Global Information Assurance Certification Paper

GCUX Practical Assignment (V2.0), Option a,

Securing Unix Step By Step : Hardening RedHat Linux for File Exchange Server

Yong Seok, Oh
June 9, 2004

Table of Contents

I. Abstract

This guide is for file exchange server of small business web site. This server offer secure file transfer, mail transfer only.

In this server system, Redhat Linux is installed. Redhat Linux is famous in open source operating system. Redhat linux is suitable for small business, so the Redhat linux was chosen.

In this server system,

- Openssh
- Tripwire
- Sendmail
- Syslog
- Iptables

are installed.

Openssh offer secure connection, secure file transfer between server and client system.
User can send mails by sendmail.
And administrator(or user of root account, or operators) can verify integrity of files by tripwire and check the logs of system.

In this guide,
Redhat Linux Installation process,
Installation & Customization several packages for Hardening OS
are described.

II. System Specification

A. Hardware Spec.

Server System Hardware Spec. :

CPU	
Main Memory	512MB

HDD	Matrox 40GB IDE x 2 EA
NIC	3Com 2 EA
SCSI Adapter	No
Monitor	LG FLATRON LCD 782TFT
Video Card	Riva TNT2
Sound Card	CMI8738/C3DX PCI
IP 1 IP 2	172.16.3.47 (Reserved)
Netmask	255.255.255.0
Keyboard	103 Keyboard
Mouse	Wheel Mouse (PS/2)
CD-ROM driver	LG 52X CD-ROM driver

Client System Hardware Spec. :

CPU	
Main Memory	512MB
HDD	Matrox 40GB IDE
NIC	3Com 1 EA
SCSI Adapter	No
Monitor	LG FLATRON LCD L1810B
Video Card	Matrox G459 DualHead
Sound Card	CMI8738/C3DX PCI
IP	172.16.3.46
Netmask	255.255.255.0
Keyboard	103 Keyboard
Mouse	Wheel Mouse (PS/2)
CD-ROM driver	LG 52X CD-ROM driver

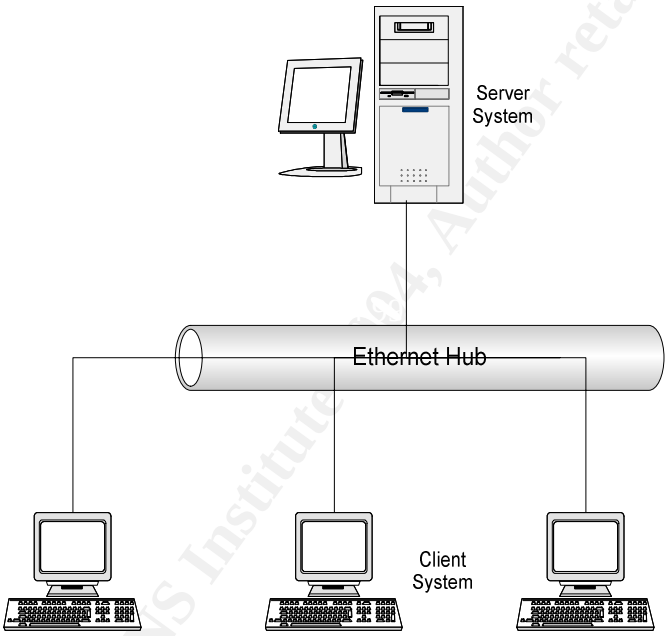
B. Software Spec.

Server System	OS	Redhat 9
	Application Program	OpenSSH
		Sendmail
		Syslog
		Tripwire (for Integrity Check)
		Iptables (for Firewall)

Client System1	OS	Hancom Linux 3.1 based on Redhat Linux (Kernel ver : 2.3.13 1hl)
Client System2	OS	Windows 2000 Server

C. Network Configuration

These server & client systems are located in an isolated network environment. However isolated network, they can be connected to Internet to download updated application version, patch files. Other computer is connected to same Ethernet hub, but I use only two machines(server, client) here.



