

# **RedHat Linux 9 Workstation Security Best Practices**

Johns Hopkins Network & Information Security  
June 2003

## Secure installation of RedHat 9 as a workstation

Information you may need ahead of time:

- How many hard drives do you have?
- What size is each hard drive (e.g., 3.2GB)?
- If you have more than one hard drive, which is the primary one?
- What kind of hard drive do you have (e.g., IDE, SCSI)?
- How much RAM do you have (e.g., 256MB RAM)?
- Do you have a SCSI adapter? If so, who made it and what model is it?
- Do you have a RAID system? If so, who made it and what model is it?
- What type of mouse do you have (e.g., PS/2, Microsoft, Logitech)?
- How many buttons does your mouse have (2/3)?
- If you have a serial mouse, what COM port is it connected to (e.g., COM1)?
- What is the make and model of your video card? How much video RAM do you have (e.g., 4MB)?
- What kind of monitor do you have (make and model)?
- Will you be connected to a network? If so, what will be the following:
  - Your IP address?
  - Your netmask?
  - Your gateway address?
  - Your domain name server's IP address?
  - Your domain name?
  - Your hostname?
  - Your number and types of network(s) card(s) (make and model)?

### Basic Steps to follow

- 1.Install Operating System
  - a.Configure Partitions
  - b.Create strong root password
- 2.Strip the Operating System
  - a.Disable unneeded startup scripts.
  - b.Remove unnecessary user accounts
  - c.Set /dev/null shells for unused accounts
- 3.Harden Operating System
  - a.Remove unneeded packages
  - b.Configure global login settings
  - c.Set global umask
- 4.Configure Networking
  - a.Ensure routing settings are appropriate for environment.
  - b.Disable dhcp and multicast if not in use
  - c.Configure dns and routing
  - d.Configure syslog to log authentication information
- 5.Install and configure Security Tools
  - a.TcpWrappers
  - b.Secure Shell
- 6.Monitor Activity and Patches

## 1.Install the OS

- a. Obtain the software, either download ISO image and make a CD. Or you can install it via ftp over the Internet or from another box.
  - i. You may or may not need a boot floppy.
  - ii. Use rawrite to write one of the images found on the CD to a floppy.
    - 1. Rawrite can be found in the dosutils directory of the RedHat CD.
  - iii. Images are found in the images directory.
    - 1. Depending on the version of RedHat there may be different images you need.
    - 2. The bootdisk.img is used to install from CD.
    - 3. There are supplemental driver disks, if you wish to install from the network, or have an unrecognized block device.
- b. **\*Important\*** Do not connect to a network until machine is fully configured and secured. Default RedHat installation is very vulnerable to attack. If you must install via ftp, disconnect as soon as install is finished.
- c. Most new computers will boot off the CD, so just put the CD in and power on. If the machine will not boot off the CD, you will need to use one of the boot images to install from the CD.
- d. There are 3 options for default installs, and then a custom
  - i. Personal Desktop, Workstation, Server
    - 1. Each will pre-select which packages you will most likely need.
    - 2. Each option allows for custom, and individual package selection
  - ii. Custom
    - 1. Asks more questions, fewer default package groups selected.
- e. Plan the disk space, according to use of machine.
  - i. You should at least have a separate partition for /, /var, /usr and swap. /home and /usr/local are optional depending on your requirements.
    - 1. / 150MB
    - 2. /boot ~100MB
      - a. This is where your kernel will sit.
    - 3. swap -2x Installed memory (max. 1GB swap)
      - a. It is a good idea to put the swap partition near the beginning of the drive. The beginning is physically located on the outer portion of the cylinder, so the read/write head can cover more ground per revolution.
    - 4. /var > 256MB
      - a. Logging information will can be kept here.
      - b. For syslog/web/news/proxy servers, consider using a larger partition and/or a separate disk.
    - 5. /home >256MB
      - a. Size according to type & number of users on system.
      - b. If possible put on a separate disk
    - 6. /usr > 768MB
      - a. Contains system files and directories that can be shared with other users.
      - b. Files that run only on certain types of systems are in the /usr directory.
      - c. Files (such as manual pages) that can be used on all types of systems are in /usr/share.
      - d. If using separate /usr/local partition, it is possible to make /usr as read-only, this will protect your server from some types of attacks and rootkits
        - i. /dev/hda9 /usr ext2 defaults 1 2
        - ii. /dev/hda9 /usr ext2 ro 1 2**
    - 7. /usr/local - rest of drive space

