

RedHat Linux 9 as a Server Best Practices

Johns Hopkins Network & Information Security
June 2003

Secure installation of RedHat 9 as a Server

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 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 Software upgrades

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. Boot disk images are found in the images directory.
 - 1. Depending on the version of RedHat there may be different images you need.
 - 2. The boot.img is used to install from CD.
 - 3. Bootnet.img and pcmcia.img are used if you are installing over the network.
- 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. On the first screen hit enter to select the standard GUI install.
 - i. Select the custom install.
 - 1. This will allow you to select particular packages you want to install or not install.
 - 2. You want to load the minimum amount of packages, without losing functionality.
 - 3. The less software that resides on the box, the fewer potential security exploits or holes may appear.
- 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. 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.
 - 3. /var > 512MB
 - 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.
 - 4. /home >256MB
 - a. If going to be webserver, you will want to increase this partition greatly.
 - b. Size according to type & number of users on system.
 - c. If possible put on a separate disk
 - 5. /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.
 - 6. /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.
 - 7. If you plan on having an anonymous ftp server or any sort of chroot environment, it is best to put that on a separate partition as well.

- f. Select either lilo or grub bootloader
 - i. Selecting Grub as a bootloader will allow you to add a password
 - 1. This protects the system against physical access issues
 - 2. Boot options cannot be passed without this password
 - 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 lilo 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. Authentication Configuration.
 - i. MD5 passwords and shadow passwords should be enabled.
 - ii. And you should not be using NIS.
- j. You can now select which packages to install or, if you didn't select custom watch as the packages you didn't get to choose are installed. It is fairly easy to uninstall 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.
 - i. Select groups of packages based on need. For example if you need printer support, install it.
 - 1. For basic network connectivity and tools, install these software groups.
 - a. Networked Workstation
 - b. Network Management Workstation
 - c. Utilities
 - 2. Selecting these groups will NOT install support for any sort of GUI interface.
 - 3. The reason for selecting these limited groups is any software on the CD will be out of date.
 - a. It is better to make sure you have the latest, most secure version of any software you run.
 - b. Also, this ensures that you install the minimum amount of packages.
 - ii. Packages will now be installed. Time may vary greatly depending on amount of packages and hardware.
- k. 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
 - i. indentd

- 1. Operates by looking up specific TCP/IP connections and returning the user name of the process owning the connection.
- 2. It can optionally return other information instead of a user name
- ii. sendmail
 - 1. Mail server
 - 2. If not configured properly can be severe security risk
- iii. xfs
 - 1. X Window System font server. It supplies fonts to X Window System display servers.
 - 2. Only needed if running GUI
- iv. inetd
 - 1. Daemon which listens for TCP or UDP connections then passes that connection to the appropriate service.
- v. portmap
 - 1. Server that converts RPC program numbers into DARPA protocol port numbers.
 - 2. Must be started before any RPC servers are invoked.
- vi. lpd
 - 1. line printer spooler daemon
 - 2. You will need this if you are going to be running print services

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.
 - i. /etc/sysconfig/network-scripts/
 - 1. ifcfg-eth[depends on # of interfaces]
 - a. here you can set ipaddress, broadcast information
 - b. Can be used to bring interface up and down for configuration changes.
 - c. -- sample --


```

DEVICE="eth0"
BOOTPROTO="none"
IPADDR="128.220.72.xxx"
NETMASK="255.255.255.0"
NETWORK=128.220.72.0
BROADCAST=128.220.72.255
ONBOOT="yes"

```
 - sample --
 - ii. /etc/sysconfig/network
 - 1. Default gateway information
 - 2. --sample

```
NETWORKING=yes
FORWARD_IPV4="no"
HOSTNAME="<hostname>"
GATEWAY="128.220.72.1"
GATEWAYDEV="eth0"
```

-- Sample --

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

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

1. 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 #**

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

a. For runlevel 3 in directory: `/etc/rc.d/rc3.d`

b. For runlevel 5 look in: `/etc/rc.d/rc5.d`.

3. 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.

4. 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.

5. For example to turn off the web server type in: **`/etc/rc.d/init.d/httpd stop`**.

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

e. Disable Internet Daemon Services

i. A default server install with no package groups selected will NOT install `xinetd`

ii. `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.

1. 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.

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

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

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

c. 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.

3. If you are not planning to run any services from `inetd` prevent the service from restarting.

a. **`chkconfig xinetd off`** will do this.

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

c. Be sure the new file name does NOT begin with a S.