D. Physical Security

Server system is more important than client system in Network. So, this server system use UPS, AVR to protect power failure.

And, server & client systems are located a lab that is controlled by Card Key.

E. Purpose of this system

This server system is file exchange system in small business website. To secure file exchange, this server is hardened to serve secure file exchange.

F. Risk mitigation

I needed a security policy; a kind of list of what I consider allowable and not allowable, upon which to base any decisions regarding security. The policy should also determine my response to security violations.
The answers to the following questions should provide some general guidelines:

- How do you classify confidential or sensitive information?

  After installation, /usr partitions should not change. -> Read-only partition of /usr partition

- Does the system contain confidential or sensitive information?

  Yes, file exchange server should not be modified, monitored during file exchanging. -> Use of SSH, Tripwire

- Exactly whom do you want to guard against?

  By use of SSH, file exchange server will be guarded from the snipper.

- Do remote users really need access to your system?

  Yes, but it could be only by ssh. -> SSH, Iptables

- Do passwords or encryption provide enough protection?

  No, needed more secure method. -> Remove the SUID, SGUID bits of programs.

- Do you need access to the Internet?

  Yes, it is. But it could be by only ssh.

To make risk mitigation, firstly check whether this system have some vulnerability. To check whether vulnerability is, investigate vulnerabilities of application program.

You can find Vulnerability of OS, Application(OpenSSH, Tripwire, IPtables, Sendmail) in below Web site :
http://www.cert.org/
http://www.kb.cert.org/vuls/byid?searchview
http://cve.mitre.org/
http://www.redhat.com
http://www.linuxsecurity.com/advisories/redhat.html

More detailed information is described in <Appendix A>.

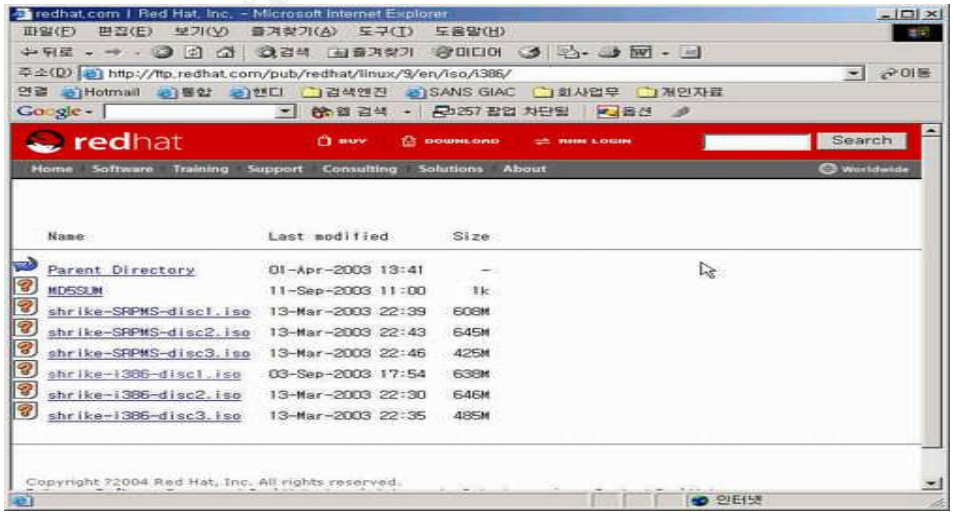
However applications and OS had been some vulnerabilities, Most vulnerability of that application, OS could be fixed by patching.
And, to adapt above security policy, I will patch application programs.

III. Installation of Redhat 9

A. Preparation

Download Redhat

Redhat 9 can be downloaded at http://ftp.redhat.com/pub/redhat/linux/9/en/iso/i386/



And make CD-ROM for installation.

