



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Installing and Securing a Mail Server

Using SuSE Linux, Professional 7.3

Submission for GIAC UNIX System Administrator (GCUX) Certification
Practical Assignment (v.1.8) (October 2001), Option 1
San Diego, CA SANS Conference

Joanne K. Joki

1. Background and Assignment:	2
2. Security Review and Risk Assessment:	2
3. Services and Software Packages required to be Installed and Secured:.....	4
4. Initial Description of Server:.....	4
5. Pre-installation Activities:.....	6
6. System Design:.....	8
7. Basic Installation Instructions and Security Tips during Installation:.....	9
8. Securing the Server/Network Configuration:.....	14
9. Configuring and Securing sendmail:	22
10. Install and Configure Tripwire:.....	24
11. Post Installation Testing:	28
12. On-going Maintenance and Management Considerations:	33
13. Final Steps:	35
Appendices	37
Appendix A: Sample Secure Configuration Files for the Environment.....	38
Appendix B: SAINT Report.....	42
Bibliography	43
Web Site References	44

1. Background and Assignment:

Recently, the client company contracted a web page be constructed through an ISP and had email accounts created for each of their managers and sales people. Although the client wishes to begin receiving sales inquiries and receiving and initiating customer correspondence through email, the client does not want to allow all of their employees direct or dial-up access to the web.

After evaluating several options, it was decided that the least amount of affordable risk would be obtained by utilizing a LINUX-based Sendmail system working in conjunction with IMAP/POP3 desktop email clients. The server will perform automated periodic connections to the ISP through ISDN to collect and send mail as well as deliver it to employee desktops. The client has purchased a NetScreen-5xp firewall appliance. The NetScreen-5XP offers 10 Mbps performance with a simple, wizard-driven interface for easy installation by non-security experts. An e-mail virus checking and/or scanning system will be in place either on the LINUX box or as a separate appliance.

This paper will address the installation and securing of the Linux operating system and the securing of sendmail and its POP/IMAP environment. The configuring of the commercial firewall, the integration of the commercial gateway virus scanner, configuring and administration of sendmail, and configuring of the desktop environment are outside of the scope of this paper.

2. Security Review and Risk Assessment:

- a. Security Compliance: The existing security policy was reviewed and the configuration of this server will comply with their pre-established guidelines. This review disclosed the following items that are pertinent to this installation:
 - i. Passwords are to be a minimum of eight characters
 - ii. Regular passwords should expire every 90 days
 - iii. Administrative passwords should expire every 60 days
 - iv. Systems must be backed up via the enterprise backup system and its schedules.
 - v. Servers should be kept in a secured environment
 - vi. Administrators are responsible for the security of their systems including keeping them current with security and system patch levels.

It was agreed in writing that this installation would meet these basic requirements.

- b. Environment and Considerations:
 - i. This server is being implemented for a small, industrial sales business.
 - ii. There are approximately 10 employees.
 - iii. Their budget is small.

- iv. Server management will be performed on-site and **no remote access** will be required.
- v. The office LAN is not on a WAN and does not interface with the Internet except through one workstation that has a modem dial-up. The company wants to limit access to the Internet to this single workstation but would like to utilize e-mail to send and receive messages via the Internet.
- vi. The company security policy will be amended to include desktop email clients. The users will be required to have their clients be set to not keep any email on the server itself and to automatically delete them from the server after they are read. This is a precaution to avoid turning the server into an archiving system for important documents that may be transmitted via email.
- vii. This system will be backed up using their Enterprise backup system and will be put into rotation having backups performed in compliance with their backup policy. This will eliminate the need for a dependency on another backup system and having to train some to use another package of software for backups and restores. Once the system is installed, a backup will be run and a restore will be performed and verified.
- viii. The system logs are to be checked daily by an individual with minimal training as a system administrator and trimming and manipulating will be performed manually. The logging system on the LINUX box will be configured to consolidate error and warning logs into a syslog file. Automated log scanning and alerting will be put into place at a later date. This will allow the administrator to become more familiar with the system and be more capable of manually discovering problems if the automated system should ever fail.
- ix. Because of the isolation of this system and because it is currently the only UNIX-based system in their environment, multiple location logging is not necessary or practical.
- x. To monitor access and changing to critical system files due to outside influence or internal manipulation, Tripwire will be installed and configured.
- xi. Although access to the outside world is severely limited, the system is periodically exposed during the time it is dialing out to reach the ISP. A simple firewall will be installed.
- xii. The system will be kept in a locked and climate controlled area.

c. General Assessment:

At this time, the server is not considered mission critical. Their customers are familiar with alternate means of contacting them via phone and regular mail. However, they do realize that once e-mail become “institutionalized” in their business, this consideration will probably change.

This system will be a “unique” system in that it is the only Linux or Unix box running in this environment. Therefore, one of the greatest risks at this time is the inability of anyone to fully manage the system. I have agreed to work with the company to train an individual in best security and administration practices. Until the company is fully comfortable, I will have certain reports and logs mailed to me for my review and will work with them to develop a patch management strategy.

Because no data is actually going to be stored on the machine and there will only be a small number of accounts and those accounts will have limited access, a backup and recover strategy is more important at this time than protecting data integrity. The system will be incorporated into the enterprise backup strategy and regular recovery testing will be done in line with what is currently done for their other systems.

This system will be behind a fully configured firewall that they opted to purchase. As there is no one on staff with firewall expertise, they purchased an appliance with a commercial support agreement for initial setup and on-going maintenance. However, in support of a Defense-in-Depth strategy, the operating system and applications on this box will be secured in accordance with industry practices wherever possible to an extent that is practical. Because this system will act as a gateway for mail, it has been decided that the system will be enhanced with commercial virus checking and mail scanning software at either the host level or as a separate appliance.

3. Services and Software Packages required to be Installed and Secured:

The following software packages and services were identified as the minimum required to operate this system.

- a. SuSE Linux 7.3 Operating System
- b. Sendmail
- c. Tripwire

4. Initial Description of Server:

Vendor: Dell OptiPlex
Model: GX1
Processor: 450 MTbr+
Service Tag: GKXF9
RAM: 246 Megabytes
BIOS: Version A09
Number of Hard Drives: 1
Network Interface Card: 3Com 3C90X
Hard Drive Type: Maxtor 90648D4

Hard Drive Capacity: 6 Gigabytes
 CDROM: NEC:28C
 ZIP Drive: IOMEGA ZIP 100
 Floppy Drive: 3.5", 1.44 Megabyte
 Sound: TBS Montego PCI Audio AU8820 MPU 401 Midi
 Video: ATI 3D RAGE PRO AGP 2x (at-c2u2), ATI Internal PAC 8 Megabytes; ATI
 Graphics Acc, ATI Video Bios
 Operating System: WindowsNT

BIOS Settings were documented as follows:

Dell OptiPlex GX! 450 MTbr+ BIOS version A09							
Drives	Type	Cyls	Hds	Pre	LZ	Sec	Size
Drive 0:	Auto	784	255	-1	784	63	6448
Drive 1: None							
Secondary:							
Drive 0: Auto				CDROM			
Drive 1: Auto				ATAPI Device			
Reserved Memory:				None			
CPU Speed:				450 MHz			
NumLock:				On			
Chassis Intrusion:				Disabled			
DAC Snoop:				Off			
ACPI:				Off			
Pentium II Processor CPUID:				652			
Level 2 Cache:				512 Kb Integrated			
System Memory:				256 Mb SDRAM			
Video Memory:				8 Mb SGRAM			
Service Tag:				GKXF9			
Keyboard Errors:				Report			
System Password:				Not Enabled			
Password Status:				Unlocked			
Boot Sequence:				Diskette First			
Setup Password:				Not Enabled			
Auto Power On:				Disabled			
Power Management:				Disabled			
Wake up on LAN:				Off			
Integrated Devices							
Sound:				Off			
NIC:				On			
Mouse:				On			
Serial Port 1:				Auto			
Serial Port 2:				Auto			
Parallel Port:				378h			
Parallel Mode:				PS/2			

IDE Hard Disk	Auto
Diskette:	Auto
Speaker:	On

5. Pre-installation Activities

a. Gather networking information:

IP Address of Server
 Hostname
 DNS Server IP addresses (primary and secondary)
 Gateway Address
 Subnet Mask
 Modem and dial out information

b. Decide on root password and an account name and password for an initial user account.

c. After documenting the hardware and BIOS information, this information was compared against the system compatibility listing on the SuSE web site at <http://www.suse.com> and against the vendor latest download list at www.dell.com.

- The hardware met SuSE hardware compatibility requirements.
- There was a new BIOS available at Dell.
- There was a new video driver available.

The new driver and BIOS were downloaded.

d. BIOS was then updated and secured.

