Global Information Assurance Certification Paper

Name: Paul DePriest
GIAC Area: Securing UNIX GCUX Practical Assignment
Version: 1.6d
Title: CHECKLIST FOR SECURING REDHAT LINUX 7.1 ON AN IBM THINKPAD LAPTOP

This is a step by step checklist for securing Redhat Linux 7.1 on an IBM ThinkPad. I have used this checklist with both the IBM ThinkPad A21m and the A22m. These procedures should work for other laptops with minor modifications. The ultimate goal of this checklist is to provide a Linux system that will be secure in multiple network environments (such as a corporate network, customer's network, high speed Internet at a motel, or your home network).

The hardware configuration of the ThinkPad laptops I use are: 256 Mbytes of DRAM, 20 Gbyte disk, CD Drive, Zip250, floppy drive, Mini-PCI ethernet / modem Combo-Card, ATI Rage Mobility graphics card with 8 Mbyte Video RAM, and a 15 in. LCD display. If you have different hardware on your laptop, then you may need to select different configuration settings during the Linux installation process. After Linux installation, the remainder of the checklist should be the same for all hardware configurations you may encounter.

The following assumptions are made for this checklist:

1. You have some experience with using Linux or UNIX.
2. You can use an editor, such as `vi` or `emacs`.
3. You will be installing RedHat Linux 7.1
4. This laptop requires network access.
5. Netscape will be used for Web browsing.
6. You will need to compile and build executables.
7. This laptop has an ethernet adapter.
8. Networks that this laptop will connect to are assumed to be insecure.
9. This laptop will not provide any network services, such as sendmail, telnet, NFS, SSH, FTP, or DNS.

LEGEND: In this checklist, file names, lines of text from a system file, and commands are all in the `Courier` font. All commands are prefaced with: `[root]#` that represents a command prompt.

Suggestion: Record any specific information you decide to change from what is in this checklist. One approach is to print this checklist out and record all notes on the checklist itself.

Physical Security / BIOS Configuration

Since you are working with a portable system, you are the primary source of physical security for the laptop. Do not leave the laptop unattended in public environments (airports, hotel lobbies, and restaurants). Always make sure to either lock the screen or

log out when you are not at your system.

Before beginning the Linux installation, you should first make sure that the laptop itself is secure. The BIOS that is provided with the IBM ThinkPad gives you several security features. Note that some of the following BIOS options may not be available on your laptop. If you come to a step that mentions an option not available to you, please skip that step. Enable these security features by:

1.___ Power-on the Laptop.
2.___ Press the F1 key to enter the IBM BIOS Setup Utility.
3.___ Highlight "Config" and press the Enter key.
4.___ Highlight "Network" and press the Enter Key.
5.___ Disable "Wake on LAN" by:
    a. ___ Highlight "Wake on LAN and press the Enter key.
    b. ___ Highlight "Disabled" and press Enter key.
    c. ___ Press the Enter key once more to confirm your selection. The current setting will show Disabled.
6.___ Disable "Flash Over LAN" (follow pattern from step 5)
7.___ Disable "Alert On LAN 2"
8.___ Disable "Watchdog timer at ROM scan"
9.___ Press the <esc> key to return to the "Config" section
10.___ Highlight "Serial Port" and press the Enter key.
11.___ Disable the serial port and press <esc> key to return to "Config" section.
12.___ Disable "Infrared port".
13.___ Disable "Parallel port".
14.___ Press <esc> key to return to main section.
    NOTE: When selecting the passwords in the following steps, it is vital that you remember these passwords. If you forget them, you will have to return your laptop to IBM to get the passwords removed. Also, BIOS passwords can only be 7 characters long and may only consist of alphanumeric characters (A-Z, 0-9). I would suggest that you record these passwords, just in case you forget them. Of course, you will want to secure the written passwords in an appropriate manner (i.e., place in safe, sealed in envelope and given to your Security Officer, or place in Safe Deposit Box).
15.___ Highlight "Password" and press the Enter key.
16.___ Highlight "Power-On Password", press the Enter key.
17.___ Enter a password. Enter again to confirm.
18.___ Repeat Step 16 and 17 for "Supervisor Password"
19.___ Highlight "Lock BIOS Settings" and press the Enter key. Select Enable.
20.___ Highlight "Hard Disk1 Password" and press the Enter key.
21.___ Highlight "User", press Enter key and enter a password for User access. Press Enter key again for confirmation.
22.___ Press <esc> key to return to the main section.
23.___ Highlight "Startup", press Enter key.
24.___ Highlight "Boot", Press Enter key.
25.___ Highlight "Network Boot", Disable by pressing the <INS> key. An exclamation mark will appear to the left of the text to indicate Disabled.

26.___ Highlight "Intel(R) Boot Agent", Disable by pressing the <INS> key.
27.___ Press <Esc> key and Highlight "Network". Press Enter key.
28.___ Repeat Steps 25 and 26 to disable "Intel(R) Boot Agent" and "Network Boot" in this section also.
29.___ Press <Esc> key twice to return to the Main section.
30.___ Highlight "Restart". Press Enter key. Highlight "Exit Saving Changes". Press Enter key. Confirm by highlighting "Yes" and press Enter key.
31.___ When the Power-On Password prompt appears, turn off power to the laptop.

Note: If you will be using any of the ports disabled by the above steps, such as the serial or parallel ports, you will want to enable them when they are actively being used. Otherwise, keep them disabled.

You have now completed the most important steps in assuring the physical security of the laptop and its information contained within.

Pre-Installation Setup
Before beginning the RedHat Linux 7.1 installation, disconnect the laptop from any "live" network, whether connected to the Internet or not. Systems are extremely vulnerable during the software installation phase. Having done that, for ease of installation, I always connect the laptop to a hub so that network support will be installed during Linux installation. Obviously, you will not have a name server or DHCP server on this network of one laptop and a hub, so the network settings you use here will not be the same as you will need to enter later when you connect to a "live" network. This checklist will explain how to modify the network settings at the appropriate time.

