[advertising]
        comment = Advertising data
        path = /data/acct
        valid users = @frontoffice
        writable = yes
[design]
        comment = Design data
        path = /data/design
        valid users = @frontoffice
        writeable = yes

[inventory]
        comment = Inventory data
        path = /data/inventory
        valid users = @shop
        writeable = yes

[maintenance]
        comment = Maintenance data
        path = /data/maintenance
        valid users = @shop
        writeable = yes

[personnel]
        comment = Personnel data
        path = /data/personnel
        valid users = @woodone
        writeable = yes

[purchasing]
        comment = Purchasing data
        path = /data/purchasing
        valid users = @frontoffice
        writeable = yes

[sales]
        comment = Sales data
```

```
                path = /data/sales
                valid users = @frontoffice
                writeable = yes

        [printers]
                comment = Printers
                path = /var/spool/samba
                browseable = no
                public = yes
                guest = yes
                writable = no
                printable = yes
                use client driver = yes
```

Appendix M – Errata Alert

-----Original Message-----
From: Red Hat Network Alert [mailto:xxxxxxxxl@rhn.redhat.com]
Sent: Thursday, July 22, 2004 8:38 PM
To: xxxxxxxx@xxxxxxxxxxxx.xxx
Subject: RHN Errata Alert: Updated samba packages fix vulnerabilities

Red Hat Network has determined that the following advisory is applicable to one
or more of the systems you have registered:

Complete information about this errata can be found at the following
location:
    https://rhn.redhat.com/network/errata/errata_details.pxt?eid=2218

Security Advisory - RHSA-2004:259-23

--
Summary:
Updated samba packages fix vulnerabilities

Updated samba packages that fix buffer overflows, as well as other various bugs,
are now available.

Description:
Samba provides file and printer sharing services to SMB/CIFS clients.

Evgeny Demidov discovered a flaw in the internal routine used by the Samba
Web Administration Tool (SWAT) in Samba versions 3.0.2 through 3.0.4. When
decoding base-64 data during HTTP basic authentication, an invalid base-64
character could cause a buffer overflow. If the SWAT administration service is
enabled, this flaw could allow an attacker to execute arbitrary code. The
Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the
name CAN-2004-0600 to this issue.

Additionally, the Samba team discovered a buffer overflow in the code used to
support the 'mangling method = hash' smb.conf option. Please be aware that the
default setting for this parameter is 'mangling method = hash2'
and therefore not vulnerable. The Common Vulnerabilities and Exposures
project (cve.mitre.org) has assigned the name CAN-2004-0686 to this issue.

This release includes the updated upstream version 3.0.4 together with
backported security patches to correct these issues as well as a number of
post-3.0.4 bug fixes from the Samba subversion repository.

The most important bug fix allows Samba users to change their passwords if
Microsoft patch KB 828741 (a critical update) had been applied.

All users of Samba should upgrade to these updated packages, which resolve
these issues.

--

Taking Action

You may address the issues outlined in this advisory in two ways:

  - select your server name by clicking on its name from the list
    available at the following location, and then schedule an
    errata update for it:
        https://rhn.redhat.com/network/systemlist/system_list.pxt

  - run the Update Agent on each affected server.

Changing Notification Preferences

To enable/disable your Errata Alert preferences globally please log in to RHN
and navigate from "Your RHN" / "Your Account" to the "Preferences" tab.

      URL: https://rhn.redhat.com/network/my_account/my_prefs.pxt

You can also enable/disable notification on a per system basis by selecting an
individual system from the "Systems List". From the individual system view click
the "Details" tab.

Affected Systems List

This Errata Advisory may apply to the systems listed below. If you know that this
errata does not apply to a system listed, it might be possible that the package
profile for that server is out of date. In that case you should run 'up2date -p' as
root on the system in question to refresh your software profile.

There is 1 affected system registered in 'Your RHN' (only systems for which you
have explicitly enabled Errata Alerts are shown).

Release   Arch   Profile Name