- Following the instructions from Dell, BIOS install floppies were prepared and installed on the system.
- Boot Sequence was changed to CDROM, Hard drive C: (excluding A: and PXE).
- BIOS Password was enabled, password assigned, and password was locked.
- The BIOS was re-documented:

Dell OptiPlex GX1 450 MTbr+ BIOS version A09							
Drives	Type	Cyls	Hds	Pre	LZ	Sec	Size
Drive 0:	Auto	784	255	-1	784	63	6448
Drive 1: None							
Secondary:							
Drive 0: Auto				CDROM			

Drive 1: Auto	ATAPI Device
Reserved Memory:	None
CPU Speed:	450 MHz
NumLock:	On
Chassis Intrusion:	Disabled
DAC Snoop:	Off
ACPI:	Off
Pentium II Processor CUID:	652
Level 2 Cache:	512 Kb Integrated
System Memory:	256 Mb SDRAM
Video Memory:	8 Mb SGRAM
Service Tag:	GKXF9
Keyboard Errors:	Report
System Password:	Enabled
Password Status:	Locked
Boot Sequence:	CDROM, Hard Drive C: (see Note below)
Setup Password:	Not Enabled
Auto Power On:	Disabled
Power Management:	Disabled
Wake up on LAN:	Off
Integrated Devices	
Sound:	Off
NIC:	On
Mouse:	On
Serial Port 1:	Auto
Serial Port 2:	Auto
Parallel Port:	378h
Parallel Mode:	PS/2
IDE Hard Disk	Auto
Diskette:	Auto
Speaker:	On

Note: Once the installation is complete and tested, the BIOS Boot Sequence will be changed to Hard Drive C: only.

- e. The latest security tools were downloaded from www.suse.de/~marc/SuSE.html and placed on a floppy. At a minimum I would recommend downloading the hardening script. SuSE 7.3 Professional comes with the same script, but it is probably a good thing to download the one on the site because it will probably be newer.
- f. If you have not purchased a commercial version of Tripwire, download the latest version of Tripwire from <http://www.tripwire.com/downloads> and place on a floppy.

6. System Design:

a. Layout Initial Partition Design:

Sitting at the Partition Screen of the Linux Install is not the time to figuring out how to set up your partition. Partition modification after the fact is never any easy task. Think about your system and what it is going to be used for and then plan ahead.

There is many philosophies on how, why, or if multiple partitions should be used. There are three at least very good reasons to do so:

Reinstallation of Operating System: If you use only one partition / (root) and place user files and system files on it, reinstallation of the operating system becomes impossible. A reinstallation would destroy your systems current configuration, your software and all of your user files.

Running Out of Space: If you only have one partition, and for some reason a huge file is unexpectedly created on it and that partition becomes full, the operating system will not be able to write to it. The system will then freeze up and will become unusable to all users. If on the other hand, you have multiple partitions and any one of them fills up, the other partitions are still available and the system can operate. This is an excellent reason to keep user data off of system partitions.

Security: The files on the /, /boot, and /usr partitions should remain fairly static and should only change when the system administrator adds, deletes, or modifies the system software. If those partitions are logically separated from the user partitions and other partitions such as /var which tend to be more dynamic, they can be placed under stricter security rules – such as making them read-only – which will prevent anyone but the root user from modifying them.

Another point of consideration is whether to make a partition primary or extended. Only four primary partitions can be created on a disk and only one Linux partition can be created on each one. Therefore, only four Linux partitions can be created if you wish to use only primary partitions. However, many Linux partitions can be created within a singled extended partitions. Although you can design a system that utilizes both primary and extended partitions, it is probably much simpler to create a single, large extended partition and place all of your Linux partitions within it.

With these concepts in mind and because this server is an e-mail server that will performing a lot of activity on the /var and could require a larger amount of temporary storage space there, this is the recommended partition configuration:

Device	Size	F	Type	Mount	Start	End
/dev/hda	6.0G		Maxtor 90640d4		0	783
/dev/hda1	6.0G		Extended			
/dev/hda5	100M	F	Linux Native (ext2)	/boot		
/dev/hda6	500M	F	Linux Native (ReiserFS)	/		
/dev/hda7	1.5G	F	Linux Native (ReiserFS)	/usr		
/dev/hda8	2G	F	Linux Native (ReiserFS)	/var		
/dev/hda9	1G	F	Linux Native (ReiserFS)	/opt		
/dev/hda10	200M	F	Linux Native (ReiserFS)	/home		
/dev/hda11	100M	F	Linux Native (ReiserFS)	/work		
/dev/hda12	512M	F	Swap	Swap		

Note also that not all the space on the hard drive is used. It is a good practice to leave a little “wiggle room” in case on expected developments and you suddenly need more space or another partition.

If you are new to partitioning and would like more information on it, Paul G. Sery and Mohammed J. Kabir cover this subject very well in Chapter 1 of their book The SuSE Linux Server.

- b. Decide on which software package you will install:

SuSE Linux 7.3 offers several different levels of installation:

- Minimum System – a fully functional Linux operating system that is geared towards a text-based mode. It is recommended for dedicated server systems that do not need a graphical desktop.
- Minimum Graphical system (without KDE) – the same as Minimum but with some graphical support (not KDE, Gnome, or X)
- Default System – a well-balanced, basic software system that includes a CD Player and editor. This is recommended if you have no Linux experience – aimed at Windows users.
- Default System with Office – a wide variety of office programs that would not be needed on a server.
- All - as it says, it will install all programs. This is very time-consuming and has large space utilization (more than 6 Gigabyte)
- Detailed Selection – this is available if you pick Minimum or Default and allows you to pick and choose extra programs.

The Minimum System selection will be chosen on this installation.

7. Basic Installation Instructions and Security Tips during Installation:

The following procedures are a combination of major step directions and installation notes that include some of the security or procedural reasons behind the selections.

We will be installing SuSE LINUX 7.3 Using YaST2:

- a. Insert the first CD of the set into the CDROM drive. Reset the PC and reboot it. If you have set your BIOS up correctly, the system will boot off the CDROM and the installation will begin.
- b. The Opening SuSE screen will appear. Installation is pre-selected and countdown will begin. Allow the countdown complete.
- c. An initial boot sequence will begin and boot messages will appear on the screen.
- d. Now the actual installation will begin. The first step is a hardware probe of the system. The Probing Hardware screen appears and checks for:
 - USB
 - Mouse
 - Floppy
 - Controllers
 - Controller Modules
 - Hard Disks
 - Partitions
- e. After the probe completes, the WELCOME to YaST2 screen appears, choose your language, and select NEXT to continue.
- f. On the Basic Configuration screen, you asked to choose your keyboard layout (which normally matches you language), your Time zone, and your Hardware clock set source as well as gives you an area to do a keyboard test if you so desire. As always, when you are ready, click NEXT.
- g. At the Install SuSE Linux screen you are presented with three installation options:
 - New Installation (which this is)
 - Update an existing system (when you want to upgrade to another newer version of SuSE in the future), and
 - Boot Installed system (this is if you have an LINUX already installed on your hard drive and for some reason in the future your system will no longer boot. With this option you can try to manually fix your system's problems)

Select New Installation and click NEXT.

- h. The next screen is suggested partitioning. You will basically be advised that the install is recommending create a root partition and a swap partition and resize the Windows partition if it exists. You are given the options of:

- Accept Suggestion
- Modify Suggestion
- Discard Suggestion

In actuality the suggested set up would be ideal if this were a workstation install. **However**, because the intention of this installation is create a single-use email server, a more complex partitioning scheme is required. Custom partitioning is required so –

Select Discard Suggestion and click NEXT.

- i. Preparing Hard Disk – Step 1 screen, select Custom partitioning. Because the partition design has already been documented in step 2, we can cut through a lot of the GUI provided by the other selections and get down to laying out the partitions.
- j. The Expert Partition Screen will appear displaying a rudimentary layout. All that should be seen at this time is an entry(s) that describe the physical hard drives. For example:

Device	Size	F	Type	Mount	Start	End
/dev/hda	6.0G		Maxtor 90640d4		0	783

Delete any other entries by highlighting them and then pressing delete.

With that in mind, we are ready to create the partitions according to the design that was prepared in Step 2. This is a reminder of that layout:

Device	Size	F	Type	Mount	Start	End
/dev/hda	6.0G		Maxtor 90640d4		0	783
/dev/hda1	6.0G		Extended			
/dev/hda5	100M	F	Linux Native (ext2)	/boot		
/dev/hda6	500M	F	Linux Native (ReiserFS)	/		
/dev/hda7	1.5G	F	Linux Native (ReiserFS)	/usr		
/dev/hda8	2G	F	Linux Native (ReiserFS)	/var		
/dev/hda9	1G	F	Linux Native (ReiserFS)	/opt		
/dev/hda10	200M	F	Linux Native (ReiserFS)	/home		
/dev/hda11	100M	F	Linux Native (ReiserFS)	/work		
/dev/hda12	512M	F	Swap	Swap		

First, create the Extended partition:

Select Create
Select Extended Partitions
Accept defaults
Select Okay

The extended partition will be created and, by default, it will be the full size of the hard drive.