1.___ Disconnect laptop from any "live" networks.
2.___ Connect laptop to a stand-alone network of just the laptop.
3.___ Collect the following network configuration information for placing the laptop on your "live" network:
   a)DHCP: Yes:___ No:___ If yes, you may not require the information below. Consult with your network administrator to determine which parameters are necessary for use with your DHCP Server. If no, then you will need all of the parameters below.
   b)Host IP address: _____
   c)Netmask: _____
   d)Default Gateway: _____
   e)Primary DNS Server: _____
   f)Secondary DNS Server: _____
4.___ Define and record disk partition information. Note that the size and which partitions are used is up to you. The following partitions are only suggestions.

	Mount Pt.	Disk Partition	Requested Size in MBytes
a)	/	_____	_____
b)	swap	_____	_____
c)	/var	_____	_____
d)	/usr	_____	_____

e) /opt _____ _____
f) /home _____ _____
g)_____ _____ _____

See Appendix A for the Disk partitions I use on my laptops.

RedHat 7.1 Linux Operating System Software Installation

The following steps are used to perform the RedHat Linux 7.1 operating system installation. Note: If you are familiar with the RedHat Installation process, your specific process may vary from the one presented here.

1.___ Power on laptop and press F12 to select alternate boot device
2.___ Insert RedHat Linux 7.1 CD (1 of 2) into CDROM drive
3.___ Enter Supervisor BIOS password.
4.___ Enter Hard Disk password.
5.___ Select ATAPI CD-ROM Drive as the temporary boot device by using the arrow keys. Press the Enter key to begin the boot process.
6.___ Press Enter key when prompted to begin the install process from the CD
Note: The remainder of the RedHat Linux 7.1 installation is done in a X-Windows Interface, so you will be using the mouse to select items on the menus and for navigation between the numerous screens.
7.___ Select installation language (Default = English), click Next button.
8.___ Leave default selections for Keyboard Configuration, click Next button.
9.___ Leave default selections for Mouse Configuration, click Next button.
10.___ After reading the Online Help frame, click Next button.
11.___ Select "Custom System" as the Install Type, click Next button.
Note: This checklist does not address setting up a laptop with multiple operating systems installed on the same hard disk. If you are wanting to run multiple operating systems on your laptop, please refer to http://www.redhat.com/docs/manuals/linux/RHL-7.1-Manual/custom-guide/dualboot-choosing.html
12.___ Disk Partitioning – Select "Manually partition with Disk Druid", click Next button.
13.___ For each existing disk partition:
a. ___ Highlight a line containing the partition information
b. ___ Click on the Delete button. Click on Yes button to confirm.
c. ___ Repeat until there are no more partitions defined.

NOTE: The following disk partitioning instructions are based on the definitions presented in Appendix A. Please make the appropriate changes to the Mount Points and Size fields in the steps below for your particular configuration.

Setup the / partition

14.___ Click the Add button to create a new partition.
15.___ Type / as the mount point for the first disk partition. (This is the slash character)
16.___ Enter the size of the / partition in Mbytes: 1024
17.___ Verify that the Partition Type is "Linux Native"
18.___ Click OK button.

Setup the swap partition

19.___ Click the Add button.

20.___ Leave the Mount Point field blank. Enter `512` for the Size.
21.___ Select "Linux Swap" for the Partition Type.
22.___ Click the OK button.
Setup the `/usr` partition
23.___ Click the Add button.
24.___ Enter `/usr` as the partition name.
25.___ Enter `6000` for the Size.
26.___ Verify that the Partition Type is "Linux Native" and click OK button.
Setup `/var` partition.
27.___ Click the Add button.
28.___ Enter `/var` as the Mount Point.
29.___ Enter `2048` for the Size.
30.___ Verify that the Partition Type is "Linux Native" and click OK button.
Setup `/opt` partition.
31.___ Click the Add button.
32.___ Enter `/opt` for the Mount Point.
33.___ Enter `4096` for the Size.
34.___ Verify that the Partition Type is "Linux Native" and click OK button.
Setup `/home` partition.
35.___ Click the Add button.
36.___ Enter `/home` for the Mount Point
37.___ Since this is the last partition, leave the Size field blank and Select "Use remaining space?" option.
38.___ Verify that the Partition Type is "Linux Native" and click OK button.
39.___ Record your Disk Partition Information here:

Mount Point	Device	Requested Size	Actual Size	Type
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

40.___ Click Next button.
41.___ Select all partitions for formatting.
42.___ Select "Check for bad blocks while formatting"
43.___ Click Next button.
44.___ In the "Lilo Configuration" section, select Create boot disk and Install LILO.
45.___ Deselect "Use linear mode."
46.___ Click Next button.

Network Configuration: (for this standalone network, please enter the address information provided in the steps below, not your information collected in the Pre-Installation Section)

47.___ Deselect "Configure using DHCP"
48.___ Enter the following network parameters:
IP Address: `10.10.10.10`
Netmask: `255.255.255.0`
Hostname: `localhost.localdomain`
Name Server IP Address: `10.10.10.1`
Note: Some of the remaining fields will be completed by the software for you. Leave these fields alone for now.
49.___ Click the Next button.
50.___ In the "Firewall Configuration" section select "High" security level and "Use default firewall rules."
51.___ Click Next button.
52.___ In the "Language Selection" select appropriate languages to install. Normal selection for USA based systems is "English (USA)". Click the Next button.
53.___ Select the "UTC Offset" Tab on the "Time Zone Selection" screen.
54.___ Highlight the appropriate Time Zone for your locale.
55.___ Select "Use Daylight Saving Time" if used by your locale.
56.___ Click Next button.

