

*CERT-In Security Guideline CISG-2004-01*

# **CERT-In**

**Indian Computer Emergency Response Team**  
*Handling Computer Security Incidents*

## **SECURING RED HAT LINUX 9.0 AS A WEB SERVER**

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

Issue Date: June 04, 2004

## Table of Contents

- 1) *Introduction*
- 2) *Minimization*
- 3) *Access controls*
- 4) *File system Security*
- 5) *Kernel Security*
- 6) *Log Security*
- 7) *Iptables / Checksum*
- 8) *Security Tools*
- 9) *References*

## 1. Introduction

This document has been created for: RedHat Linux 9.0 available from <http://www.redhat.com/download/products.html>

Update patches downloaded from <http://www.redhat.com/apps/support/errata/>

The commands and configuration contained in this document have been tested on the above mentioned platform.

### Assumptions

The configuration contained in this document attempts to minimize the services so as to run as a web server only. Thus the server shall not have the following

- Xwindows
- Any remote commands
- Minmal/no xinettd services (telnet, ftp etc)
- network services (NFS, NIS etc)
- RPC services, no portmapper
- Printer, kudzu daemon
- default web/mail/DNS services

## 2. Minimization

### Installation requirements

- i. Partition: Use separate partitions for /, /boot, /usr, /swap, /var
- ii. File System: Use ext3 file system.

- iii. Boot Loader: Use GRUB (Grand Unified Boot Loader) as this boot loader stores the boot loader password in encrypted form.

Use the “minimal” option with “select individual packages” in the package selection menu

A possible minimal package listing is given below -

```
acl, attr, cron, devlabel, diffutils, dump, eject, elfutils, ethtool, flex, iptables, libtool-libs, logrotate, mt-st, netconfig, ntsysv, pax, pciutils, rmt, slocate, setuptool, sudo, time, tmpwatch, gcc, make, libstdc++, binutils, cpp, glibc-devel, glibc-kernheaders
```

The following packages (gcc, make, libstdc++, binutils, cpp, glibc-devel, glibc-kernheaders etc) can be removed after initial compilation of required applications like apache etc.

### Further Minimization:

Check the startup scripts at /etc/rc3.d, disable the unrequired startup scripts. To disable the startup scripts either remove the files from rc3.d folder or rename the files without a “S” at the start.

e.g mv S25netfs nostart-S25netfs

A possible listing of the minimal services required is given as below

```
S08iptables, S10network, S12syslog, S17keytable, S90crond
```

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

Syntax: rm -rf <service\_name>

**Remove Remote services daemons and binaries:** Remove files *.rhosts* and *.netrc*, used by remote services like *rsh* and *rlogind*.

```
find / -name “.rhosts” -print
find / -name “.netrc” -print
rm -rf <filename>
```

### Minimize xinetd services

If the above installation steps (with only specified packages selected), the xinetd services are not installed.

However if any of the xinetd services are required

Remove unnecessary xinetd services from /etc/xinetd.d

Apply proper access control at /etc/xinetd.conf using *only\_from*, *no-access*, *access\_times* etc.

### 3. Access controls

i. **BIOS Password:** Set Bios Password

ii. **Boot Loader Password:** Set GRUB boot loader password through the following steps:

#### Encrypted

- i. Create a password hash by issuing the command `/sbin/grub-md5-crypt`
- ii. Add the following directives and the password hash created above to the `/boot/grub/grub.conf` file after `timeout` tag `password --md5 <password_hash>`
- iii. Change the permission of this file. This can be done by issuing command `chmod 600 /boot/grub/grub.conf`

#### Clear Text

Add this line to `/etc/grub.conf` before the first uncommented line.

`password <password>`

iii. **Banner Creation:** Create a secure banner for the system in `/etc/issue` and `/etc/issue.net` file

An example of Banner: “UNAUTHROISED ACCESS IS PROHIBITED”

iv. **Password Security:** Set password parameters (max days, min days, minimum length etc) in `/etc/login.defs`.

v. **Disable CTRL+ALT+DEL:** Avoid abnormal shutdown by pressing CTRL+ALT+DEL, Put a '#' sign in front of the `ca::ctrlaltdel:/sbin/shutdown -t3 -r` no line in `/etc/inittab` file.

vi. **Specify the timeout for the root user.** This can be done by adding a line `TMOUT=3600` in `/etc/profile` just above the `HISTSIZE` tag.

vii. **Restrict the root user** logging into tty's and Virtual Consoles. This can be done by removing the `tty/x – tty/xx` and `vc/1 – vc/11` in `/etc/securetty` file

viii. **Delete un-necessary users and groups:** Delete un-necessary users and groups from `/etc/passwd` and `/etc/group` file.