Verify the S/W :
To confirm the integrity of files in web sites, Check the MD5 checksum that can be compared against an MD5 checksum computed during the download process.
To verify a package against its MD5 checksum, run the command:

md5sum package-name

B. Installation

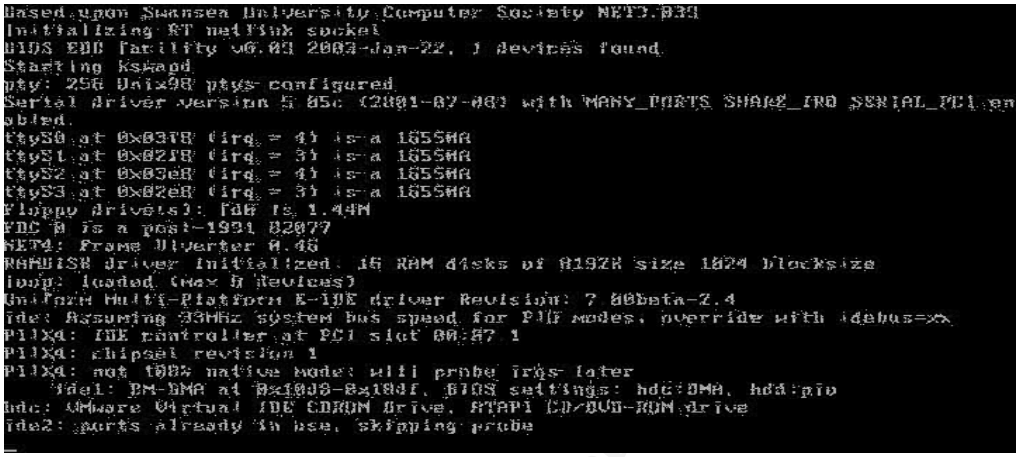
In installation guide of RedHat, a server installation requires 850MB for a minimal installation without X (the graphical environment), at least 1.5GB of free space if all package groups other than X are installed, and at least 5.0GB to install all packages including the GNOME and KDE desktop environments.

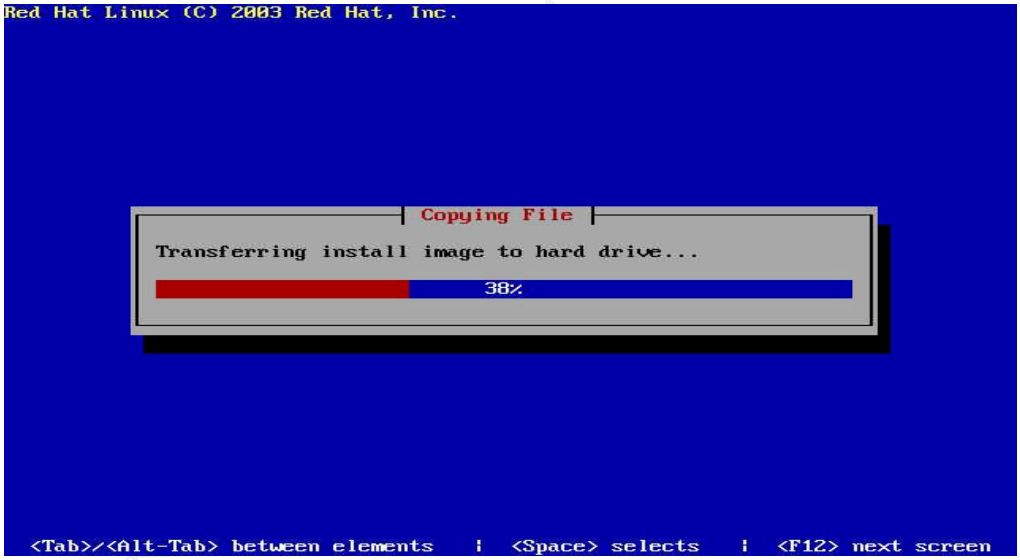
I will install Redhat linux for File Exchange & Mail Server, so this server system has to have at least 4.0GB of free space.