- a. Most common location for custom applications. Many system administrators compile applications here.
  - b. If you know you will be storing large amounts of data, it does not hurt to put it on a separate disk if possible. That way if the system crashes it is possible to recover data easily.
- 8. If you plan on having a user environment, it is always a good idea to put that on a separate partition or disk.
  - a. This allows you to separate the users files from the system files
  - b. Can also allow for more control of what type things users are allowed to do
  - c. Helpful for quotas as well.
- f. Choice of Grub or Lilo – just a preference choice, the default is grub.
  - i. Grub will allow you to set a grub password.
    - 1. This password will need to be entered to make changes to booting?
    - 2. Can help with linux single boot issue.
  - ii. For most cases the master boot record is the best place.
  - iii. Depending on your hardware you may need to send commands to the SCSI controller at boot time, here is where you can do that.
  - iv. Can also decide not to install a bootloader at all.
    - 1. If this is a dual boot machine, you may need to do this.
  - v. You can create a boot disk here also. Even if you don't think you need one, it is a good idea to make one anyway.
- g. Set the time zone
- h. Set root password and set a user account. \*\*Make sure all user accounts, especially root, have a good password
  - i. The password should not be based on any personal information such as: names, addresses, phone number, birthday, etc.
  - ii. The password should be a minimum of 6 characters long.
  - iii. The password should be a combination of uppercase and lowercase letters.
  - iv. The password should include letters, digits, and special characters
    - 1. Including: [ '~!@#\$%^&\*()-\_+=+{[]}\|'";:,<.>/? ]
  - v. The password should not be any word found in any language. Substituting numbers for letters does not help here, because password-cracking utilities take this into account. For example, using r1dg3 instead of ridge is still a bad idea.
  - vi. A good password makes it much harder for a hacker to break into your system.
- i. Firewall Configuration
  - i. High, Medium, No Firewall
  - ii. If you know that you will not be providing servers from this machine, you can select HIGH
- j. X configuration
  - i. Select monitor type.
  - ii. Select video card and amount of memory on video card.
  - iii. Also, when you run the Xconfiguration it will ask you if you want the graphical interface to startup on boot.
    - 1. This determines whether your machine boots to the GUI (runlevel 5) or the command line (runlevel 3)
    - 2. This can be changed later by editing the default runlevel line in /etc/inittab.
- k. You can now select which packages to install or, if you didn't select custom, you have the option to just take what packages were pre-selected, or to customize. It is fairly easy to remove

packages after installation of OS is complete. Or install new ones for that matter. However, make sure to view the install.log to see if there are some things installed you do not need. You can consult RedHat.com for information on packages if you don't know what they mean.

1. Select groups of packages based on need.
  2. The best practice is to install as little as possible.
    - a. With the RedHat network, it is very easy to add packages after the fact
    - b. If it isn't installed it can't be exploited
    - c. The less services and applications you have running, the smoother your system will run.
  - ii. Packages will now be installed. Time may vary greatly depending on amount of packages and hardware.
1. When you first reboot the following services will be started, and need to be stopped. To stop the services, go to /etc/rc.d/init.d and type ./<servicename> stop. It is also possible to turn these services off via the Services GUI. Which can be found under system settings → Server Settings → Services.
- i. nfslock
  - ii. sendmail
    1. Mail server
    2. If not configured properly can be severe security risk
  - iii. xinetd
    1. Daemon that listens for TCP or UDP connections then passes that connection to the appropriate service.
  - iv. portmap
    1. Server that converts RPC program numbers into DARPA protocol port numbers.
    2. Must be started before any RPC servers are invoked.
  - v. isdn
  - vi. pcmcia
    1. If you don't have pcmcia devices you can safely turn this off.

## 2. Configuring Networking and Services

- a. Here you can list any aliases or DNS information you wish the computer to have or for other machines DNS information.
  - i. /etc/hosts
- b. DNS information, DNS server IP addresses and search domains. It is important to have this set correctly if you want your computer to access the network or Internet.
  - i. /etc/resolv.conf
    1. domain jhu.edu
    2. nameserver 128.220.2.7
    3. nameserver 128.220.2.82
- c. Scripts to start and stop networking. Scripts for network interfaces can be manipulated with different IP or broadcast information.
  - ii. /etc/sysconfig/network-scripts/
    1. ifcfg-eth[depends on # of interfaces]
      - a. Here you can set the IP address and broadcast information
      - b. Can be used to bring interface up and down for configuration changes.
      - c. -- sample --

```
DEVICE="eth0"
BOOTPROTO="none"
IPADDR="128.220.xxx.xxx"
```

```
NETMASK="255.255.255.0"
NETWORK=128.220.xxx.0
BROADCAST=128.220.xxx.255
ONBOOT="yes"
```

-- sample --

iii./etc/sysconfig/network

- 1.Default gateway information
- 2.--sample

```
NETWORKING=yes
FORWARD_IPV4="no"
HOSTNAME="<hostname>"
GATEWAY="128.220.xxx.1"
GATEWAYDEV="eth0"
```

-- Sample --

d.Disable Network Services not being used. Leaving these services running opens you to vulnerabilities, as well as impacting performance.