`userdel <user_name>`

`groupdel <user_name>`

Following is list of users and groups which can be deleted

#### Users

Lp, sync, shutdown, halt, news, operator, games,  
gopher, mail, ftp, uucp

#### Groups

lp, games, uucp

- ix. **Change Default shell for other users:** Change the default shell to */dev/null* in */etc/passwd* file for the following users.

**Users**

Bin, daemon, rpm, vcsa. Nobody

## 4. File system security

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

- ii. **World writable files/directories:**

Find world writable files

```
find / -perm -2 -type f -print
```

Change the permission if world writable permission is not required

```
chmod <permissions> <filename>
```

- iii. **Hidden directories and files:**

Find out hidden files and directories by the following command.

```
find / -name “.” -print -xdev
```

```
find / -name “.*” -print -xdev | 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

```
rm -rf <file_name>
```

If any world writable file is required, set the sticky bit.

```
Chmod +t <file_name>
```

- iv. **SUID and SGID** bit set files-

Due to these bits a normal user can execute those files with the same user privileges set for the binary.

Find SUID root files

```
find / -type f -perm -04000 -ls
```

Find GUID root files

```
find / -type f -perm -02000 -ls
```

Check the executables with *suid* or *guid* bit set, if not required change the permission and keep a list of all such files for later on audit reference.

```
chmod -t <filename>
```

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

**File /etc/fstab**

*mount /boot with nodev option*

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:**

```
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
```

viii. **Change the attributes for the following files**

For the following directories and binaries; change the file permissions or change the attributes as immutable.

```
chattr +i /etc/passwd  
chattr +i /etc/shadow  
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
```

## 5. Kernel setting:

- i. Set the following kernel parameters

```
echo 0 > /proc/sys/net/ipv4/tcp_syncookies
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_repsonses
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 /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.default.secure_redirects = 0
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

- iii. Disable core dumps

```
File: etc/security/limits.conf
*      soft   core    0
*      hard   core    0
```

## 6. Log Security:

- i. Add an entry in /etc/hosts file for the central sysloger. The entry should be  
*<ipaddress>*                      *loghost*

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

Syslog log level

```

*.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. This can be done by issuing the following command.

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

- iv. Turn on accounting of processes.

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

**Centralized log server: Syslog-ng**

## 7. Iptables / Checksum

### Configure iptables

```
Iptables -A INPUT -j DROP
```

```
Iptables -A OUTPUT -j DROP
```

```
Iptables -A FORWARD -j DROP
```

```
iptables -A INPUT -s 0/0 -i eth0 -d localhost_ip -p TCP --dport 80 -j ACCEPT
```

```
iptables -A OUTPUT -d 0/0 -i eth0 -s localhost_ip -p TCP --sport 80 -j ACCEPT
```

**\*\*localhost\_ip** is the own ip address.

**\*\*Change iptable configuration as required by other applications like ssh etc.**

### Calculate checksum

After completion of installation of OS and required application calculate the checksum of the entire file system by using `md5sum` command or `sha1sum` command

Syntax: md5sum <filename> > <file.md5>  
sha1sum <filename> > <file.sha>

**Tool: tripwire**

ftp://ftp.redhat.com/pub/redhat/linux/9/en/os/i386/RedHat/RPMS//tripwire-2.3.1-17.i386.rpm

Generate database: tripwire –init

Take backup of created database and policy file

Check against earlier database and generate report: tripwire –check > report.txt

## 8. Security Tools

### External Scanning

*Port scanning*

*Nmap <Ip\_address of the web server>*

In order to have remote connectivity to the web server install **SSH** to make the server more secure.

Check for the open ports by issuing the following commands from different machine

*nmap -sS -PO <ipaddress>*  
*netstat –tuan*

**Benchmarking Tools** : CISscan

**Automated security configure tool:** Bastile

## 9. References

www.cisecurity.com

www.redhat.com

www.securityfocus.com