After the Extended Partition is created, continue to create the other partitions in the table following the directions on the screens. There are a few points to consider when actually building the partitions:

- It is good practice to create the /boot partition first to make sure that it resides about the 1024 cylinder.
- The partitions can be built either using the Start and End Cylinders (absolute location) or by providing the size in Megabytes or Gigabytes.
- In most cases there is no right or wrong file type. Except for /boot, which is normally ext2, any file type will work.
- It is not generally necessary to reformat the partitions. However, if you are reinstalling LINUX and want to reformat them, it is only necessary to reformat the system partitions (/, /boot, and /var). Leaving the others unformatted allows the existing data and third party software to be saved and reused.
- When specifying the mount points, it simplifies administrator and makes reconstruction of a system easier if mount points for the partitions have the same name as the partition. This is the default when building these partitions.
- The swap partition is slightly different from the other partitions.
 - It should be roughly 2x the size of the physical memory of the machine.
 - Its type must be swap.
 - It has no mount point.

Once partitioning is completed, Click NEXT

- k. Once the partitioning is complete, the Software Selection screen is displayed. The selections are:

- Minimum system
- Minimum graphical system (with KDE)
- Default system
- Default system with Office
- All

Select Minimum: For security reasons (the fewer extra features available, the fewer exploits to secure against) and to simplify administration, I wanted the most bare bones system possible. Although graphical displays

and mouse support are nice features, this is server is going to be a very simple, single-use server with very little system administration required. The individuals managing this server are familiar with the System Administration Menu in HP/UX and the interfaces provided by this option are very similar.

I do not choose any additional software at this point. It is very easy to install any additional software after the system has been booted. I like to keep my installation as clean and free from complication as possible.

Click NEXT.

- l. The System Boot Configuration screen and informs you where LILO will be installed. Depending on whether you are installing to a multiple hard drive or single hard drive machine, you may get one or more screens. Click NEXT.
- m. After satisfying the LILO screens, you will receive a screen prompting you for the password of “root”, the system administrator.

Notes on Root Password:

- The root account exists on all UNIX machines and has extensive rights. All the security rules for passwords should apply here, but even more so. Root passwords should always be a combination of words, numbers, and special characters and should utilize upper and lower case.
- Do not forget the password. Take precautions so that it will be remembered. If you have a system where passwords are written down and secured in a locked drawer or vault, add this password to that list immediately. If you have a backup administrator that you trust, or if you have a security officer that is privy to root or administrator passwords, let them know immediately. If you forget this password, you will not be able to logon to your system and use administrative rights. The only recourse that I am aware of to recover forgotten root passwords is a re-install.

Supply the password, confirm it, (secure it!) and click NEXT.

- n. With the Personalize screen, the first user account will be created. Assign yourself an account by filling in the information, and click NEXT.
- o. The Confirm Installation screen will appear. This is a summary of the information you have entered in until now.
 - Please review. If there is something this needs adjusting, you can use the BACK buttons to arrive at the screen and make the change. This is your last chance!
 - You can also save settings to a floppy if you wish.

- Click NEXT when are satisfied.
- YaST2 will then proceed with a confirmation check. By answering Yes-Install, the installation will begin in earnest.

p. Several screens will appear during the install most of which require no intervention.

- Preparing Hardware
- Congratulations and Installation Time bar
- Finishing Basic Installation
- And so on

Eventually a Message Screen appears and announces the LILO Boot Sector has been written to disk and tells you how to restore the old boot sector using the `lilo -u /dev/hda` command. Click OK.

- q. If all has gone well, the system will not go into a boot sequence.
- r. YaST2 begins to initialize. Because Minimal Install was chosen, a warning appears stating that your computer does not fulfill all the requirements to allow a graphical install. After responding to the warning, the Text User Interface (TUI) takes over.
- s. The installation log continues and system configuration is written.
- t. A Congratulations screen appears and prompts you to login. It also gives you a chance to configure additional hardware, but also informs you that you can do this in YaST2 at any time after you login. At this point, I configured the network and modem with the information I collected in Step 2. This is optional and can be done later. Tab to Finish Install.
- u. Installation is complete. You are ready to login and begin to secure the system.

8. Securing the Server/Network Configuration

- a. Login with user account and su to root

```
[~user]$ su - root
password: XXXXXX
[/root]#
```

From here on out you should be at the `[/root]` prompt unless otherwise noted.

- b. Check what processes are running and document:

ps -x

- c. Check what ports are open and document:

ls -i

- d. Change to the /etc/init.d directory and document what services are listed /etc/init.d

ls

Because we have utilized the minimal install, there should be nothing in here to cause us concern. However, we should document what was there for future reference. If there are services which you know will not be need, you can use the rm command to remove them or you can us vi to edit all those offending services and add 'disable=yes' inside the brackets. Another nice trick is to take the offending service and rename it to being with a _.

mv process _process

- e. Because the hardening script is likely to change over time, I decided to install hardening script previously downloaded from www.suse.de/~marc/SuSE.html a floppy disk.

```
cd /usr/sbin
mkdir /harden_suse-3.5
cd /harden_suse-3.5
mount /dev/fd0 /media/floppy
cp /media/floppy./harden_suse-3.5.tar.gz /usr/sbin/harden_suse-3.5
gunzip harden_suse-3.5.tar.gz
tar xvf harden_suse-3.5.tar
```

Before we run this script, a note of explanation is in order. Harden_Suse by Marc Huese is an excellent script that does a very nice job of tightening up a SuSE installation. It makes several changes to the system configuration and makes the system more resistant to local and remote attacks. You can make up to ten different types of security changes as are described with the scripts on-line documentation:

- i. Deactivation of all network services except for SSH, Firewall, and VPN.
- ii. Changing Filer permissions to a secure state
- iii. Commenting out all service in the /etc/inted.conf and secure the tcpwrapper to allow only localhost access.
- iv. Securing the login process by logging all login attempts, show last/failed logins, and allow root login only from console.

- v. Securing passwords enforcing long passwords, requiring password change after 40 days, and warning against weak passwords.
- vi. Strengthening permissions on /home directories of users and placing a strict umask (077) for all users.
- vii. Securing configuration of SSH/SSHD by disabling/enabling options for better security.
- viii. Removing privileges of all unknown suid files
- ix. Remove world write permissions on all unknown world writeable files on the system
- x. Showing legal disclaimer in the login banner, motd and lilo boot menu.

If you wish to know exactly how all of this is done, a print out of the .pl file is included as an appendix. When time allows, it would be a good idea to look through this file to get a handle on how all of this was done in case you have to remove or change things manually. Huese does include an undo-script in case things go totally awry and you want to start over.

The documentation states that this script can be run with the command line option “yes” and an automatic yes to all questions is assumed. You can also “auto-answer” by putting ten command line parameters of “y” or “n” depending on your configuration. You can also run the script with no parameters and it will run interactively. In our case we will run Huese’s script in interactively using the options as he recommends for servers – yes to all questions except for 6 (strengthening permissions on home directories) and 8 (removing privilege of all unknown suid files on the system).

sh harden_suse-3.5

or if you do want to watch the questions being asked

sh harden_suse-3.5 yyyyyynynyy

- f. To recheck services what services are running with your ps -x command and compare them with your documentation step 2 above. If extraneous services are still running, you may stop them by following the instructions in step 4.
- g. To recheck what ports are open, run lsof -i again and compare and document. In our case, we noticed that ssh was still listening. We are not going to do remote dialin to this server and we did not configure ssh. This is not a task we are going to tackle right now, so we want to make sure that service no longer runs until we are ready.

cd /etc/init.d
mv ssh

- h. You may want to check what was done to the user security environment and make some tweaks. We can do this using the YaST2 configuration and system management tool. It is a good idea to get to know this tool as it will help both experienced and inexperienced system administrators by a “wizard-like” approach to editing configuration files and doing many administrator tasks. There are two “YaST” tools with this edition of SuSE Linux. There are some things that each does better than the other so get to know them both. We are going to use YaST2 to explore some of the security settings. Mark each of the three password options by highlighting and pressing space bar on each one.

Working with YaST and YaST2 without graphical or mouse support can be kind of tricky at first, but it is fairly simple once you get used to it. It works much the same way as SAM does at the console on many UNIX boxes. You use tab to move around the screens and when you want to select something you must highlight it with tab and press the space bar to select it. You enter modules by highlighting the Launch Module section at the bottom of the screen and pressing enter. You move back and forth between screens by highlighting the next and back buttons and you finish a session by highlighting and selecting the Finish button.