Account Configuration: Note: You are about to select your passwords for your Linux users' accounts. Be sure to follow good rules for password selection. See http://www.redhat.com/docs/manuals/linux/RHL-7.1-Manual/install-guide/s1-guimode-account.html#S2-GUIMODE-ROOT for details.
57.___ Enter the password you select for root. (Must be entered twice.)
58.___ Setup user account by defining, recording, and entering the following fields:
Account Name: _____
Password: _____ Note: *Do not record your password here*
Password (confirm): ____ Note: *Do not record your password here*
Full Name: _____
59.___ Click the Add button to actually create the account
Note: Normally you will be the only user for a laptop. If you have multiple users of the laptop, then repeat steps 59 and 60 as required.
60.___ Click the Next button.
61.___ Verify selection of "Enable MD5 passwords and "Enable shadow passwords."
62.___ Click Next Button.
63.___ Package Group Selection – select the Package Groups for your specific needs. See Appendix B for a list of Package Groups I use for my laptops. I would suggest that you use my list as a starting point. Only add packages to this list if you know you will need them.
64.___ Select "Select individual packages" option at the bottom of the screen.
65.___ Click Next button.
66.___ Click on the Triangle pointing to the right next to "Amusements". This will open up the sub areas for selection.
67.___ Highlight "Graphics". A list of Packages will appear.
68.___ Select "xlockmore"
69.___ Leave all other package selections as they are in this section.

70.___ Using the list provided in Appendix C, repeat this process for each of the Application Areas displayed on the left side of the screen.
71.___ Click the Next button.
72.___ If any Unresolved Dependencies are listed other than Canna-libs, you must decide whether to install the required packages or to not install packages with dependencies. Normally I select "Install packages that have dependencies" if it is obvious that I just forgot to select a package. Otherwise, I select "Do not install packages that have dependencies."
Note: the software packages actually installed will be recorded in the file `/tmp/install.log`
73.___ Click Next button
74.___ Verify that the "Skip X Configuration" option is NOT selected and click the Next button.
75.___ No changes required on the Monitor Configuration section. Click the Next button.
76.___ Select "Color Depth" to be: `True Color (24 Bit)`
77.___ Select Screen Resolution: `1024x762`
78.___ Select `Text` as the "Login Type"
Note: The choice of Login Type made here can be changed after installation. See Appendix D for details.
79.___ Click the Next button.
80.___ Click the Next button to begin actual installation.
81.___ Insert RedHat Linux 7.1 (2 of 2) CD when prompted and click OK button.
82.___ Insert a formatted floppy disk now.
83.___ Verify that the "Skip boot disk creation" option is NOT selected.
84.___ Click the Next button to create the boot floppy disk.
85.___ Click the Exit button.
86.___ Remove the floppy disk and the RedHat Linux CD.

The Laptop should now reboot and you should have a `login` prompt. Login as `root`.

NOTE: The remainder of the checklist will need to be performed as the user `root`. Either `login` as `root` or `su` to `root` to successfully complete this checklist.

Basic Post Installation Security Tasks
Disable the "Control-Alt-Delete" key sequence to prevent someone from trying to gain access to your system by rebooting to single user mode.
1.___ Edit the following line in the `/etc/inittab` file:
```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```
to read
```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Enforce use of `root` password for single user mode.
2.___Add the following line in `/etc/inittab` immediately after the line that begins with `si::sysinit ...`

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

3.___Activate the changes to `/etc/inittab` by executing the following command:

```
[root]# /sbin/telinit q
```

4.___(optional) If you are like me and don't like the graphical LILO startup window, delete the following line from `/etc/lilo.conf`

```
message=/boot/message
```

To provide another level of security, I recommend adding the use of a LILO Password. It is only used for the instances when you specify a boot option (such as when booting in single user mode).

5.___Edit the file `/etc/lilo.conf` and add the following 2 lines immediately after the `prompt` line:

```
password=<your-password>
restricted
```

Replace <*your-password*> with a strong password. Note: this password should be different from your other passwords.

6.___ Because this password is stored in clear text:

```
[root]# /bin/chmod 0600 /etc/lilo.conf
```

7.___Activate the above changes:

```
[root]# /sbin/lilo
```

Verify that `root` can only login locally and not over the network. The file `/etc/securetty` contains the list of "devices" `root` is allowed to login from. Verify that this file does not contain any "virtual" terminals. The only lines that should be in this file are lines containing `vc/[`<*number*>`]` and `tty[`<*number*>`]`, for instance, `vc/1`, `vc/2`, or `tty1`. Any other lines should be removed.

8.___ Edit `/etc/securetty`. Delete any lines not of the form:

```
vc/[<number>]
or
tty[<number>]
```

Delete all unnecessary accounts. Note: When deleting the account, do NOT delete the account's home directory. In some cases this directory is shared with another account.

9.___ Run the following program:

```
[root]# /sbin/userconf
```

a. ___ Highlight "User accounts" and press the Enter key.
b. ___ Highlight the account to be deleted: `ftp` and press the Enter key.
c. ___ Use the <TAB> key to select the "Del" option and press the Enter key.
d. ___ Use the down arrow key to highlight "leave the account's data in place" and press the <space> key to select this option.
e. ___ Use the <TAB> key to highlight the Accept button and press enter.

Repeat the above four steps (b-e) for the following accounts:
`gopher, gdm, games, news, operator`

f. ___ Use the <TAB> key to highlight the Dismiss button and press the Enter key.

g. ___ Use the <TAB> key to highlight the Quit button and press the Enter key.

10.___ View `/etc/shadow`. Only the `root` account and any user accounts you added during installation should have valid password entries. An account with a valid password will look like:

`root:`**`$1$GpWfImaA$Ijns59y37JHYTFPXc7YDy1`**`:11608:0:99999:7:::`

The bolded text is the encrypted password. If you find any entries other than `root` and the user accounts you created, remove the valid passwords, and thus disable logins for this account by:

a. ___ Edit `/etc/shadow`

b. ___ Replace the encrypted password string with an asterisk. Repeat for each password you need to invalidate.

Delete all occurrences of the file `.rhosts`. This file is used to define trusts between hosts so that users are not required to enter their passwords when accessing the remote (trusted) host.

11.___ Find and remove all instances of `.rhosts` file:

```
[root]# /usr/bin/find / -name '.rhosts' -exec /bin/rm {} \;
```

Configure Logging

Vital to Linux security is the ability to record what is happening on your system. This is accomplished by use of the `syslog` utility. Log rotations will be set up to ease in the review process and in compressing and archiving the older logs. The default settings for log rotations are for weekly rotations and to keep four weeks of backup logs. For more information on log rotation, view the `man` page for `logrotate`.