- 1.There are several network services that start up at boot time, and run until the system is shutdown. Examples are:

- a.httpd: for the web server
- b.named: for DNS services
- c.smbd : for Samba SMB networking services

- 2.You can check which processes are started at boot time. Different processes are started for different runlevels.

- a.Typing **chkconfig --list** will show which services are set to run in which runlevels. You can turn services on or off with:

**chkconfig servicename off/on --level #**

- b.The 2 normal runlevels are 3 (console) and 5 (X Windows). You can find all the processes that are started automatically.

- i.For runlevel 3 in directory: /etc/rc.d/rc3.d

- ii.For runlevel 5 look in: /etc/rc.d/rc5.d.

- c.Files found in these directories are links to /etc/rc.d/init.d/, so you can safely delete unused files as long as the original script remains in the init.d. You will only need to do this if you do not have the chkconfig command.

- d.Each of the scripts is prefixed with an S or K. The S means the script is used for startup, and the K means the script is called for shutdown (Kill). At any time, user root can start or shutdown any of these services.

- e.You should also remove all start up scripts from unused runlevels

- i.You can use `chkconfig servicename off --level#`

- ii.Or you can use `rm S*` in each unused runlevel directory rc4.d, rc2.d

- f.For example to turn off the web server type in:

**/etc/rc.d/init.d/httpd stop.**

3.The best way to test your setup is to reboot. If services still startup that shouldn't, use **chkconfig --list** and the /etc/rc.d/rc\*.d directories again and verify services are turned off.

ii.Disable Xinetd

1.Xinetd is a daemon whose purpose is to listen for TCP or UDP connections.

When a connection is received, inetd passes that connection to the appropriate service.

a.You will want to disable any of these services that might enable someone to get unwanted access to your computer. Unless you need access to your machine from a different computer, there is no need to run these services.

b.Remember that when you disable these services, you may still use telnet on your computer, but people cannot telnet to your machine.

i.You only want to run the processes you need.

ii.Anything additional gives hackers more of a chance to gain access to your machine.

iii.If you absolutely have to have remote access to your computer, do not use telnet or ftp. Instead use ssh or scp. See documentation on SSH for more information.

c.If you have no services running with xinetd prevent the service from restarting.

i.**chkconfig xinetd off** will do this.

ii.If you do not have chkconfig installed, you can rename the xinetd startup script in /etc/rc.d/rc{?}.d.

iii.Be sure the new file name does NOT begin with an S.

e.You can create a message that appears whenever someone accesses or logs in to your machine.

This may be required on some systems, to alert people they are accessing a sensitive system and that they are being monitored.

i./etc/issue is banner that comes up when system is accessed. It is a good idea not to reveal too much information as to the contents and use of the box in issue. Any user who attempts to connect to your box will see this information and can use it to find vulnerabilities.

ii./etc/motd is shown after a successful login. Here you can give more specific information if you desire, because the user has already authenticated to the box. Issue is not shown when using ssh, however motd can be if selected in ssh config.

iii.Sample motd or issue:

\*\*\*\*\*

Use of this system is restricted to authorized personnel only.

All use of and activity on this system is monitored and logged. Use of this system constitutes consent to such monitoring.

See <http://www.nts.jhmi.edu> or contact

security@jhmi.edu for more information.

\*\*\*\*\*

- iv. Use secure shell if you need remote access to your computer. If you don't need remote access to your computer, then you do not need secure shell.
- v. Remember that instead of ftp you can use the sftp or scp that comes in the ssh package you have just installed.

### 3. Hardening the OS

#### a. Password protect boot loader

- iv. It is possible to boot linux in single user mode and gain root access without a password. Setting a password on the bootloader will prevent this access.

#### v. lilo

1. at the following lines to the beginning of /etc/lilo.conf  
restricted  
password=<password>
  2. Change permissions to ensure only root can read lilo.conf  
chown root:root /etc/lilo.conf  
chmod 600 /etc/lilo.conf
- lilo

#### vi. grub

1. Add this line to /etc/grub.conf  
Password <password>
2. Change permissions to ensure only root can read grub.conf  
chown root:root /etc/grub.conf  
chmod 600 /etc/grub.conf

#### b. By default if the most minimal RedHat install will install unneeded packages.

- i. Remove as many unneeded packages as possible.
- ii. The more packages the more exploits.
- iii. Rather than trying to keep up with security alerts, simply remove all items you are not planning to use.