YaST2 #yast will also be acceptable
Highlight Security&Users/ Security Settings
Tab to Launch Modules
Select Level 3 – Network/Server
 Password Screen
 Under Checks all three options should be X'd

 Checks for New Passwords
 Plausibility Check for Passwords
 Activate MD5 Encryption for Passwords

 Set Minimum password length to eight (8) to
 conform to client's Security Policy.

 Leave Days of Password Change and Days Before
 Password Expire as is.

Boot Settings

How to Interpret CTL-ALT-DEL – ignore
Shutdown Behavior of KDM – only root

Logon Settings

Leave Seconds after Incorrect Login at three (3) and make sure both successful and unsuccessful logon attempts are logged.

Miscellaneous Settings

Leave these with their defaults.

- i. Even though we are not planning to run FTP or TELNET on these boxes it is always a good idea to make sure from the outset that these security measures are accounted for. You may in the future decide to add these services and assume that these measure have been taken care of – when in fact they have not. It is always a good thing to do security when it is foremost in your mind.

- i. Verify that remote logins are disabled for FTP

The file that you will look at contains account names that are NOT allowed to login with FTP. There may be many names in this file, but that is fine. Verify that the root is included in this list.

more /etc/ftpusers

Any new accounts you make are not automatically added here. There are scripts and commands that can be run to do so. However, if you are new to Linux, it may be easier to simply add a step in the account creation section of your system documentation stating that the names of all new user accounts created on this system need to be manually added to this file.

- ii. Verify that remote root logins are disabled for TELNET

vi /etc/secretty

This file contains a list of all TTY interfaces that allow root logins. It should only contain virtual (vc's) and consoles (tty's).

- j. After identifying where root can log in from remotely, it is a good idea to identify what system accounts can login at the console. The /etc/security/access.conf contains the login parameters for all accounts on the system. You may wish to only allow root to login at the console. To accomplish this you need to edit the /etc/security/access.conf file to include the entry which denies all logins at the console except for User and Group root and admin.

-:ALL EXCEPT root admin :console

Be care with this command because you want to make sure that SOMEONE will be able to login at the local console.

k. Download latest patches:

Note: Before you actually do this, I would recommend that **you skip down to Step 10: Installing and Configuring** Tripwire and complete steps a and b. Before I ever go live on a network with a server, I do a rudimentary install of Tripwire and make sure I have a footprint of the system in its original installed condition. An unprotected and unpatched system can actually be hacked and compromised in the time it takes to download and install the patches.

Yast2 makes this very easy. From the command line, type:

```
yast2
```

Select Software On-line update and Launch Module

A screen will appear to the right which has three sections that give you information and choices on last update, update modes, installation source.

Tab to Update Mode section, arrow to Manual and press space bar to select.

Tab to Installation Mode and make sure ftp.suse.com is shown.

Tab to Finish and allow the system to go on. Informational screens will appear to let you know what the status of the transfer is and so on. Eventually, the word disconnected will appear at the bottom of the dialog screen. This is the queue to tab to Next to finish the process.

Because you have selected the manual process, you go to a screen entitled: List of Available Patches. Individual patches can be deselected/selected using the space bar. Until you become very familiar with your system, it is a good idea to follow SuSE's lead and take their selections. I would still recommend that you still review the patches before going ahead. It is a good idea to know what you are patching in case problems occur or if you have specialized software on your box with special dependencies. Please note that yast2 patches will always be installed on a "first run". Other patches will be downloaded by will not be must be installed on a "second run".

Status Flags (first column):

G: Not relevant not relevant to this installation of SuSE.

No Flag (blank): Not selected.

X: Relevant for this installation of SuSE. Will downloaded and installed.

Mode Flags (second column):

Optional
Recommended
Security

The first two types are self-explanatory. It is highly recommended that any relevant patch marked Security be installed.

Arrowing to an individual patch and then tabbing to Show Description at the bottom of the screen can obtain more information.

Once you are satisfied with your selections, tab to Next. The installation process will begin and the transfer and connection screen will report and activities and errors.

1. Enhance your logging.

Make sure that the following entries are in your /etc/syslog.conf and that they are not commented (#) out:

```
.warn*;*err    /var/log/syslog
kern.*         /var/log/kernel
```

Configure real-time logging to VTY's. Setting up the Alt-F7 and Alt-F8 screens to display real-time logging can be very useful. To do this, you will need to append the following to the /etc/syslog.conf:

```
*.info;mail.none;authpriv.none    /dev/tty7
authpriv.*                        /dev/tty7
.warn*;*err                       /dev/tty7
kern.*                            /dev/tty7
mail.*                            /dev/tty8
```

Separators between columns must be TABS, not SPACES.

Once this /etc/syslog.conf has been edited and saved, you may need to create new log files. From the command prompt, type:

```
touch /var/log/syslog /var/log/kernel
```

Then change their permissions as follows:

```
chmod 700 /var/log/syslog /var/log/kernel
```

Restart your syslogd daemon and watch for any errors in case you have made any typos.

killall -HUP syslogd

- m. Install TCPWrappers: Using yast2 makes this a snap. At the command line type

yast2

Choose Software / Install/Remove software and tab to Launch Module.

Tab to Search (at the bottom)

Type tcp in the search screen

Tab to Search at the bottom of the dialog box, wait for results to return

At result screen, tab to packages area, arrow to tcpd and press space bar to select

Tab to Ok

The tcpd daemon will install in /usr/sbin

Check the contents of the /etc/hosts.allow and /etc/hosts.deny files:

By default, there should be no uncommented lines in /etc/hosts.allow (nothing should be allowed)

By default, there should be only the following uncommented line in /etc/hosts.deny

ALL:ALL EXCEPT localhost

- n. Ensure that inetd is running on your system:

ps -ef | grep inetd

If it is not running, make sure it is still installed:

find / -name inetd

If found, go to Step 9.

If it is not found, install it through yast2 – much the same way you did tcpd in step 8.m Install TCP Wrappers above:

Choose Software / Install/Remove software and tab to Launch Module.

Tab to Search (at the bottom)

Type inetd in the search screen

Tab to Search at the bottom of the dialog box, wait for results to return

At result screen, tab to packages area, arrow to inetd and press space bar to select, Tab to Ok

If you had to re-install inetd, I would reboot.

shutdown -r y0

Once, the system is backup, re-login as root as re-check for the process:

ps -ef | grep inetd

9. Configuring and Securing sendmail:

Configuring sendmail is very complex and the actual administration of it can be very complicated. It is recommended that anyone who really wants to understand the rich environment of sendmail should obtain a copy of “sendmail”, Costales and Allman, O’Reilly & Associates and become very familiar with the www.sendmail.org and www.sendmail.net web sites

Much of the is taken from Security Linux, Step By Step, v1.0 by the SANS Institute, step 4.4. I have verified that the names and entries as they apply to the SuSE Linux 7.3 installation and have incorporated the use of yast2 where appropriate.

- a. First we will enable smtp and make it so that it starts up every time at reboot. There are manual steps to do this. However, for beginners and old hands alike, I find that the yast2 tool is a very nice way to hand this.

At command prompt, start yast2 and follow the menus: (Remember tab to item, press space bar to select, and then tab to option)

```
yast2
Network/Basic /Start /stop services (inetd)
Launch Module
(x) on with custom with custom config and tab to next
Smtp (use tabs and then enter then space bar to select)
Tab to bottom menu, and tab to activate/inactivate toggle
“Active!” will appear by smtp entry and then tab to Finish and
enter
```

inetd will be automatically stopped and restarted.

You can manually reload the inted configuration with the following command:

/etc/init.d/inetd reload

- b. Turn Off SMTP vrfy and expn commands in /etc/sendmail. The vrfy SMTP command allows a remote user to verify e-mail addresses for local users on your server and the expn command expands aliases and mailing :include aliases. This information should be considered to be at least sensitive and not for public consumption.

Find the entry for PrivacyOptions in the /etc/sendmail.cf file. Change it to read:

O PrivacyOptions=goaway

This is shorthand for a variety of switches including: authwarnings,neoxpn,novrfy,needmailhello,needexphelo and so on. Full descriptions can be found in the “sendmail” book referenced above.

- c. Define hosts to relay mail

Check to make sure that the access database is active. At the command prompt, type:

grep Kaccess /etc/sendmail.conf

With our version of SuSE and its default sendmail install, this string will appear:

Kaccess hash -o /etc/mail/access

Set access for domains to allowed to relay:

The access database has a simple “key value” format: the key is a fully qualified hostname, subdomain, domain or network: the value is an action: REJECT, DISCARD, OK, RELAY, or some arbitrary message. Edit the /etc/mail/access file to contain entries appropriate for those hosts you wish to relay mail through your server and no other.