Caution: In the `/etc/syslog.conf` file, the whitespace between the two columns must be made up of only `<TAB>` characters. If not, the file will not be parsed properly and no logging may be done.

1.___ Modify the default logging by editing the `syslog` configuration file, `/etc/syslog.conf` First, modify the line:

```
#kern.*                 /dev/console
```

to

```
kern.*                  /var/log/kernel
```

Now add the following lines to the end of the `/etc/syslog.conf` file:

```
# Log all warnings and errors to syslog
*.warn;*.err            /var/log/syslog
```

2.___ Create new log files and set their permissions:

```
[root]# /bin/touch /var/log/syslog /var/log/kernel
[root]# /bin/chmod 0700 /var/log/syslog /var/log/kernel
```

3.___ Now force `syslogd` read the new configurations:

```
[root]# /usr/bin/killall -HUP syslogd
```

4.___ Configure log rotations for `/var/log/syslog` and `/var/log/kernel` by appending the following lines to the end of `/etc/logrotate.d/syslog`:

```
/var/log/kernel {
compress
postrotate
/usr/bin/killall -9 klogd
/sbin/klogd -2 &
endscript
}

/var/log/syslog {
compress
postrotate
/usr/bin/killall -HUP syslogd
endscript
}
```

xinted and TCP Wrappers

Remove all unnecessary services being offered by `xinetd`. Verify that that only the `rsync` service remains and is turned off.

1.___ Run the following commands:

```
[root]# /bin/rm /etc/xinetd.d/chargen
[root]# /bin/rm /etc/xinetd.d/chargen-udp
[root]# /bin/rm /etc/xinetd.d/daytime
[root]# /bin/rm /etc/xinetd.d/daytime-udp
[root]# /bin/rm /etc/xinetd.d/echo
[root]# /bin/rm /etc/xinetd.d/echo-udp
[root]# /bin/rm /etc/xinetd.d/time
[root]# /bin/rm /etc/xinetd.d/time-udp
[root]# /bin/rm /etc/xinetd.d/linuxconf-web
```

2.___ Confirm that the above services have been removed by running:

```
[root]# /sbin/chkconfig --list
```

The lines of interest will be all those immediately following the line:

```
xinetd based services
```

The only line after the above line should be:

```
        rsync:  off
```

If your output has more lines than this, check to make sure that you performed all of the above remove commands.

Set up the default TCP Wrappers configuration to deny all system access.

3.___ Add the following line to `/etc/hosts.deny` at the end of the file:

```
ALL:  ALL
```

Disable sendmail daemon mode and record what network services(ports) are active

Running `sendmail` in daemon mode is not necessary on this system. By running `sendmail` in daemon mode, it will be listening for a network connection, and thus would possibly be vulnerable to a network attack.

1.___ Disable `sendmail` daemon mode by editing the file `/etc/sysconfig/sendmail` to read:

```
DAEMON=no
QUEUE=15m
```

2.___ Restart `sendmail` by running:

```
[root]# /etc/rc.d/init.d/sendmail restart
```

3. ___ Record what network services/ports are currently active:

```
[root]# /bin/echo "netstat -at" > /tmp/net-serv.orig
[root]# /bin/netstat -at >> /tmp/net-serv.orig
[root]# /bin/echo -e "\nlsof -i +M" >> /tmp/net-serv.orig
[root]# /usr/sbin/lsof -i +M >> /tmp/net-serv.orig
```

See Appendix E for the contents of `/tmp/net-serv.orig` obtained from my system. Realize that this list will change depending on what software is running on your system. This file will serve as a reference point for you, so that you can become familiar with what services/ports are being used on your system and will be able to detect when some port is being used that shouldn't be.

IPCHAINS setup

During the installation process, "High" security mode was selected. Verify that this was set up properly.

1.___ Run the command:

```
[root]# /sbin/ipchains -L
```

2.___ Compare your output with the output provided in Appendix F.

3.___ If the output is the same, then you are through with this section, otherwise:

4.___ Run the command:

```
[root]# /usr/sbin/lokkit
```

This brings up a Graphical User Interface.

5.___ Select "High" Security Level

6.___ Using the <TAB> key, highlight the OK button and press the Enter key.

7.___ Repeat steps 1 – 3 above.

You are now ready to connect to a live network. Shutdown your system by entering:

```
[root]# /sbin/shutdown -h now
```

Connect to live network

Use the data collected in the Pre-Installation Setup to complete this section.

1.___ Connect the laptop to the desired network. Note: you will need Internet connectivity to complete this checklist.
2.___ Boot your laptop.
3.___ Login as `root` .

Reconfigure the networking parameters

4.___ Run the following:

```
[root]# /sbin/linuxconf
```

5.___ If this is the first time you have executed linuxconf, a help screen will be displayed. When you are through reading it, highlight the Quit button and press the Enter key.
6.___ Highlight "Client tasks", press the Enter key.
7.___ Highlight "Host name and IP network devices", press the Enter key.
8.___ Select the proper "Config mode" for your network. Normally this will be either "Manual" or "DHCP". If DHCP is chosen, then enter only the information not provided by your DHCP server. If you are not sure which parameters are provided by your DHCP server, please contact your network administrator before proceeding to the next step.
9.___ Enter "Primary name + domain". This is your fully qualified Domain Name.
10.___ Enter "IP Address" of your laptop and "Netmask" for your network.
11.___ Use the <TAB> key to select the Accept button and press the Enter key.
12.___ Highlight "Name server specification" and press the Enter key.
13.___ Enter the IP Addresses of the DNS servers for your network here.
14.___ (Optional) Enter the "default domain" and any "search domains" you use.
15.___ Use the <TAB> key to select the Accept button and press the Enter key.
16.___ Highlight "Routing and Gateways" and press the Enter key.
17.___ Highlight "Set Defaults" and press the Enter key.
18.___ Enter the IP Address of the Default Gateway for your network.
19.___ Use the <TAB> key to select the Accept button and press the Enter key.
20.___ Use the <TAB> key to select the Dismiss button and press the Enter key.
21.___ Use the <TAB> key to select the "Do it" button and press the Enter key.
22.___ Activate the changes:

```
[root]# /etc/rc.d/init.d/network restart
```

23.___Verify that your network settings are working by running:

```
[root]# /bin/ping <IP address of your default gateway>
```

Note: If you get errors on the above, verify your entries in the above steps. You may need to work with your network support personnel to verify that you have the correct addresses and that your laptop is connected to the network properly.