#### c. Typing "**rpm -qa > installed\_rpm**" will create a file displaying all the packages installed.

- i. Even if you plan to run some of the services not included in this list, it is a good idea to remove them anyway.
- ii. You will want to install the latest possible version of all programs, and to start from a solid baseline.
- iii. **rpm -e <packagename>** will remove packages from system.
- iv. **rpm -i <packagename>** will install packages. You can find most packages on the RedHat CD in the RPMS directory.
- v. **rpm -U <packagename>** will upgrade packages.

#### d. If you don't know for sure if you **need** a package, do not install them.

- i. Almost every new software you try to install will tell you what it depends on to run
- ii. Always try to upgrade to most recent version.
- iii. Using the Redhat Network is a good way to keep up with the current fixes.
  1. It can automatically tell you what packages you need to update
  2. Even if you only use this as a notification process, it can be very helpful
  3. It is also helpful when installing new packages, as it will automatically find dependencies and install the appropriate packages.

#### e. Time to verify configurations.

- i. Before starting the GUI type **ps -ef** the typical output should look like this:

```
UID    PID  PPID  C  STIME TTY      TIME CMD
```

```

root    1    0 0 Aug30 ?    00:00:01 init [3]
root    2    1 0 Aug30 ?    00:00:01 [kswapd]
root    3    1 0 Aug30 ?    00:00:00 [kflushd]
root    4    1 0 Aug30 ?    00:00:00 [kupdate]
root   328    1 0 Aug30 ?    00:00:00 syslogd -m 0
root   506    1 0 Aug30 tty1   00:00:00 login -- <username>
<username> 871 506 0 07:51 tty1   00:00:00 -bash
daemon 349    1 0 Aug30 ?    00:00:00 /usr/sbin/atd
xfs    1657    1 0 11:22 ?    00:00:03 xfs -port -1 -daemon
root   336    1 0 Aug30 ?    00:00:00 klogd
root   362    1 0 Aug30 ?    00:00:00 crond
root   442    1 0 Aug30 ?    00:00:00 gpm -t ps/2
root   507    1 0 Aug30 tty2   00:00:00 /sbin/mingetty tty2
root   508    1 0 Aug30 tty3   00:00:00 /sbin/mingetty tty3
root   509    1 0 Aug30 tty4   00:00:00 /sbin/mingetty tty4
root   510    1 0 Aug30 tty5   00:00:00 /sbin/mingetty tty5
root   511    1 0 Aug30 tty6   00:00:00 /sbin/mingetty tty6
root  1536 1535 0 11:01 pts/5   00:00:00 bash

```

1.If you are running other services, you will also see them here

ii.Type netstat -an

1.This shows you active connections. If you are not running any network services, you should not see an services in "LISTEN" state

Active Internet connections (servers and established)

```

Proto Recv-Q Send-Q Local Address      Foreign Address   State
udp      0    0 128.220.xxx.xxx:123  0.0.0.0:*
udp      0    0 127.0.0.1:123     0.0.0.0:*
udp      0    0 0.0.0.0:123      0.0.0.0:*

```

Active UNIX domain sockets (servers and established)

```

Proto RefCnt Flags   Type       State      I-Node Path
unix  2    [ ACC ] STREAM   LISTENING  1182    /dev/gpmctl
unix  5    [ ]     DGRAM          673    /dev/log
unix  2    [ ]     DGRAM          1767
unix  2    [ ]     DGRAM          1001
unix  2    [ ]     DGRAM          743

```

#### f. Configure Sendmail.

i. Some Standard Mail User Agents invoke sendmail directly to deliver mail; therefore even if sendmail is not running as a service, it still needs to be configured.

ii. If you are only using sendmail to send email, edit /etc/sysconfig/sendmail and change the DAEMON option to no.

iii. You will need to add the fully-qualified domain name to /etc/hosts

1. Be sure to add it after the short name

2. 128.220.xxx.xxx                   servername   servername.jhu.edu

iv. Configure the /etc/mail/sendmail.cf so sendmail uses a "Smart" relay

1. Look for this line:

```
# "Smart" relay host (may be null)
```

2. Then add this below it: DSsmtp.jhu.edu

g. Restrict at/cron to authorized users

- i. The cron.allow and at.allow files are lists of users are allowed to run the crontab and at commands to submit jobs to be run at scheduled intervals.

```
cd /etc
rm -rf cron.deny at.deny
echo root > cron.allow
echo root > at.allow
chown root:root cron.allow at.allow
chmod 400 cron.allow at.allow
```

