CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

RedHat Enterprise Linux 3.0 Minimization and Hardening Guidelines

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: 13-05-2005

Contents

1. Introduction

This document discusses about hardening and securing RHEL 3.0 server, Kernel version 2.4. The emphasis is laid on securing the server by installing the minimal required packages only. Server with this configuration can be extended for using as a web or mail server by adding the additional packages as per requirement. The commands and configurations mentioned in this document have been tested on the same platform

2. Installation

Installation Requirements

i. Partition: Use separate partitions for ***/boot, /, /usr, /home*** and ***/var***

ii. File System: Use ***ext3*** file system

iii. Boot Loader: Choose ***GRUB*** as the boot loader as it stores the boot loader password in encrypted form.

Selection of Packages

The users are suggested to install only the required packages, however unlike Red Hat Linux 9.0 and previous versions there is no option for individual package selection in case of RHEL 3.0. The default minimal installation of RHEL 3.0 includes 253 packages We can further minimize it by removing not required packages. This can be done by using Kickstart installation. The Kickstart installation provides a way of deselecting the packages from the base component (minimal installation). A possible list of minimum packages and related configuration (ks.cfg) file is also given for reference.

i. From any other RHEL installation copy the ***anaconda-ks.cfg*** file present in /root directory and rename it as ***ks.cfg*** or edit a text file and rename it as **ks.cfg.**

```
[root@localhost root]# cp    anaconda-ks.cfg     ks.cfg
```

ii. Edit the ***ks.cfg*** to mention the installation type, root password, timezone, etc.

iii. In ***%packages*** section of ***ks.cfg*** enter name of the packages that are not required as given below.

```
@base
  -at
  -attr
  -wvdial
```

```
-ppp
  …..
  …..
```

A sample ***ks.cfg*** file can be downloaded from http://cert-in.org.in/knowledgebase/guidelines/ks.cfg

iv. Copy ***ks.cfg*** file into a floppy

```
[root@localhost root]# cp   ks.cfg   /mnt/floppy/
```

v. Boot the system with first RHEL CD-ROM

vi. Insert the floppy into floppy drive

vii. At the boot prompt type ***linux ks=floppy*** and press enter

```
boot: linux ks=floppy
```

viii. After completion of installation checkout the install.log file in the /root directory. It should list 95 packages, which are listed in Annexure A.

Post Installation Minimization

There are some packages which do not get removed by kickstart installation due to their inter-dependency. Among these are ***comps, cyrus-sasl, cyrus-sasl-md5, openldap, openssl, kbd, kudzu, krb5-libs, lvm, mkinitrd*** and ***usermode***.These can be removed with the help of rpm utility by using ***--nodeps*** option.

```
[root@localhost root]# rpm   -e   - -nodeps   cyrus-sasl
```

.Further Minimization

i. Remove unnecessary documentation related to software

```
[root@localhost root]# rm    -rf    /usr/share/doc/*
```

ii. Remove unnecessary empty files and directories

iii. Disable unnecessary services

a. Check the startup scripts in ***/etc/rc3.d***; disable the not required startup scripts. To disable scripts either remove the files from ***rc3.d*** folder or rename the files without “S” at the start

For e.g.,

```
[root@localhost root]# mv   S25<service name>   nostart-S25<service name>
```

A possible listing of minimal services is

S10network, S12syslog and S17keytable

b. List the services that are running by the command

```
[root@localhost root]# ps   -aux
```

To disable the service from /etc/rc.d/init.d directory simply delete the service by issuing a command

```
[root@localhost root]# rm –rf <service name>
```

iv. Remove Remote service daemons and binaries

Remove files like ***.rhosts*** and ***.netrc*** used by remote services like ***rsh*** and ***rlogind***

```
[root@localhost root]# find / -name ".rhosts" –print
[root@localhost root]# rm –f <filename>
```

Update software

The Red Hat Network allows administrators to efficiently manage software installation and upgrades using a combination of RHN account and the **up2date** utility. If support is available to you install the rpm **up2date** and upgrade all installed packages.