Setup ipchains with the new network settings.

24.___ Run the following:

```
[root]# /usr/sbin/lokkit
```

25. ___ Select "High" Security Level
26. ___ Using the <TAB> key, highlight the OK button and press the Enter key.
27.___ Verify that ipchains is setup properly by:

```
[root]# /sbin/ipchains -L
```

The DNS server addresses you entered in the network configuration above should be listed. See Appendix G for my results.

Install currently available patches and updates

Note: This process is extremely important to the security of your system. You should make sure that you keep the patches and updates on all the software you use current. I am presenting a process to get the initial system up to date. You will want to customize this process over time so that your system will remain current.

1.___Create a directory structure to store the updates in:

```
[root]# /bin/mkdir /usr/local/updates
[root]# /bin/mkdir /usr/local/updates/i386
[root]# /bin/mkdir /usr/local/updates/i686
[root]# /bin/mkdir /usr/local/updates/noarch
[root]# /bin/mkdir /usr/local/updates/kernel
```

The updates on the FTP sites are separated into the i386, i686, and noarch directories. I follow this same structure on my local system.

2.___Download the current package updates from either `updates.redhat.com` or one of their mirror sites (see html://www.redhat.com/download/mirror.html for listing). I used `metalab.unc.edu`. (Note that the upper level directory structure of the FTP site you are using may be different than that shown by the following instructions. The important thing to remember is to get the updates from the 7.1 directory tree.) Using `ncftp` to download, do the following:

```
[root]# cd /usr/local/updates
[root]# /usr/bin/ncftp metalab.unc.edu
ncftp> cd  \
/pub/Linux/distributions/redhat/updates/7.1/en/os/i386
ncftp> lcd i386
ncftp> get *
ncftp> cd ../i686
ncftp> lcd ../i686
ncftp> get *
ncftp> cd ../noarch
ncftp> lcd ../noarch
ncftp> get *
ncftp> quit
[root]# cd /usr/local/updates/i386
[root]# /bin/mv kernel-* /usr/local/updates/kernel
```

Perform the last two steps to separate the kernel updates from the other updates. This will enable all non-kernel updates to be made in one step. The kernel updates will be applied separately.

3.___Apply all but the kernel updates:

```
[root]# cd /usr/local/updates/i386
[root]# /bin/rpm -F -v *.rpm
[root]# cd /usr/local/updates/noarch
[root]# /bin/rpm -F -v *.rpm
```

Note: If either of the above commands generates a dependency error, then move the file that caused the error to another directory, such as `/tmp`, and try the command again.

4.___ Apply kernel updates.

First, you must "prepare" the kernel rpm files for updating. There will be two kernel rpm files of the form `kernel-2.x.x-xx-i386.rpm` and `kernel-2.x.x-xx-i686.rpm`. When you perform the following steps, you only want to install the "`i686`" version of this file. To do this, perform the following:

```
[root]# cd /usr/local/updates/kernel
[root]# /bin/rm kernel-2.*.i386.rpm
[root]# /bin/cp ../i686/kernel-2.*.i686.rpm .
[root]# cd /usr/local/updates/kernel
[root]# /bin/rpm -F -v *.rpm
```

Note: This step will normally result in five kernel rpm files. Four will come form the i386 directory and one from the i686 directory.

5.___ Get the version number of your updated kernel by:

```
[root]# /bin/ls /boot/vmlinuz*
```

This will output one file name, that will be used by the next command. At the time of the writing of this checklist, the file is `/boot/vmlinuz.2.4.3-12`

6.___ Update LILO information by editing `/etc/lilo.conf` to contain the file name for the new kernel found in step 5 above. Modify the following line

```
image=/boot/vmlinuz-2.4.2-2
```

to read:

```
image=<name of new kernel file>
```

7.___ Now execute the following command to save the new LILO information:

```
[root]# /sbin/lilo
```

8.___ Reboot the laptop now to make the updates active.

Setup tripwire

`tripwire` tests the integrity of the important files on the laptop. `tripwire` will test for changes to permissions of a file or if the contents of a file has been altered. Although it is somewhat cumbersome to configure, the benefits far outweigh the initial pain.

1.___ Login as root and start X-Windows by running:

```
[root]# /usr/X11R6/bin/startx
```

Note: Use X-Windows because later in this process, you will need to view the contents of two files simultaneously.

2.___ Open a "Terminal emulation program" window by clicking on the icon of the

terminal at the bottom of the screen. Repeat this, so that you have two windows open. The second window will be used later.

3.___ Run the following script to complete the tripwire installation process:

```
[root]# /etc/tripwire/twinstall.sh
```

Note: you will be prompted for both "site" and "local" keyfile passphrases. As always, select a strong password for each. Unlike the Linux password for your account, these can be longer than eight characters.

4.___ Initialize the tripwire databases by running:

```
[root]# /usr/sbin/tripwire -m i
```

5.___ Verify that tripwire can send email to the root account by:

```
[root]# /usr/sbin/tripwire --test --email root
```

6. ___ Check email and delete the tripwire message:

```
[root]# mail
& p
& d
& q
```

The `p` command prints the current message, `d` deletes the current message, and `q` quits the mail program. Note that if you have more than one email message in the queue, you will have to perform multiple `p` and `d` commands to get to the `tripwire` test message. The message you should have received should contain the following text:

"`If you receive this message, email notification from tripwire is working correctly.`"

7.___ Now perform the initial check of your system by running:

```
[root]# /usr/sbin/tripwire -m c
```

This compares the current state of the system files to the initial state saved in the `tripwire` database.