- Boot by CD-ROM

My server system have CD-ROM driver, so I booted Server system by CD-

ROM. At boot prompt,
Boot: *[Enter]*





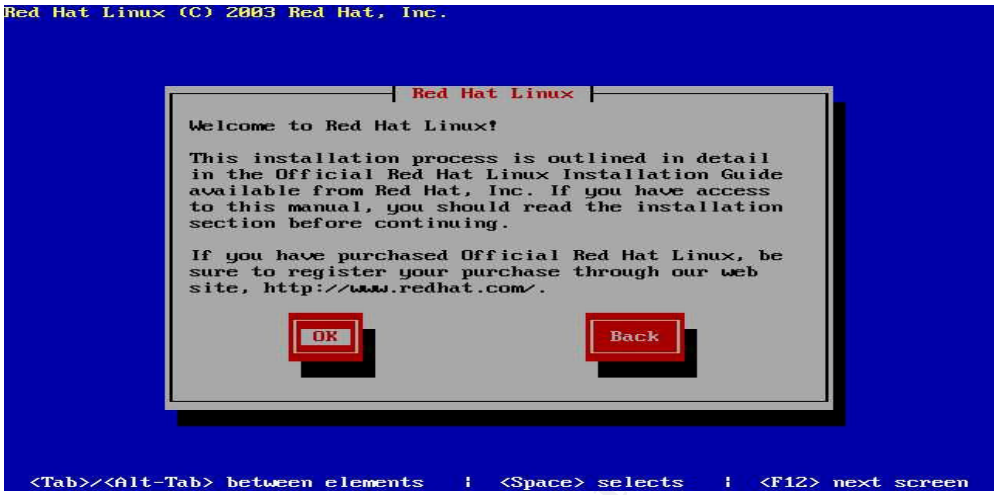
[CD Found] Message
Message box's contents :

To begin testing the CD media before installation press OK.
Choose Skeip to skip the media test and start the installation.

Choose 'Skip' button to skip the testing the CD media.

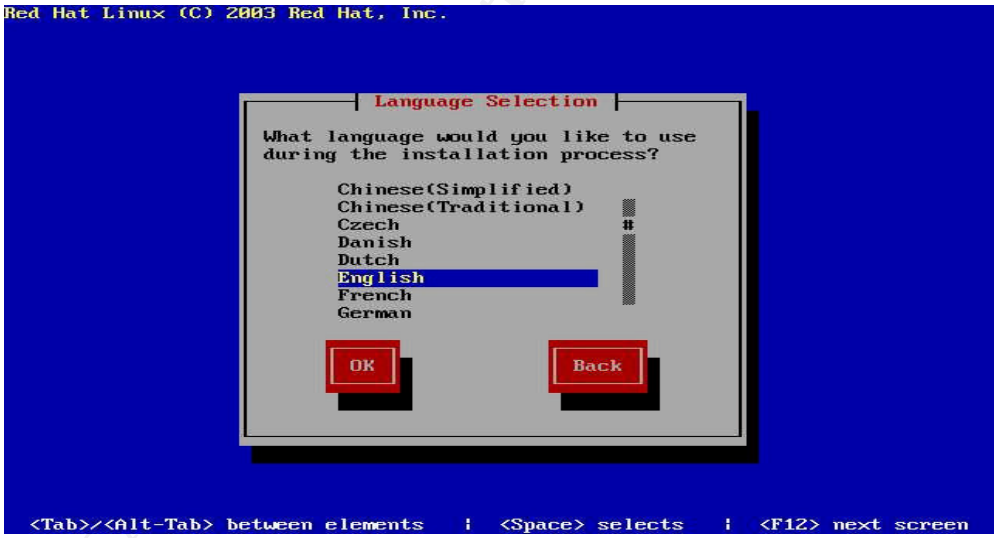
- Welcome to Red Hat Linux

Click on the Next button to continue.



- Language Selection

Select ‘English(English)’. And Next button.