3. Access Controls

i. Set BIOS password

ii. Set GRUB boot loader password through the following steps

a. Create a password hash by issuing the command ***/sbin/grub-md5-crypt***

b. Edit ***/boot/grub/grub.conf*** to add the following line after timeout tag

```
password -md5 <generated md5 hash>
```

iii. Avoid booting into single user mode without root password. Edit ***/etc/inittab*** and add the following line after *id:3:initdefault:*

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

iv. Create a custom banner message in ***/etc/issue*** and ***/etc/issue.net***

Example banner message: UNAUTHORISED ACCESS IS PROHIBITED

v. Choose passwords that are complex to guess. Set password parameters (max. days, min. days, min. length etc.,) in ***/etc/login.defs***

vi. Disable ***CTRL+ALT+DEL*** by commenting the line ***ca::ctrlaltdel:/sbin/shutdown -t3 -r now*** in ***/etc/inittab***

vii. Edit ***/etc/profile*** file and set TMOUT=3600. This will automatically timeout bash shell after 3600 seconds

viii. Restrict root login to only one ***tty*** and one ***vc***. Edit ***/etc/securetty*** to comment out the lines tty2 to tty11 and vc/2 to vc/11

ix. Delete unnecessary system users and groups from ***/etc/passwd*** and ***/etc/group\***

```
[root@localhost root]# userdel    <username>
[root@localhost root]# groupdel   <groupname>
```

Following are some system users and groups that can be deleted

Users: ***lp, sync, shutdown, halt, news, gopher, operator, games, mail , uucp, ftp***

Groups: ***lp, games, uucp***

x. Change default shell for users ***bin, daemon, rpm, vcsa, nobody*** to ***/dev/null***

4 File System Security

i. Set the UMASK attribute in ***/etc/profile*** to ***033***

ii. Find world writable files and change the permission if world writable permission is not required

```
[root@localhost root]# find   / -perm -2 type f –print
[root@localhost root]# chmod   <permissions>   <filename>
```

iii. Find out hidden files and directories

```
[root@localhost root]# find / -name “..” –print –xdev
[root@localhost root]# find / -name “.*” –print –xev | cat –v
```

Carefully check the files and keep a list of default hidden files for later on regular audit reference. If any of the files are not required remove them by

```
[root@localhost root]# rm –rf <file name>
```

If any world writable file is not required, set the sticky bit

```
[root@localhost root]# chmod   +t   <file name>
```

iv. Find out the executables with SUID or SGID bit set and keep track of what they are so that administrator is aware of any changes.

```
[root@localhost root]# find / -type f \( -perm -04000 -o -perm -02000 \) -exec ls -l {} \;
```

v. Removable media ***nosuid*** and ***nodev*** option

Edit ***/etc/fstab*** to

mount /boot with ***nodev*** and read only option

```
Label=/boot  /boot          ext3          nodev,ro……
```

mount cdrom and floppy with ***nosuid*** and ***nodev*** option

```
/dev/cdrom      /mnt/cdrom    udf,iso9660    nosuid,nodev,noauto,…….
/dev/fd0        /mnt/floppy   udf,iso9660    nosuid,nodev,noauto,……
```

vi. Remove the files with no user and no group

```
[root@localhost root]# find / -nouser –o –nogroup –exec rm –rf {}\;
```

vii. Change the permissions for the following files

```
chmod 600 /etc/passwd
chmod 600 /etc/shadow
chmod 100 /bin/rpm
chmod 100 /bin/tar
chmod 100 /bin/gzip
chmod 100 /bin/ping
chmod 100 /bin/gunzip
chmod 100 /bin/mount
chmod 100 /bin/umount
chmod 100 /usr/bin/gzip
chmod 100 /usr/bin/gunzip
chmod 100/usr/bin/who
chmod 100 /usr/bin/lastb
chmod 100 /usr/bin/last
chmod 100 /usr/bin/lastlog
chmod 100 /sbin/arping
chmod 100 /usr/sbin/arping
chmod 100 /usr/sbin/usernetctl
chmod 100 /usr/sbin/traceroute
chmod 400 /etc/syslog.conf
chmod 400 /etc/hosts.allow
chmod 400 /etc/hosts.deny
chmod 400 /etc/sysconfig/syslog
chmod 644 /var/log/wtmp
chmod 644 /var/log/utmp
```

viii. Change the attributes for the following files

```
chattr +i /etc/passwd
chattr +i /etc/shadow
chattr +i /etc/services
chattr +i /etc/gshadow
chattr +i /etc/group
chattr +i /etc/login.defs
chattr +i /etc/init.d/
chattr +i /etc/services
chattr +i /etc/inittab
chattr +i /etc/fstab
chattr +i /usr/bin/who
chattr +i /usr/bin/lastb
chattr +i /usr/bin/last
chattr +i /usr/bin/lastlog
chattr +i /etc/syslog.conf
chattr +i /etc/sysconfig/syslog
```

ix. Set file system limits instead of allowing unlimited usage. Control the per-user limits using the resource-limits file ***/etc/security/limits.conf*** and a PAM module For example, limits for group `***users***' might look like this:

```
@users    hard  core    5000
@users    hard  nproc   50
@users    hard  rss     5000
```