You will notice several "*File system error ... No such file of directory*" errors in the output. This is due to the initial `tripwire` policy being configured to analyze files that do not exist on your system. The next steps presented here will show you how to remove these non-existent files from the `tripwire` policy.

8.___ Create a new text copy of the tripwire policy file:

```
[root]# cd /etc/tripwire
[root]# /bin/cp  twpol.txt newtwpol.txt
```

9.___ Generate a tripwire report:

```
[root]# /usr/sbin/tripwire -m c -r twreport
```

10.___ In one terminal window, enter the following commands:

```
[root]# cd /etc/tripwire
[root]# /usr/sbin/twprint -m r -r twreport | more
```

This will allow you to view the report generated in step 9.

11.___ Scroll down until you can see the line:

```
Error Report:
```

Immediately after this line there will be several groups of numbered lines in the following format:

```
1.   File system error.
     Filename: /proc/scsi
     No such file or directory
```

12.___ In a second terminal window, bring up the new tripwire policy text file: `newtwpol.txt` in an editor.

13.___ Beginning with the first error (shown in the first terminal window), search for that file name in the `newtwpol.txt` file and delete the line containing the file name. Remember to search for the complete path name of the file as there could be multiple occurrences of the same file name in different directories. Repeat this step until you have located and deleted all file names not found by `tripwire`.

14.___ Delete all lines in `newtwpol.txt` that reference `/root/.<name>` except `/root/.bashrc` and `/root/.bash_profile`

15.___ Delete the line referencing `/var/lock/subsys`

16.___ Delete the line referencing `/var/log`

17.___ Save your modified `newtwpol.txt` file and exit the editor.

18.___ Execute the following to activate your newly defined policy.

```
[root]# /usr/sbin/tripwire -m p -Z low  \
          /etc/tripwire/newtwpol.txt
```

You will be prompted for both your site and local passphrases.

19.___ Now run `tripwire` with integrity checking:

```
[root]# /usr/sbin/tripwire -m c
```

This should generate a minimal number of errors now depending on .

20.___ Verify that tripwire will be run daily by checking for the existence of the file `/etc/cron.daily/tripwire-check`. This shell script will run daily to verify that the system files have not been tampered with.

Secure Netscape Browser

Complete this section only if you plan to use the Netscape Web browser. The following are the steps all users should perform to help in securing their Web browsing. The primary areas focused on here are cookies, application control, and history information. Cookies can contain sensitive and/or personal data that a Web Site will use to "recognize" you when accessing their Web Site.

1.___ Run Netscape Communicator:

```
[root]# /usr/bin/netscape
```

2. ___ Select "Preferences" from the Edit menu.

Note: The "Preferences" window will be used through step 24.

3.___ Highlight "Advanced" to display the Advanced Preference Section.

4.___ Under "Cookies" Select "`Only accept cookies originating from the same server as the page being viewed`".

5.___If you would like to be notified every time a cookie is being sent to your system, then select "`Warn me before accepting a cookie`". Note: Select this option if you want to find out just how many systems are using cookies. If it turns out that the sites you customarily visit use a lot of cookies, this will become a nuisance and you will want to disable it.

Netscape can process dozens of file types. This can cause numerous programs to be executed on your system. If the file contained a virus or Trojan, your system could be damaged or information be compromised. You need to limit the file types that Netscape will automatically process for you. These file types should be saved to disk, checked for problems, then executed if found to be safe.

6.___ Click on the triangle beside Navigator. Highlight "applications".
7.___ Highlight the first line that reads: "TROFF Document". Click the Edit button.
8.___ Select "Save to Disk" and click the OK button.
9.___ Repeat steps 7 and 8 for the next two lines that also read "TROFF Document".
10.___ Repeat steps 7 and 8 for "Word Perfect Document".
11.___ Repeat for all lines beginning with "Lotus".
12.___ Repeat for all lines beginning with "Microsoft".
13.___ Repeat for “Perl Program”
14.___ Repeat for "Bourne Shell Program".
15.___ Repeat for "C Shell Program".
16.___ Repeat for "Postscript Document".
17.___ Repeat for "Java Archive".
18.___ Repeat for "Unix CPIO Archive"
19.___ Repeat for "GNU Tape Archive"
20.___ Repeat for "Unix Tape Archive"
21.___ Repeat for “Unix Shell Archive”
22.___ Repeat for "Zip Compressed Data"
23.___ Repeat for all lines beginning with "Macintosh"

See Appendix H for a list of these applications and the reason for not executing them with any review.

Web sites can use the URL to encode some of your sensitive personal data. Since the URL's you have visited are stored in the history, it is in your best interest to remove them from your system after a short period. You should also limit access to the history list.

24.___ Highlight the line "Navigator" on the left side of the Preferences Window.
25.___ Modify the "History expires after" to be 1 day.
26.___ Click on the OK button of the "Preferences" Window to save these changes.
27.___ Exit the Netscape program.
28.___ Run the following command:

```
[root]# /bin/chmod 0600 $HOME/.netscape
```

NOTE: The commands, in the section above, will need to be repeated for each user account on the system that uses Netscape.

Testing your system's Security

The “final” step before you start using your system is to test your system's security posture.

1.___ Verify that you cannot get into BIOS setup without entering the correct Supervisor BIOS password.
   a. ___ Power on the laptop.
   b. ___ Press <F1> key to enter Setup.
   c. ___ Enter Power-On password.
   d. ___ Enter Hard Disk Password.

   The message "`BIOS setup is locked. Only the System Supervisor can make changes`" should appear at the top of the screen.

   Repeat entering the Supervisor password in place of the Power-On password.

   You should now be able to modify BIOS Configuration Settings.

2.___Verify that you cannot boot Linux in single user mode without entering the LILO password and the `root` account password.
   a. ___ At the LILO Prompt, enter the following line:
   ```
   boot: linux -s
   ```
   b. ___ Enter your LILO password here.
   c. ___ Enter the `root` password when prompted.
   d. ___ Enter the following command to complete the boot process:
   ```
   [root]# exit
   ```

3.___Verify that the audit logs contain data.
   ```
   [root]# cd /var/log
   [root]# ls -ltr
   ```
   You should see numerous log files output from the ls command, each of which should have recent modification times (i.e., `pacct, cron, lastlog, messages, wtmp`, ...)