```
-------- -------- ------------
3ES      i686     hfm101
```

The Red Hat Network Team

This message is being sent by Red Hat Network Alert to:
   RHN user login: xxxxxxxxxx
   Email address on file: xxxxxxxx@xxxxxxxxxxxx.xxx

If you lost your RHN password, you can use the information above to retrieve it
by email from the following address:
   https://rhn.redhat.com/forgot_password.pxt

To cancel these notices, go to:
   https://rhn.redhat.com/oo.pxt?uid=3580861&oid=4130140

Appendix N – Nmap Output Example

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host HFM101 (192.168.0.51) appears to be up ... good.
Initiating SYN Stealth Scan against HFM101 (192.168.0.51)
Adding open port 22/tcp
Adding open port 445/tcp
Adding open port 139/tcp
The SYN Stealth Scan took 1 second to scan 1601 ports.
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
Interesting ports on HFM101 (192.168.0.51):
(The 1598 ports scanned but not shown below are in state: closed)
Port        State        Service
22/tcp      open         ssh
139/tcp     open         netbios-ssn
445/tcp     open         microsoft-ds
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=4B9B18%IPID=Z%TS=100HZ)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%
DAT=E)

Uptime 0.001 days (since Sun Aug 15 16:36:14 2004)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4954904 (Good luck!)
TCP ISN Seq. Numbers: 79033E72 78EDB888 78FCA441 79A53F34 78DAEC23
793BAD24
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
```

Appendix O – TARA Output

```
Security scripts *** 3.0.2 ARC, 2002.0513.2100 ***
Sat Aug 7 17:48:11 EDT 2004
08:48> Beginning security report for HFM101 (2003 Linux 2.4.21-
4.ELsmp).

# Performing check of passwd files...

# Performing check of group files...

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID adm is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID bin is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID daemon is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID lp is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID nobody is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID nscd is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID pcap is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID rpm is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID smmsp is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID sshd is disabled, but still has a valid
shell.
--WARN-- [acc001w] Login ID vcsa is disabled, but still has a valid
shell.

# Performing check of /etc/hosts.equiv and .rhosts files...

# Checking accounts from /etc/passwd...
# Performing check of /etc/default/login, /securetty, and
/etc/ttytab...


# Performing check of PATH components...
# Only checking user 'root'
--WARN-- [path002w] /bin/rpm in root's PATH from default is not owned
by root
        (owned by rpm).
--WARN-- [path002w] /usr/bin/gendiff in root's PATH from default is not
owned
        by root (owned by rpm).
--WARN-- [path002w] /usr/bin/rpm2cpio in root's PATH from default is
not owned
        by root (owned by rpm).
--WARN-- [path002w] /usr/bin/rpmdb in root's PATH from default is not
owned by
        root (owned by rpm).
--WARN-- [path002w] /usr/bin/rpmquery in root's PATH from default is
not owned
        by root (owned by rpm).
--WARN-- [path002w] /usr/bin/rpmsign in root's PATH from default is not
owned
        by root (owned by rpm).
```

68

```
--WARN-- [path002w] /usr/bin/rpmverify in root's PATH from default is
not
          owned by root (owned by rpm).

# Performing check of anonymous FTP...
--WARN-- [ftp006w] Anonymous FTP enabled, but directory does not exist.

# Performing checks of mail aliases...

# Performing check of `cron' entries...

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
# Checking inetd entries from /etc/xinetd.d

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm001w] /etc/exports should not have group read.
--WARN-- [perm001w] /etc/exports should not have world read.
--WARN-- [perm001w] /etc/fstab should not have group read.
--WARN-- [perm001w] /etc/fstab should not have world read.

# Performing signature check of system binaries...
--ERROR-- [init005e] Don't have required file SIGNATURE_FILE.

# Checking for known intrusion signs...
# Testing for promiscuous interfaces
# Testing for backdoors in inetd.conf

# Performing check of files in system mail spool...

# Performing system specific checks...
# Performing checks for Linux/2...
# Running './scripts/check_sendmail'...

# Checking sendmail...
# Running './scripts/check_printcap'...

# Checking printer configuration files...
```