- f. 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
 - i. 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.
 - ii. `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
```
 - iii. `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.If you are running a user system, it is a very good idea to configure the /usr partition to be read-only

i.edit /etc/fstab

- 1.find the line referencing /usr
- 2.change the options to "ro"
- 3.You will need to reboot for this to take effect

ii.This works best if you have created a separate /usr/local partition

iii.To remount as read-write

- 1.mount -o remount rw /usr
- 2.You will need to do this for patching
- 3.must reboot to remount as read-only

c.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.

d.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.

e.If you do not know for sure if you **need** a package, do not install it.

i.Especially for user systems, being sure of what packages are installed can help prevent compromise

ii.Always try to upgrade to most recent version.

iii.If you have KDE installed, there is kpackage, this program will display all installed packages and descriptions.

iv.It will warn you of dependencies and give recommendations on when packages should or shouldn't be installed.

f.It is a good idea to check out www.freshmeat.net.

i.Here you can find information on most packages and new releases and security fixes for them.

ii.If you plan to run a web server or and other network service, you should download the latest possible version and verify patch levels.

g.Time to verify configurations.

i. 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
```

```

root    336    1 0 Aug30 ?    00:00:00 klogd
root    362    1 0 Aug30 ?    00:00:00 crond
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

Active UNIX domain sockets (servers and established)

Proto RefCnt Flags Type State I-Node Path

h.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.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

iii.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

i.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

j.Harden /etc/passwd and /etc/shadow

i.Remove unneeded system accounts

ii.the command userdel can be used to remove accounts

for user in uucp uucp nuucp adm lp smtp listen

do

userdel \$user

done

k.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
l.Remove unneeded groups
i.use groupdel to remove unneeded groups
for group in news uucp games dip lp
do
  groupdel $group
done
m.Set the shell for the following accounts to /dev/null: (disables login)
i.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
n.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.
    a.If someone is monitoring network traffic, they can see all your files.
o.Protect suid & sguid executables
i.Restricting who can run certain executables is a very good way to protect your server
ii.Change permissions on /bin/su
  1.chmod 750 /bin/su
  2.chmod u+s /bin/su
  3.chgrp wheel /bin/su
iii.Then add any users that should have rights to switch users to the wheel group
p.Restrict outbound access
i.Use iptables to control what outbound connections can be made from your system
ii.Will help prevent your system from being used in initiating attacks against others
iii.Example: /etc/sysconfig/iptables

*nat
PREROUTING ACCEPT [4:168]
POSTROUTING ACCEPT [2:335]
OUTPUT ACCEPT [2:335]
COMMIT
*mangle
:PREROUTING ACCEPT [23:3207]
:INPUT ACCEPT [23:3207]

```

```

:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [21:8428]
:POSTROUTING ACCEPT [21:8428]
COMMIT
*filter
:OUTPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
-A OUTPUT -p tcp -m tcp -d 128.220.2.66 --dport 25 -j ACCEPT
-A OUTPUT -p tcp -m tcp -d 128.220.2.67 --dport 25 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp -d 128.220.2.7 --dport 123 -j ACCEPT
-A OUTPUT -m state --state NEW,INVALID -j DROP
COMMIT

```

- iv. These rules will prevent any new connections being initiated from your system
 - 1. except mail, to the mail relays
 - 2. dns requests
 - 3. SSL for connections to the RedHat Network
 - 4. NTP connections to the NTP servers
- v. All traffic is allowed inbound with these rules.

4. Install tools

- a. Use tcpwrappers to 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

```
 - b. To allow access using tcpwrappers, edit the /etc/hosts.allow file.
 - i. For example to allow ftp access you would add the line:
 - ii. in.ftpd : host.you.want.to.allow
 - iii. You can use ip addresses or dns information here.
 - c. Install SSH <ftp://ftp.ssh.org/> (see http://nts.jhmi.edu/es/infosec/ssh2_stock_config.pdf)
 - d. 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 the nts website (<http://nts.jhmi.edu/es/infosec/>) for more information.

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 www.redhat.com/errata frequently. It contains bugfixes and security advisories.
- c. There are some programs that will search the internet and install updated packages for you.
 - i. These programs will only upgrade packages you already have installed.
 - ii. They explain the reasons the new versions were released.
 - 1. Up2date is the name for RedHat 6.1 and newer.

- a. Allows for demo account, but you get a survey every 6 months in order to keep the account open
 - b. If you pay, you get better access to iso images, and will always be able to download updates
 - c. Has a notification service to keep you updated.
2. MandrakeUpdate works for Mandrake.