Example.com RELAY

- d. Set domain name masquerading You want to rewrite all headers of outgoing mail to masquerade as the central mail server.

Edit /etc/mail/send.conf . Find the DM entry and edit it to read

Dmexample.com

- e. Install POP and IMAP daemons:

It is very important that you have downloaded and configure the most current POP/IMAP daemons. There are many to choose from. The following URLs will take you to two popular sites:

Eudora Qpopper: http://www.eudora.com/qpopper_general/
CyrusIMAPD: <http://asg.web.cmu.edu/cyrus/imapd>

SuSE 7.3 seems to be very current, so I checked first with the website and got the latest version number. I then went into yast2, Software / Install/Remove software and searched for qpopper. I found that I had the latest release, so I was able to install it from there using the yast2 menu.

It installed its executable as /usr/sbin/popper

I then went into yast2 and followed the same steps in 12.a.1, but activated the pop3 entry. Make sure that the entry in the inetd.conf looks like this and is uncommented out (no # preceding it)

```
pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/popper -s
```

(the -s parameter allows for statistical logging)

f. Secure Pop and IMAP daemons:

Control Access to POP and IMAP with TCP Wrappers. Limit hosts to only those that have a legitimate need for the service.

Edit /etc/hosts.allow to include these entries:

```
popper: .example.org
```

Make sure that /etc/hosts.deny has only

```
ALL:ALL
```

g. Additional Security:

If you are planning to run SSL, you can install an SSL wrapper for secure POP/IMAP connections. Two applications that are useful in this regard are stunnel and sslwrap. For a list of third party applications, you may go to <http://www.openssl.org/related/apps.html>.

10. Install and Configure Tripwire:

Tripwire is a very powerful and complex tool that computes a MD5 checksum of files that you wish to observe for evidence of tampering. Although once you become familiar with Tripwire you can observe any file or files on your system that you deem critical, normally these would include files in /etc, system programs in /bin and /usr/bin, applications and user accounts. It is not the intention of this paper to teach you how to use Tripwire. The purpose of installing and configuring Tripwire at this point is to get a “virgin” footprint of your system into Tripwire’s database and suggestions on how to secure that footprint before you actually put the system onto the network. Unfortunately, there is no simple way of doing this without getting into some detail

Although there is a version of Tripwire that comes free with the SuSE Linux 7.3, I chose to use a commercial version. I have found the documentation and support that comes with the commercial version to be invaluable. I have documented my installation, but depending on the download or install you plan to use, installation scripts will vary. In any case, I would make sure that if I was installing a free version, I would download the latest and greatest from <http://www.tripwire.com/downloads>. Good documentation for installing and configuring Tripwire does exist and it can be found in Real World Security by Bob Toxen.

- a. Either from a CD or from the directory to which you have installed your download directory, issue this command:

./install.sh

(With commercial version you will be presented with a license agreement and you are instructed to read it carefully and then accept the terms of agreement by typing the word accept and pressing enter).

Type yes to continue installation if the installer detects fields in the installation directory.

Specify a site pass phrase. This pass phrase protects the site key that cryptographically signs site-specific data files. Use common sense and choose a good phrase following the same rules you would for your root password.

Specify a local pass phrase. It is recommended that it be a different pass phrase than the one you used for the site pass phrase. This pass phrase would of course protect the local key that in turn signs the machine-specific data files.

After waiting for the installer to generate these keys (it could be several minutes), the configuration file, and a default policy file.

The script may also ask for a port number for communication with Tripwire (the suggestion is to use 1169) and e-mail information such as full domain name. After supplying all the information, the script will let you know it is complete.

Locate the file structure in which Tripwire has been placed. At the command prompt, type:

locate tripwire

Change into the tripwire directory

cd (the directory discovered with your find command)

If when you tightened security you told the machine not to include the root's current path in the PATH variable, which is done when you the harden_suse script mentioned above, changing into a directory will not automatically allow you to run the executable without specifying its path, so the commands will look slightly different.

It is recommended that you change permission for the Tripwire Directories and files to Full Control for authorized administrators only. Use the chmod command to change all files and directories as follows:

chmod 700 chown root:admin

As part of the commercial installation, a default policy file for your operating system is also installed. The default policy file only monitors basic components that are common to all versions of each operating system. It is strongly recommended that you create a customized policy file for your machine. However, as long as the default file you are using is the one meant for your installation (LINUX vs HP/UX), it should be good enough for our purposes at this time. If your installation did not create a twpol.txt for you, issue this command :

(Note: where two dashes appear, the actual command has no space between them)

./twadmin -- create-polfile ../policy/twpol.txt

b. Initialize the database

./tripwire - -init

This command saves the database file to the Tripwire db directory of the location specified by the DBFILE parameter in the configuration file. At this point you have created your “virginal” footprint. I would suggest at this point you copy the

*.twd file that was created by the command above to a floppy and store it in a safe place. If you are interested in tuning the policy file (especially if you had a lot of errors in your output), read on:

- c. Run your first integrity check. If you want to see exactly what is happening with your integrity check, type in the command

./tripwire - -check - -interactive

After the integrity check is finished a report opens in your text editor.

Look for things like files being looked for in the wrong directories and so on. Mark down the changes you think need to be made. Then create a plain text version of your policy file by issuing this command:

- d. Tune your policy file:

./twadmin -- print-polfile > pol_tune.txt

Open pol_tune.txt in your favorite editor and correct the entries that are in error and then save your changes. After you are finished, update the policy file with the edited text file.

./tripwire - -update-policy - - secure-mode low pol_tune.txt

Then run the report again interactively:

./tripwire - - check - -interactive

Repeat these steps until you are satisfied with your output. After you have tuned the file to your satisfaction and are ready to run regular (non-interactive integrity checks), you are ready to move on.

- e. Run Tripwire often and get to know it well. It is highly recommended that a cron job be created to run Tripwire every day and mail a report to the administrator.

An entry like this should do the trick:

```
00 24 * * * /usr/local/tripwire/tfs/bin/tripwire --check | mailx
TRIPWIRE root
```

This is very simplistic and as you become more and more familiar with Tripwire and learn exactly what you want to check and how you want it reported, I am sure you will come up with much more sophisticated cron entries. This at least will give you a starting point.

If through the steps above you have created any extraneous clear text files (.txt), it is recommended that you delete them now.

If you do not plan to use Tripwire Manager and use the command line interface only, it is suggested that you do not install twagent at all. However, if you have by default during the installation, it is suggested that you remove the twagent executable as well. This executable makes it possible for a Tripwire Manager to register and take control of your Tripwire for Servers installation. Also go to the /etc/init.d/ directory and rename twagent to _twagent.

```
cd /etc/init.d  
mv twagent _twagent
```

11. Post Installation Testing:

a. Enhanced Logging (Section 8.1):

Real-time logging:

Toggle Alt-F7 keys to toggle to that screen. System logging should be displayed.

Toggle Alt-F8 keys to toggle to the next screen. Mail logging should be displayed.

Error reporting enhancement:

To verify kernel errors are being reported to the syslog:

```
cat syslog | grep kernel
```

To verify kernel errors are going to kernel log:

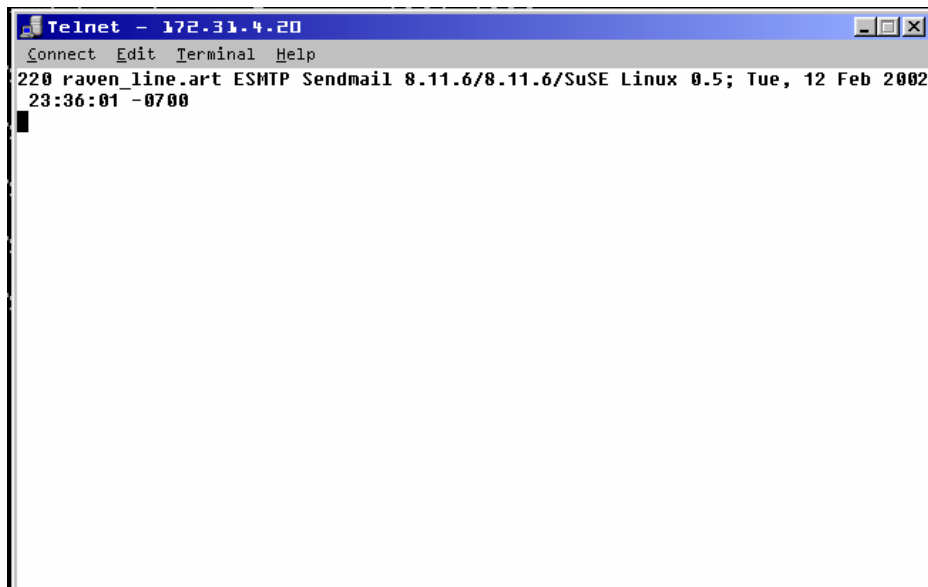
```
cat kernel | grep kernel
```

b. Verify only services running are smtp and pop3:

```
raven_line:/etc # netstat -a --inet  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 *:pop3                  *:                        LISTEN  
tcp        0      0 *:smtp                   *:                        LISTEN
```