This says to limit the creation of core files, restrict the number of processes to 50, and restrict memory usage per user to 5 MB

5 Kernel Security

i. Set the following kernel parameters

```
echo 0 > /proc/sys/net/ipv4/tcp_syncookies
echo 0 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 4096 > /proc/sys/net/ipv4/tcp_max_syn_backlog
echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```

ii. Add the following in the ***/etc/sysctl.conf***

```
net.ipv4.tcp_max_syn_backlog =4096
net.ipv4.conf.all.rp_filter =1
net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.all.secure_redirects=0
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.default.accept_source_route=0
net.ipv4.conf.default.accept_redirects=0
net.ipv4.conf.secure_redirects=0
net.ipv4.conf.eth0.forwarding =0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.defaults.send_redirects=0
```

6 Log Security

i. Add an entry in ***/etc/hosts*** file for the central syslogger . The entry could be

```
<ip address>        loghost
```

ii. Change the default ***/etc/syslog.conf*** file with the following

```
*.debug                            /var/log/messages
kern.debug                         /var/log/kernel.log
user.debug                         /var/log/user.log
mail.debug                         /var/log/mail.log
daemon.error,info,alert,notice     /var/log/daemon.log
auth.notice,crit,info              /var/log/auth.log
authpriv.debug                     /var/log/authpriv.log
local2.notice,alert                /var/log/sudo.log
syslog.debug                       /var/log/syslog.log
*.*                                @loghost
```

iii. Create *btmp* file in /var/log directory

```
touch /var/log/btmp
```

iv. Turn on accounting of processes

```
accton /var/log/pacct
```

7. Iptables Firewall

The Network firewall security policy defines the access or level of access to the different services and applications. The methods to implement firewall rules are given below.

i Everything not specifically denied is permitted

ii Everything not specifically permitted is denied

Set the firewall policy to drop all packets as defined in second method

```
iptables  -P  INPUT   DROP
iptables  -P OUTPUT  DROP
iptables  -P FORWARD  DROP
```

Now depending upon the Firewall policy, administrator can define firewall rule sets to explicitly grant access to only permitted services or applications.

8. Tools

i Integrity Checkers – ***md5sum, sha1sum*** and ***Tripwire***

ii Port Scanners - ***nmap***

iii Vulnerability Assessment - ***nessus*** and ***SARA***

9. References

1. http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/x8664-multi-install-guide/
2. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-kickstart2-file.html
3. Securing and optimizing Linux - “The Ultimate Solution” - Gerhard Mourani Available at http://www.openna.com/pdfs/Securing-Optimizing-Linux-The-Ultimate-Solution-v2.0.pdf

Annexure A

basesystem
bash
beecrypt
bzip2
bzip2-libs
chkconfig
comps-3es
coreutils
cracklib
cracklib-dicts
glib
glib2
Glibc
Glibc-common
Gpm
Grep
Grub
Gzip
hwdata
Info
libuser
losetup
Lvm
Makedev
Mingetty
Mkinitrd
Mktemp
Modutils
Mount
Ncurses
rpmdb-redhat
Sed
Setup
Setuptool
shadow-utils
Slang
Slocate
Sysklogd
SysVinit
Tar

crontabs

cyrus-sasl

cyrus-sasl-md5

db4

dev

devlabel

diffutils

e2fsprogs

elfutils-libelf

ethtool

file

filesystem

findutils

gawk

gdbm

initscripts

iproute

iptables

iputils

Kbd

kernel

kernel-utils

krb5-libs

kudzu

less

libacl

libattr

libgcc

libstdc3

libtermcap

Netconfig

net-tools

newt

openldap

openssl

pam

passwd

patch

pcre

popt

procps

psmisc

readline

rootfiles

rpm

Termcap

Tmpwatch

Tzdata

Usermode

util-linux

vim-common

vim-minimal

Which

Words

Zlib