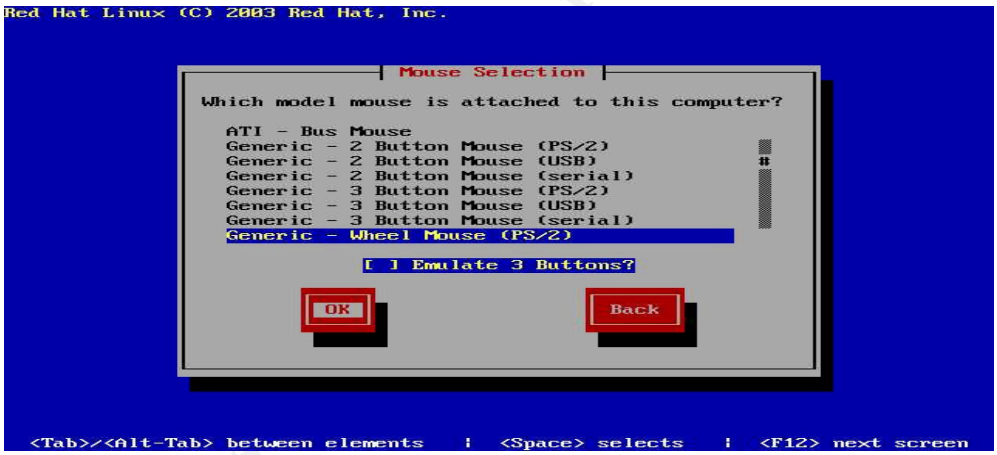


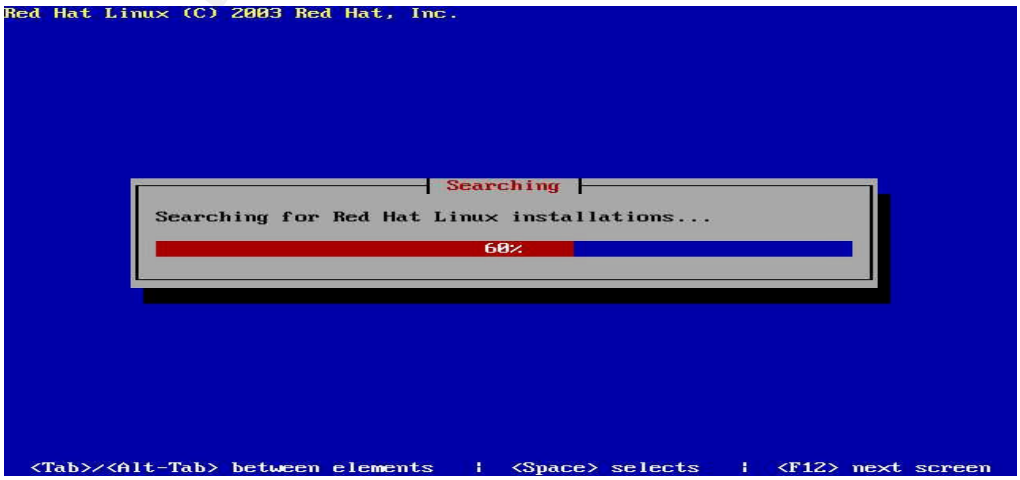
- Keyboard Configuration

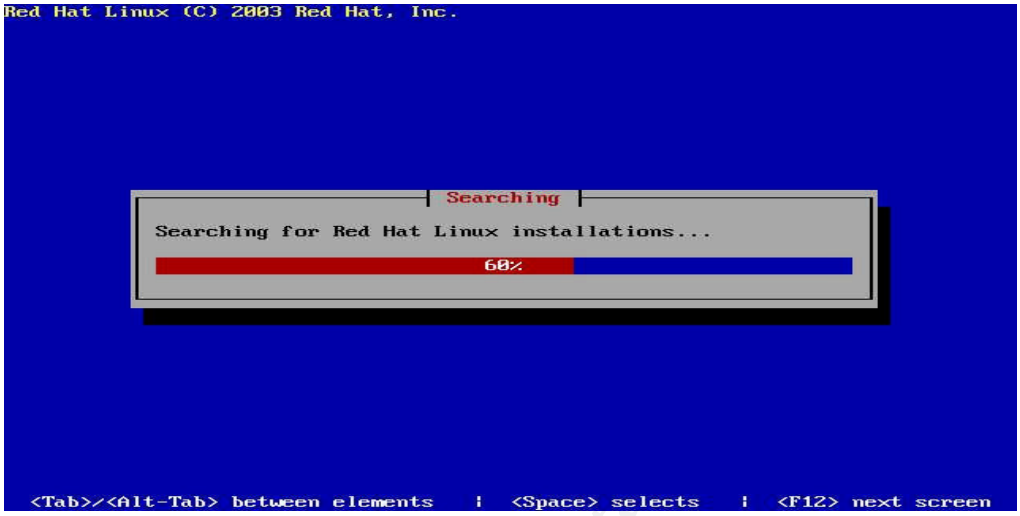
Select ‘U.S. English’. And Next button.