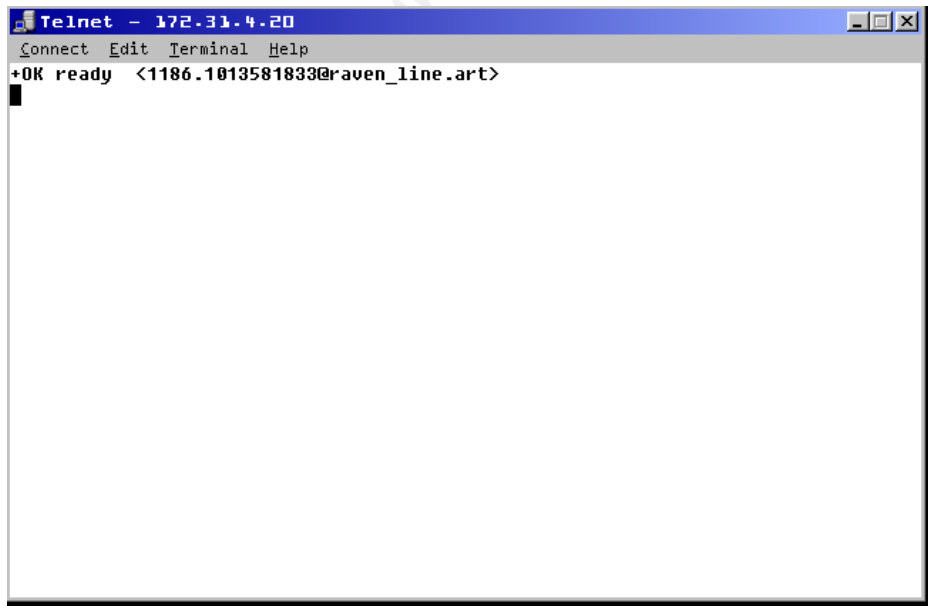
```
raven_line:/etc # lsof -i +M  
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME  
inetd    358  root   4u  IPv4  1223      TCP *:smtp (LISTEN)  
inetd    358  root   5u  IPv4  1224      TCP *:pop3 (LISTEN)
```

- c. Verify sendmail/pop3 ports are active and connectable.
1. From Workstation on network:
telnet 172.31.4.20



A screenshot of a Telnet window titled "Telnet - 172.31.4.20". The window has a menu bar with "Connect", "Edit", "Terminal", and "Help". The main text area shows the following output: "220 raven_line.art ESMTP Sendmail 8.11.6/8.11.6/SuSE Linux 0.5; Tue, 12 Feb 2002 23:36:01 -0700". A cursor is visible on the line following the output.

2. From Workstation on network:
telnet 172.31.3.20:110



A screenshot of a Telnet window titled "Telnet - 172.31.4.20". The window has a menu bar with "Connect", "Edit", "Terminal", and "Help". The main text area shows the following output: "+OK ready <1186.1013581833@raven_line.art>". A cursor is visible on the line following the output.

3. Checked port status on host while connections were active:

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
inetd	359	root	4u	IPv4	1258		TCP	*:smtp (LISTEN)
inetd	359	root	5u	IPv4	1259		TCP	*:pop3 (LISTEN)

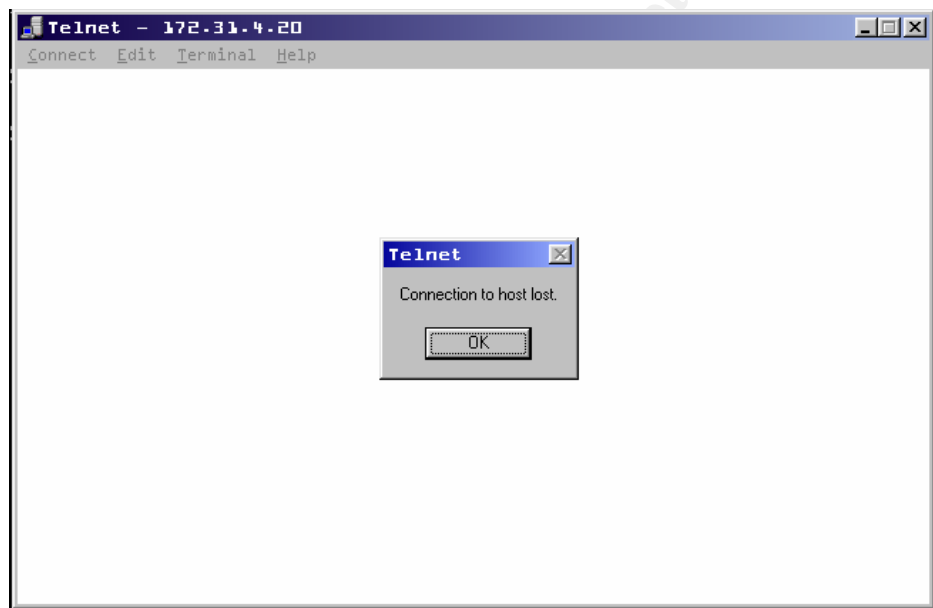
```

popper 408 root 0u IPv4 7254      TCP raven_line.art:pop3-
>172.31.4.4:essweb-gw (ESTABLISHED)
popper 408 root 1u IPv4 7254      TCP raven_line.art:pop3-
>172.31.4.4:essweb-gw (ESTABLISHED)
popper 408 root 2u IPv4 7254      TCP raven_line.art:pop3-
>172.31.4.4:essweb-gw (ESTABLISHED)
sendmail 409 root 0u IPv4 7263     TCP raven_line.art:smtp-
>172.31.4.4:kmscontrol (ESTABLISHED)
sendmail 409 root 1u IPv4 7263     TCP raven_line.art:smtp-
>172.31.4.4:kmscontrol (ESTABLISHED)
sendmail 409 root 2u IPv4 7263     TCP raven_line.art:smtp-
>172.31.4.4:kmscontrol (ESTABLISHED)

```

- d. Verify that workstations cannot not ftp or telnet in:

When a telnet and an ftp session were initiated from a workstation to the host, they received this type of screen.



- e. Verify root has restricted remote login access. The following are the steps to test telnet. When completed testing telnet, follow the same steps for ftp:

1. First you must allow temporary access in. Edit your host.allow to look like this:

```

# See tcpd(8) and hosts_access(5) for a description.

#ALL EXCEPT in.fingerd, in.identd : ALL : spawn
(safe_finger -l @%h 2>&1| \
# /bin/mail -s "%d-%h %u" root) &
in.telnetd:ALL

```

Leave your hosts.deny looking like this:

```

#
# This config file was changed by the harden_suse script to enforce a
# strict security on your system.
# This configuration was changed on the Sat Dec 22 18:37:12 MST 2001.

```

```
# harden_suse v3.5 (12-June-2001) by Marc Heuse <marc@suse.de>
#
# Think twice before changing an option.
#
#
ALL: ALL EXCEPT localhost
```

2. Uncomment your telnet lines in inetd.conf

```
# If you want telnetd not to keep-alives (e.g. if it runs over a
ISDN
# uplink), add -n. See 'man telnetd' for more details.
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
# nntp stream tcp nowait news /usr/sbin/tcpd /usr/sbin/leafnode
smtp stream tcp nowait root /usr/sbin/sendmail sendmail -bs
```

3. Then, try to telnet into the host from a workstation with the root account. If things are configured correctly, you will get a screen like this:

Warning: Unauthorized access to this system is forbidden and will be prosecuted by law! By accessing this system, you agree that your actions can be monitored if unauthorized usage is suspected.

```
raven_line login: root
Password:
Login incorrect
```

```
raven_line login: root
Password:
Login incorrect
```

```
raven_line login:
```

4. To make sure it is just not telnet itself that is not working, try logging in with a regular account. You should be allowed to telnet in:

Warning: Unauthorized access to this system is forbidden and will be prosecuted by law! By accessing this system, you agree that your actions can be monitored if unauthorized usage is suspected.

```
raven_line login: jjoki
Password:
Last login: Tue Feb 12 01:16:02 from 172.31.4.4
```

Warning: Unauthorized access to this system is forbidden and will be prosecuted by law! By accessing this system, you agree that your actions can be monitored if unauthorized usage is suspected.

```
jjoki@raven\_line:~>
```