4.___ (If available) Run a port scanner to verify that the network ports are closed and not listening for connections. I recommend `nmap` for this purpose. When I ran `nmap` against my system, it found no open TCP ports. For information on `nmap`, see http://www.insecure.org/nmap/

5.___ (If available) Run a vulnerability scanner against your system. I always run both Nessus and Sara. Both are freely available and provide useful results. For information on Nessus, see http://www.nessus.org and for Sara, see http://www-arc.com/sara/ Since your system is offering no network services, these scanners should find very few, if any, vulnerabilities with your system.

Backups

Concerning backups of the operating system you have just built, I do not think it is necessary to keep a disk image of it (not to mention that most laptops do not have a backup system installed). It is too easy to reinstall, if the need arises. Also, updates are coming out faster then ever, so you would have to create an image of your hard disk every time you update any system file or changed the configuration. It is just too easy to rebuild the laptop to justify the expense in making numerous disk images.

I would recommend that you backup the files that were recorded during the

performance of this checklist. There should be two files in the `/tmp` directory: `install.log`, and `net-serv.orig` . Also, you will want to save the `tripwire` policy file so that you do not have to repeat that long customization process and by not having the policy file on the system, a hacker does not know which files you are monitoring.

1.___ Insert a blank PC formatted floppy disk in your system.

2.___ Copy the files in /tmp to a floppy disk:

```
[root]# cd /tmp
[root]# /usr/bin/mcopy install.log a:
[root]# /usr/bin/mcopy net-serv.orig a:
```

3.___ Copy the tripwire profile to floppy disk

```
[root]# cd /etc/tripwire
[root]# /usr/bin/mcopy newtwpol.txt a:
```

4.___ Verify the files are on the floppy disk:

```
[root]# /usr/bin/mdir a:
```

5.___ Repeat steps 1 – 4 with a second floppy so that you have another copy of these files.

6.___ Remove these files from the hard disk:

```
[root]# /bin/rm /tmp/install.log /tmp/net-serv.orig
[root]# /bin/rm /etc/tripwire/newtwpol.txt
```

Note: If you need to update the tripwire policy, you will need to use the policy file from the floppy disk.

Note: These floppy disks should be treated as any normal backup. You should protect both copies of the floppy and one copy should be stored off site.

Note: Another important aspect of security is data integrity and reliability. You should backup all volatile data. This can be accomplished by using a Zip Disk or a CD RW drive if your laptop has one. Otherwise, you will want to copy your important files to a file server that is regularly backed up.

Using Your Newly Installed System

You are now ready to start using your system. You can now load any application software and get to work. However, the “real” security work on your system is just beginning. The next section covers tasks that you need to do on a periodic basis to make sure that you system remains secure.

Recurring Security Related Tasks

The frequency of the following tasks is based primarily on your specific environment. Some people will feel the need to perform them daily, while others may be content with once or twice per week. The choice is yours. The important thing to learn here is to get in the habit of performing these checks so that if your system is compromised, it will be detected in a timely manner.

1.___ At least weekly, read the email for the `root` account. It will contain information collected by `tripwire` and `syslog` programs.

2.___ At least biweekly view the log files for entries that you don’t think should be there, such as, file access violations, invalid login attempts, or system errors. Over time,

you will become familiar with the log entries and should be able to do this in a few minutes.

3.___ Periodically run the `lsof` and `netstat` commands (see "Disable sendmail daemon mode" section of this checklist for details) to see what services and ports are active on your laptop. This should be done several times during the day as you run different programs. As you become familiar with your software, you will run these commands less frequently. Ultimately, you will run them infrequently (every two weeks) or when you suspect your system has been compromised. Don't forget to compare the output to the original output you recorded during installation.

4.___ At least weekly, analyze the process accounting information to look for anomalous activity such as a user account that you did not create, or usage during a time period you were not using the system.

5.___ Check the `ftp` sites for updates to RedHat Linux packages. This should be done every two to four weeks.

6.___ Subscribe to Redhad Linux mailing lists to keep informed of what is happening in the Redhat Linux environment. See: http://www.redhat.com/mailing-lists/ .

7.___ Subscribe to security related mailing lists, such as SANS and CERT to keep up to date on security issues.

8.___ At least every three months, run a vulnerability scanner against your system to ensure that it is still secure.

NOTE: **You should keep this check list with any additional notes you made so that you will be able to repeat this process and that you will have documented what you did in securing your laptop system.**

APPENDIX A
Sample Disk Partition for 20 Gbyte Disk

The following are the disk partitions I use on my laptop systems.

Mount Point	Device	Requested Size (Mbytes)	Actual Size(Mbytes)	Type
/	hda1	1024	1026	Linux Native
/usr	hda5	6000	6002	Linux Native
/opt	hda6	4096	4097	Linux Native
/var	hda7	2048	2052	Linux Native
(swap)	hda8	512	516	Linux Swap
/home	hda9	*	5383	Linux Native

* - remainder of disk option was selected for /home partition.

APPENDIX B
RedHat Linux 7.1 Software Package Group Selection

The following is a list of the software packages I select for a laptop installation. (Note: I am not going to actually install all of the packages that are automatically selected. I always check the box to "select packages individually") to better refine my choices)

Printer Support
X Window System
Gnome
Dos/Windows Connectivity
Graphics Manipulation
Multimedia Support
Laptop Support
Networked Workstation
Dialup Workstation
Authoring/Publishing
Development
Kernel Development
Utilities

APPENDIX C
RedHat Linux 7.1 Individual Software Package Selection

The following is a list of the modifications I make when selecting individual software packages. For ease of use, I have included the changes I make and not the complete list of software packages that will be installed. Note that this list should just be used for Redhat Linux 7.1 software installation. As the software version changes, the list could also change.

To interpret this list I have provided the Major and Minor software areas and any package modifications that are needed. The software package name is preceded by an S for select and a D for deselect. Sections with no modifications are so noted.