- h. Set default umask for users

- i. This will help prevent users from accidentally creating world-writable files for file in profile csh.login csh.cshrc bashrc

```
do
if [ `grep -c umask $file` -eq 0 ];
then
    echo "umask 022" >> $file
fi
chown root:root $file
chmod 444 $file
```

done

- i. Harden /etc/passwd and /etc/shadow

- i. Remove unneeded system accounts

- 1. the command userdel can be used to remove accounts for user in uucp uucp nuucp adm lp smtp listen

```
do
userdel $user
```

- ii. Remove unneeded groups

- 1. use groupdel to remove unneeded groups for group in news uucp games dip lp

```
do
groupdel $group
```

- iii. Set the shell for the following accounts to /dev/null: (disables login)

- 1. Use usermod -L -s /dev/null username to set shell to /dev/null for user in daemon bin sys nobody noaccess nobody4

```
do
usermod -L -s /dev/null $user
```

## 7. Available tools

- a. If you have multiple similar machines, the best practice would be to compile on only one machine. Do not install compilers unless you need them, or uninstall them when not using them.

### b. Tcpwrappers

- i. Tcpwrappers allow you to control which IP addresses can connect to which services. It will create two files: /etc/hosts.allow and /etc/hosts.deny

- c. You can use IP addresses or domain name information. Do not put things like 128.220. or jhu.edu.

This makes room for a greater chance of being hacked, since internal mischief can occur.

- d. Your /etc/hosts.allow should look like this to allow ssh in from specific hosts:

**i.sshd: xxx.xxx.xxx.xxx**

- ii. Remember that services run as daemons. Meaning if you want to control who can connect to telnet, you must put in.telnetd not just telnet.
- e. In order to use Tcpr wrappers in conjunction with inetd, you must edit the lines of the services you wish to use.
  - i. To use Tcpr wrappers with ftp for example in /etc/inetd.conf:
    1. ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd
    2. change to
    3. ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd in.ftpd
  - ii. Be sure to restart the inetd process after making changes.
  - iii. Tcpr will be created during the make above, copy this to /usr/sbin for this work.
- f. Prevent access from anyone not specifically allowed.
  - i. Configure /etc/hosts.deny
    1. Blanket deny ALL:ALL statement. /etc/hosts.allow overrides /etc/hosts.deny, so deny all and allow specifically. You can have email messages sent if access is attempted
    2. /etc/hosts.deny should look like this:  
**ALL:ALL: /usr/bin/mailx \**  
**-s "%s: connection attempt from %c" \**  
**[user@domain.com](mailto:user@domain.com)**
- g. To allow access using Tcpr wrappers, edit the /etc/hosts.allow file.
  - i. For example to allow ftp access you would add the line:  
**in.ftpd : host.you.want.to.allow**
  - ii. You can use IP addresses or DNS information here.
- h. **Install SSH** <http://ftp.ssh.org/>.
  - iv. Secure shell allows you to securely connect to a remote machine. It is highly recommended that you use ssh exclusively. It replaces, telnet, ftp and all r commands. See secure shell documentation on JHNIS website (<http://nts.jhmi.edu/es/infosec/>) for more information.
  - v. NOTE\* Please be sure to check the version of SSH installed.
- j. Iptables
  - i. Iptables is a firewall which will allow you to control access to your machine.

#### 4. Should do level 0 (complete) backup now.

- i. Attempt to keep backup secure.
- ii. Keep tape separate from other backup to prevent tape from being overwritten.
- iii. If you can avoid it, do not use a networked backup scheme.
  1. Usually requires additional software to be installed.
  2. Often these programs overrides system security
  3. Data most likely passed in clear text.
  4. If someone is monitoring network traffic, they can see all your files.

### 5. Monitoring and Patching

- a. Monitor your system activity on a regular basis.
  - i. Check /var/log/syslog and dmesg frequently for any unusual activity.
  - ii. As well as changes to any system files, especially /etc/passwd and /etc/shadow.
- b. Check <http://nts.jhmi.edu/infosec> frequently, as alerts are posted here.
- c. Check [www.redhat.com/errata](http://www.redhat.com/errata) frequently. It contains bugfixes and security advisories.
- d. The RedHat Network is a service available to update RedHat packages automatically.
  - i. It helps to resolve dependencies and maintain consistency across several systems.
  - ii. Visit <http://rhn.redhat.com/> for more information.