5. Remember to remove you in.telnetd entry from your hosts.allow file when you have finished tesing.
- f. Make sure only process you need are running: This is was my ps -aux when I completed my set up:

ps -aux

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.7	0.0	452	212	?	S	23:35	0:04	init [3]
root	2	0.0	0.0	0	0	?	SW	23:35	0:00	[keventd]
root	3	0.0	0.0	0	0	?	SW	23:35	0:00	[kapm-idled]
root	4	0.0	0.0	0	0	?	SWN	23:35	0:00	[ksoftirqd_CPU0]
root	5	0.0	0.0	0	0	?	SW	23:35	0:00	[kswapd]
root	6	0.0	0.0	0	0	?	SW	23:35	0:00	[bdflush]
root	7	0.0	0.0	0	0	?	SW	23:35	0:00	[kupdated]
root	8	0.0	0.0	0	0	?	SW<	23:35	0:00	[mdrecoveryd]
root	11	0.0	0.0	0	0	?	SW	23:35	0:00	[kreiserfsd]
root	215	0.0	0.2	1396	640	?	S	23:35	0:00	/sbin/syslogd
root	218	0.0	0.4	1896	1104	?	S	23:35	0:00	/sbin/klogd -c 1
root	304	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	307	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	310	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	318	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	319	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	321	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	324	0.0	0.2	11784	760	?	S	23:35	0:00	/usr/sbin/nscd
root	344	0.0	0.2	1464	656	?	S	23:35	0:00	/usr/sbin/cron
root	359	0.0	0.2	1344	552	?	S	23:35	0:00	/usr/sbin/inetd
root	374	0.0	0.4	2080	1196	tty1	S	23:35	0:00	login -- root
root	375	0.0	0.1	1296	480	tty2	S	23:35	0:00	/sbin/mingetty tty2
root	376	0.0	0.1	1296	480	tty3	S	23:35	0:00	/sbin/mingetty tty3
root	377	0.0	0.1	1296	480	tty4	S	23:35	0:00	/sbin/mingetty tty4
root	385	0.0	0.1	1296	480	tty5	S	23:35	0:00	/sbin/mingetty tty5
root	386	0.0	0.1	1296	480	tty6	S	23:35	0:00	/sbin/mingetty tty6
root	390	0.0	0.5	2704	1508	tty1	S	23:35	0:00	-bash
root	436	0.1	0.5	4016	1428	?	S	23:44	0:00	sendmail: server
[172.31.4.4] cmd read										
root	438	0.0	0.0	0	0	?	Z	23:45	0:00	[cron <defunct>]
root	458	0.0	0.5	2480	1504	tty1	R	23:45	0:00	ps -aux

- g. After initial configuration and setup, the basic security of the system was tested and documented as follows using security analysis and port scanning utilities as follows:

1. SAINT: Text output of the report is contained in the Appendices that follow.

Vulnerability information: (Brown: 1)

[BROWN] pop receives password in clear
Ignore

This issue is addressed in the Ongoing Maintenance and Management Concerns section below.

2. NMAP: The output can be captured very nicely by entering the script command at command line, running your command, then

use CTRL D, when you the output is complete. This is a nice documentation tool and it can be used to capture the output of a series of commands in a single file:

script out_put_file.txt

It records the command entered and output received.

```
Script started on Thu Feb 14 11:55:30 2002
raven_line:~ # nmap -sT -sU -sR -v 127.0.0.1

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host localhost (127.0.0.1) appears to be up ... good.
Initiating Connect() Scan against localhost (127.0.0.1)
Adding TCP port 110 (state open).
Adding TCP port 25 (state open).
The Connect() Scan took 0 seconds to scan 1563 ports.
Initiating UDP Scan against localhost (127.0.0.1)
The UDP Scan took 2 seconds to scan 1563 ports.
Initiating RPCGrind Scan against localhost (127.0.0.1)
The RPCGrind Scan took 0 seconds to scan 1563 ports.
Interesting ports on localhost (127.0.0.1):
(The 3124 ports scanned but not shown below are in state: closed)
Port      State      Service (RPC)
25/tcp    open       smtp
110/tcp   open       pop-3

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
raven_line:~ #
Script done on Thu Feb 14 11:55:58 2002
```

The command ran was:

Nmap -sT -sU -sR -v 127.0.0.1

The output is exactly what we want in order to use this machine as a sendmail server with no remote access enabled.

12. On-going Maintenance and Management Considerations:

- a. The vulnerability discovered by the SAINT report is not considered critical at this time, but will be will be addressed. Relegation to non-critical status of this vulnerability is based on the defense-in-depth security strategy at this site which includes a firewall and because the activity on this box is not considered mission critical. However, an upgrade to Secure Pop3 Mail Server (with APOP/IIMAP4) is planned in the near future.
- b. Train personnel on and institute best practices. A very good site for Unix and Linux System Administration Best Practices can be found at The Arizon State University, Unix Network Users Group Web Site at <http://www.asu.edu/ag/unug/bestpractices> and have included some of their information here.

- c. Set up a basic system administration routine, identifying daily, weekly, and monthly tasks to monitor logs and systems for suspicious activity.

System Log and console messages: This is the primary system log and most daemons log to it. On a SuSE system it can be reviewed in its entirety with the following command:

more /etc/var/log/syslog

Or, you can look at its last 100 (or any number you choose) with

tail -100 /etc/var/syslog

Sendmail log: Sendmail keeps track of its traffic in the system log referenced above. Watch for spamming activity and suspicious mail. If it appears you are being used as a relay, make sure your relay information is set to your office domain.

Some commands to use frequently would be:

last
lsof -i
netstat -a
ps -aux

- c. Tripwire should be further configured and refined and a fuller set of reports should be generated. A scheduled update of the database should become part of the systems administration routine.
- d. After a baseline familiarity is established with the system, it is recommended that utilities be installed to automate commands and have their output emailed to the system administrator. Other utilities such as log parsers and security auditors will also be installed and added to the system administration routine.
- e. A port scanner such as nmap and a vulnerability scanner such as SAINT will be installed and ran periodically.

13. Final Steps

- a. BIOS was configured to boot from Hard Drive Only.
- b. Create the SuSE Rescue System: The greatest advantage of this system is that a system can be recovered even if a CDROM cannot be accessed.
 1. Prepare: You will need two error-free formatted diskettes. One will become a bootable disk and other will become a compressed image of a small root file system.
 2. Create your disks: There are actually three ways to set up this system, but we will use yast2. Insert an error free diskette, and from the command line, type yast2

- c. Create the Boot Disk:

From the yast2 console, select System/ Create boot, rescue or floppy module and launch module.

Boot Disks, standard floppy is already selected so Tab to Next.

You will be notified that the floppy is being created. When it is completed, you will be notified that the Boot Floppy was successfully created, press enter to accept OK.

- d. Create the Rescue Disk:

From the yast2 console, select System/ Create boot, rescue or floppy module and launch module.

Tab to Rescue Disk and select with enter and Tab to Next.

You will be notified that the floppy is being created. When it is completed, you will be notified that the Rescue Floppy was successfully created, press enter to accept OK.

- e. Test the Rescue System:

This is a quick outline of some test procedures. It is not intended to show you how to actually “Rescue” your system. The SuSE Linux 7.3 Reference Manual has very good instructions for testing and working with the Rescue System. Most of what follows is taken from Section 13.6.2 of that manual.

Make sure that, if necessary you have changed your boot series in CMOS to include the floppy drive in your boot sequence.

- Start your system with the boot disk in the floppy.
- Launch your entire system
- Make the respective settings for language, keyboard, and screen.
- Select the item Installation/Start System in the main menu.
- Remove, the Boot Disk and insert the Rescue Disk
- In the menu, Start installation/system, select 'start rescue system and then specify the desired source medium - in this case 'Floppy Disk'
- The Rescue System will be decompressed, loaded onto a RAM floppy disk as a new root file system, mounted and started.
- The system is ready for use. From here you can do many things including accessing your normal system, repairing file systems and so on.

© SANS Institute 2000 - 2002, Author retains full rights.