1.1 Amusements-Games
(no changes)

1.1 Amusements-Graphics
S - xlockmore

2.1 Applications-Archiving
(no changes)

2.2 Applications-Communications
D - efax

2.3 Applications-Databases
(no changes)

2.4 Applications-Editors
S - vim-x11
S - vim-enhanced
S - xemacs
S - xemacs-el
S - xemacs-info

2.5 Applications-Engineering
S - gnuplot

2.6 Applications-File
(no changes)

2.7 Applications-Internet
D - finger
S - ftpcopy
S - gnome-lokkit
D - gq
S - htdig
S - htdig-web
S - htmlview
S - mtr
S - mtr-gtk
S - nc
D - nmh
D - open ldap-clients
D - talk
S - tcpdump
D - xchat

2.8 Applications-Multimedia
S - transfig
S - xfig
S - xmms-gnome
D - xsane

2.9 Applications-Productivity
(no changes)

2.10 Applications-Publishing

S - enscript

2.11 Applications-System
- S - firewall-config
- S - gnome-linuxconf
- D - irda-utils
- S - linuxconf
- S - parted
- S - procinfo
- S - procps-x11
- S - psacct
- S - rpmfind
- D - sane
- S - symlinks
- S - sysctlconfig
- S - systat
- S - tripwire
- S - vlock
- S - xcpustate
- D - xisdnload
- S - xosview
- S - xsysinfo

2.12 Applications-text
- S - mawk
- S - rgrep

3.1 Development-Debuggers
- S - lslk
- S - sysreport

3.2 Development-Languages
- S - itcl

3.3 Development-Libraries
- S - blas
- S - glibc-profile
- S - lapack
- S - libpcap
- S - tcllib

3.4 Development-System
(no changes)

3.5 Development-Tools
- S - Electric fence

S - dmalloc
S - gperf
S - lclint

4. Documentation
S - Xfree86-doc
S - bash-doc
S - blas-man
S - lapack-man
S - sendmail-doc

5.1 System Environment-Base
D - rhn_register
D - rhn_register-gnome
D - up2date
D - up2date-gnome
D - wireless-tools

5.2 System Environment-Daemons
S - xinetd

5.3 System Environment-kernel
(no changes)

5.4 System Environment-Libraries
S – Wnn6-SDK

5.5 System Environment-shells
S - pdksh
S - sash
S - zsh

6.1 User Interface-Desktops
(no changes)

6.2 User Interface-X
(no changes)

6.3 User Interface X-Hardware Support
(no changes)

APPENDIX D
Switching from Text to Graphical Login

To switch from text based logins to the graphical login screen, edit the file `/etc/inittab` and modify the following line:

```
id:3:initdefault:
```

to

```
id:5:initdefault:
```

The key here is the Run Level. 3 denotes text based logins and 5 the graphical login screen.

APPENDIX E
Initial list of Network Services

```
[root]# cat /tmp/net-serv.orig
netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:32768                 *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:x11                   *:*                     LISTEN

lsof -i +M
COMMAND     PID USER   FD   TYPE DEVICE SIZE NODE NAME
portmap     528 root    3u  IPv4    806       UDP *:sunrpc[portmapper]
portmap     528 root    4u  IPv4    807       TCP *:sunrpc[portmapper] \
(LISTEN)
rpc.statd   543 root    4u  IPv4    834       UDP *:719
rpc.statd   543 root    5u  IPv4    870       UDP *:32768[status]
rpc.statd   543 root    6u  IPv4    873       TCP *:32768[status] (LISTEN)
X         16654 root    1u  IPv4  96616       TCP *:x11 (LISTEN)
```

APPENDIX F
ipchains for the "private" network configuration

```
Chain input (policy ACCEPT):
target     prot opt    source              destination     ports
ACCEPT     all  ------ anywhere            anywhere        n/a
ACCEPT     udp  ------ 10.10.10.1          anywhere        domain ->   any
REJECT     tcp  -y---- anywhere            anywhere        any ->   any
REJECT     udp  ------ anywhere            anywhere        any ->   any
Chain forward (policy ACCEPT):
Chain output (policy ACCEPT):
```

APPENDIX G
ipchains for the "live" network configuration

```
Chain input (policy ACCEPT):
target     prot opt    source              destination     ports
ACCEPT     udp  ------ ns1.mynetwk.com     anywhere        domain ->   any
ACCEPT     udp  ------ ns2.mynetwk.com     anywhere        domain ->   any
ACCEPT     all  ------ anywhere            anywhere        n/a
REJECT     tcp  -y---- anywhere            anywhere        any ->   any
```

```
REJECT     udp  ------  anywhere            anywhere        any ->   any
Chain forward (policy ACCEPT):
Chain output (policy ACCEPT):
```

APPENDIX H
Potentially Dangerous Netscape Applications

Application	Reason
GNU Tape Archive	Writes files
Unix Tape Archive	Writes files
Unix Shell Archive	Writes files / Issues commands
Zip Compression Archive	Writes files
Perl Program	Issues commands
Bourne Shell Program	Issues commands
C Shell Program	Issues commands
TROFF Document	Shell escape
WordPerfect Document	Potential/Unknown problems
Lotus *	Potential/Unknown problems
Macintosh *	Potential/Unknown problems
Microsoft *	Potential/Unknown problems
Java *	Potential/Unknown problems
PostScript Document	Possible shell escape
Unix CPIO Archive	Writes files

* Denotes names beginning with this character sequence

The majority of the above table is taken from the book “Real World Linux Security” by Bob Toxen on page 240.

REFERENCES

Brotzman, Lee. Securing Linux Step-by-Step version 1.0. SANS, 2000.

Pomeranz, Hal. “Securing UNIX Systems.” Course Reference, SANSFIRE July/August 2001

Toxen, Bob. Real World Linux Security. Prentice-Hall, Inc. 2001

Peterson, Richard. Linux The Complete Reference Fourth Edition. Osborne / McGraw-Hill. 2001

Last Updated: June 24th, 2018

Upcoming Training

SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 30, 2018**	**Live Event**
SANS London October 2018	**London, United Kingdom**	**Oct 15, 2018 - Oct 20, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**