- Mouse Configuration

Select 'Wheel Mouse(PS/2)'. And Next button.

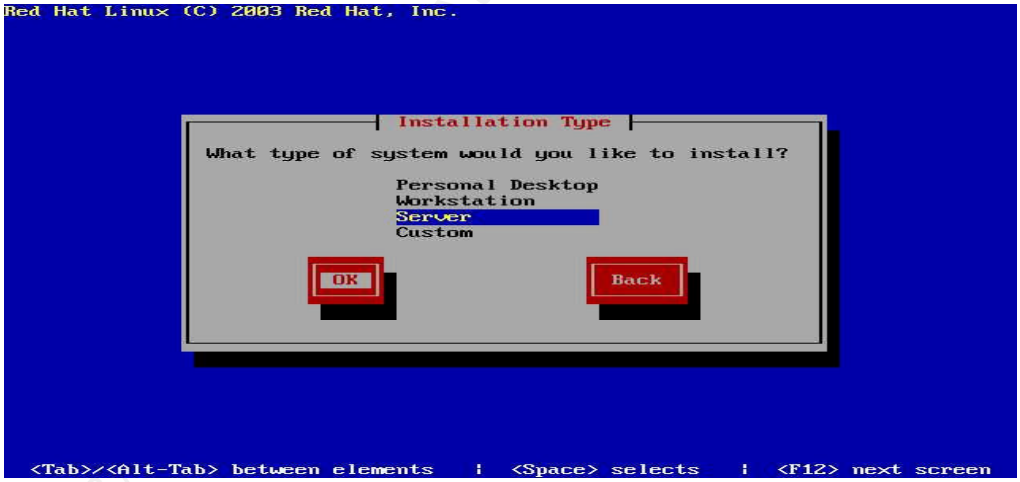






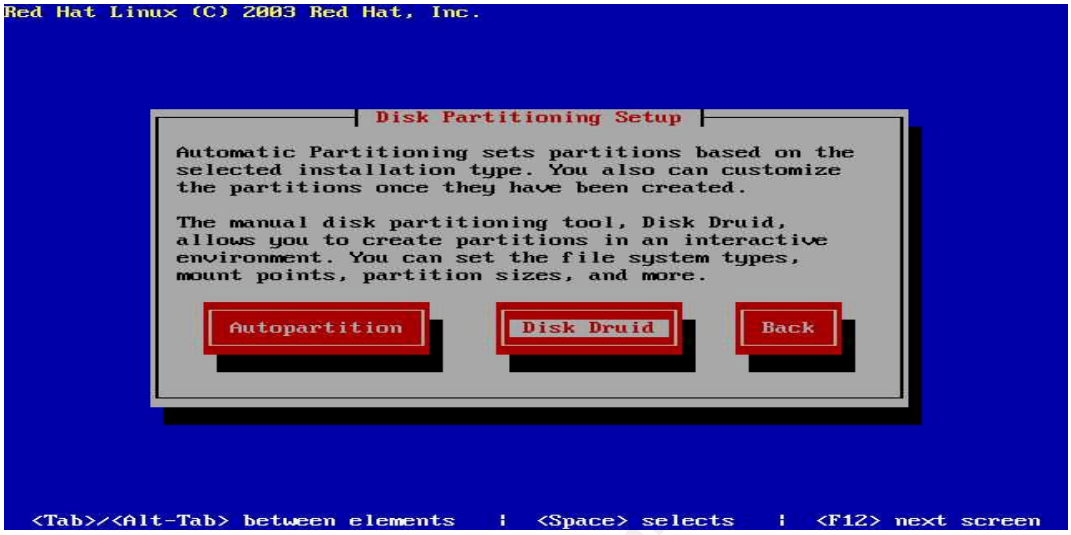
- Installation Type

I want to make this machine to test server and control over the installation process, disable useless packages. So Select ‘Server’. And Next button.