Appendices

Appendix A – Sample Configuration Files

Appendix B – SAINT Report

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix A: Sample Secure Configuration Files for the Environment

etc/inetd.conf

```
#
# This config file was changed by the harden_suse script to enforce a
# strict security on your system.
# This configuration was changed on the Sat Dec 22 18:37:12 MST 2001.
# harden_suse v3.5 (12-June-2001) by Marc Heuse <marc@suse.de>
#
# Think twice before changing an option.
#
#
# This config file was changed by the harden_suse script to enforce a
# strict security on your system.
# This configuration was changed on the Thu Dec 20 17:09:44 MST 2001.
# harden_suse v3.5 (12-June-2001) by Marc Heuse <marc@suse.de>
#
# Think twice before changing an option.
#
# See man 8 inetd for more information.
#
# If you make changes to this file, either reboot your machine or send the
# inetd a HUP signal with /etc/init.d/inetd reload or by hand:
# Do a ps x as root and look up the pid of inetd. Then do a
# The inetd will re-read this file whenever it gets that signal.
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# echo stream tcp nowait root internal
# echo dgram udp wait root internal
# discard stream tcp nowait root internal
# discard dgram udp wait root internal
# daytime stream tcp nowait root internal
# daytime dgram udp wait root internal
# chargen stream tcp nowait root internal
# chargen dgram udp wait root internal
# time stream tcp nowait root internal
# time dgram udp wait root internal
#
# These are standard services.
#
# ftp stream tcp nowait root /usr/sbin/tcpd wu.ftp -a
# ftp stream tcp nowait root /usr/sbin/tcpd proftpd
# ftp stream tcp nowait root /usr/sbin/tcpd in.ftp
#
# If you want telnetd not to keep-alives (e.g. if it runs over a ISDN
# uplink), add -n. See 'man telnetd' for more details.
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
# nntp stream tcp nowait news /usr/sbin/tcpd /usr/sbin/leafnode
smtp stream tcp nowait root /usr/sbin/sendmail sendmail -bs
# printer stream tcp nowait root /usr/sbin/tcpd /usr/bin/lpd -i
#
# Shell, login, exec and talk are BSD protocols.
# The option -h permits .rhosts' files for the superuser. Please look at
# man-page of rlogind and rshd to see more configuration possibilities about
# .rhosts files.
# shell stream tcp nowait root /usr/sbin/tcpd in.rshd -L
# shell stream tcp nowait root /usr/sbin/tcpd in.rshd -aL
#
# If you want rlogind not to keep-alives (e.g. if it runs over a ISDN
# uplink), add -n. See 'man rlogind' for more details.
# login stream tcp nowait root /usr/sbin/tcpd in.rlogind
# login stream tcp nowait root /usr/sbin/tcpd in.rlogind -a
# exec stream tcp nowait root /usr/sbin/tcpd in.rexecd
# talk dgram udp wait root /usr/sbin/tcpd in.talkd
# ntalk dgram udp wait root /usr/sbin/tcpd in.talkd
# These entries are for the KDE version of talk. If you enable them,
# you have to disable the version above.
```

```

# dgram udp wait root /usr/sbin/tcpd /opt/kde2/bin/ktalkd
# dgram udp wait root /usr/sbin/tcpd /opt/kde2/bin/ktalkd
#
#
# Pop et al
#
# pop2 stream tcp nowait root /usr/sbin/tcpd in.pop2d
pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/popper -s
#
# Imapd - Interactive Mail Access Protocol server
# Attention: This service is very insecure
# imap stream tcp nowait root /usr/sbin/tcpd imapd
#
# Comsat - has to do with mail.
#
# comsat dgram udp wait root /usr/sbin/tcpd in.comsat
#
# The Internet UUCP service.
#
# uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting. Most sites
# run this only on machines acting as boot servers.
#
# tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
# bootps dgram udp wait root /usr/sbin/bootpd bootpd -c /tftpboot
#
# Finger, systat and netstat give out user information which may be
# valuable to potential system crackers. Many sites choose to disable
# some or all of these services to improve security.
# Try telnet localhost systat and telnet localhost netstat to see that
# information yourself!
#
# finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd -w
# systat stream tcp nowait nobody /usr/sbin/tcpd /bin/ps -auwx
# netstat stream tcp nowait root /usr/sbin/tcpd /bin/netstat -a
#
# For man on the fly and ht://dig (full text search)
#
# http-rman stream tcp nowait.10000 nobody /usr/sbin/tcpd /usr/sbin/http-rman
#
# For XCept4
#
# btx stream tcp nowait root /usr/sbin/tcpd /usr/lib/xcept4/bin/ceptd -
i/usr/lib/xcept4/etc/init.ceptd -u/usr/lib/xcept4/etc/users.ceptd -l/var/log/log.ceptd
#
# For rplay daemon
#
# Old versions of rplay:
# rplay dgram udp wait root /usr/sbin/tcpd rplayd -b 8192 -c 60 -s 8192
# New Versions of rplay (>=3.3.0)
# rplay dgram udp wait root /usr/sbin/tcpd rplayd -t 30 -c 60 -s 16384 -F0 --inetd
#
# vbox (Voice Box)
# vboxd stream tcp nowait root /usr/sbin/tcpd /usr/sbin/vboxd
#
# For midinetd
# midinet stream tcp nowait root /usr/sbin/tcpd in.midinetd
#
# swat is the Samba Web Administration Tool
# swat stream tcp nowait.400 root /usr/sbin/swat swat
#
#
# amanda backup server with indexing capabilities
# amandaidx stream tcp nowait root /usr/lib/amanda/amindexd amindexd
# amidxtape stream tcp nowait root /usr/lib/amanda/amidxtaped amidxtaped
#
# amanda backup client
# amanda dgram udp wait amanda /usr/lib/amanda/amandad amandad
#
# the rsync daemon

```



```
# rsync stream tcp nowait root /usr/sbin/tcpd /usr/sbin/rsyncd --daemon
#
#
# Mimer database
# mimer stream tcp nowait root /opt/mimer/bin/mimtcp mimtcp -l
#
# CVS pserver (remote acces to your CVS repositories)
# Please read the section on security and passwords in the CVS manual,
# before you enable this.
# cvspserver stream tcp nowait root /usr/sbin/tcpd /usr/bin/cvs -f --allow-
root=/home/cvsroot pserver
#
# procstatd deamon (cluster software)
# procstatd stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/procstatd -i 7885
#
# End.
```

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix A – Continued:

etc/hosts.allow

See tcpd(8) and hosts_access(5) for a description.

```
#ALL EXCEPT in.fingerd, in.identd : ALL : spawn (safe_finger -l @%h 2>&1| \
# /bin/mail -s "%d-%h %u" root) &
popper: (enter your network range or individual ips here)
```

etc/hosts.deny

See tcpd(8) and hosts_access(5) for a description.
ALL: ALL EXCEPT localhost

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix B: SAINT Report

This is a text file output from running SAINT from a Linux laptop on our network.

```
[Data Analysis]
[WWDSI]                      Results - raven_line
[SAINT Home]
[Data Management] -----
[Target Selection]
[Data Analysis]      General host information:
[Configuration Management]
[SAINT Documentation] [BLACK] Host type: Linux 2.3.49

[Troubleshooting] [BLACK] Subnet 172.31.4
[BLACK] Scanning level: heavy
[BLACK] Last scan: Thu Feb 14 13:27:35
[-----]
2002

Vulnerability information: (Brown: 1 )

[BROWN] pop receives password in clear
Ignore

Actions:

[BLACK] Scan this host
[BLACK] Hide excluded records
-----
Back to the SAINT start page | Back to SAINT
Reporting and Analysis
```

Bibliography

Acheson, Steve; Green, John and Pomeranz, Hal, Topics in Unix Security, The SANS Institute, 2001

Barth, Stephen, et al., SuSE Linux 7.3 Quick Install Manual, SuSE GmgH Nuremberg, 2001

Brotzman, Lee, et al., Securing Linux Step-By-Step, The SANS Institute, 2001

Ball, Bill, et al., SuSE Linux Unleashed, Sams Publishing, 1999.

Butzen, Fred, and Hilton, Christopher S., The SuSE Linux Network, New York, NY, SuSE Press, 2001

Cunningham, Leah, et al., SuSE Linux 7.3 Reference Manual, SuSE GmgH Nuremberg, 2001

El-Dirghami, Nazeeth Amin, and Abu Kwaik, Youssef A., SuSE Linux Installation and Configuration Handbook, Indianapolis, IN, Que, , 2000

Pomeranz, Hal, UNIX Security Tools, Deer Run Associates, 2001

Sery, Paul G., and Kabir, Mohammed J., The SuSE Linux Server, Foster City, CA, SuSE Press, 2001

Toxen, Bob, Real World Linux Security, Upper Saddle River, NJ, Prentiss Hall, 2001

Web Site References

Arizona State University, Unix Network User's Group, "Best Practices"	http://www.asu.edu/it/ag/unug/bestpractices/
Dell Computers	http://www.dell.com
Huese, Mark "My Security Work at SuSE"	www.suse.de/~marc/SuSE.html
Imapd	http://asg.web.cmu.edu/cyrus/imapd/
OpenSSL	http://www.openssl.org/related/apps.html
Qpopper	http://www.eudora.com/qpopper_general/
Sendmail	http://www.sendmail.org http://www.sendmail.net
SuSE Home Page:	http://www.suse.com/index_us.html
Tripwire	http://www.tripwire.com

© SANS Institute 2000 - 2002. Author retains full rights.