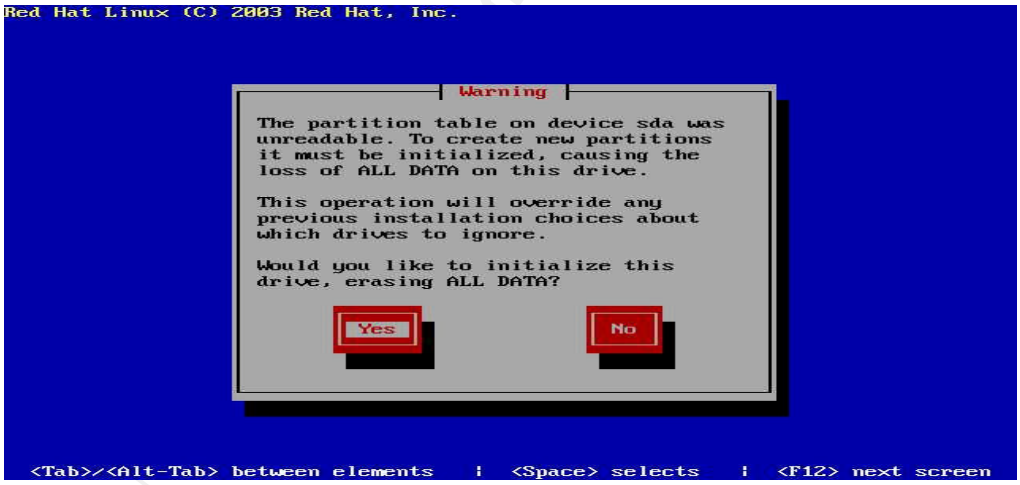
- Disk Partitioning Setup

Choose ‘Disk Druid’ and click the ‘Next’ button.

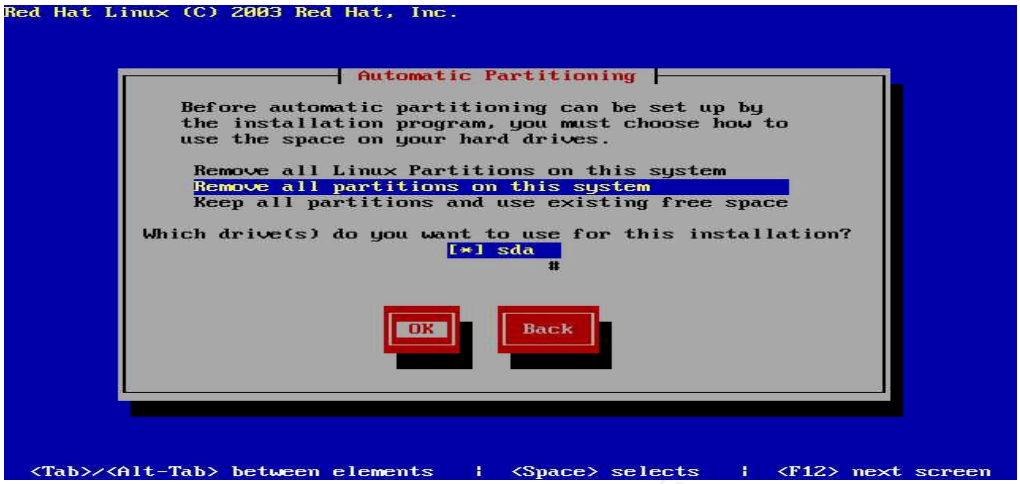


- Disk Druid

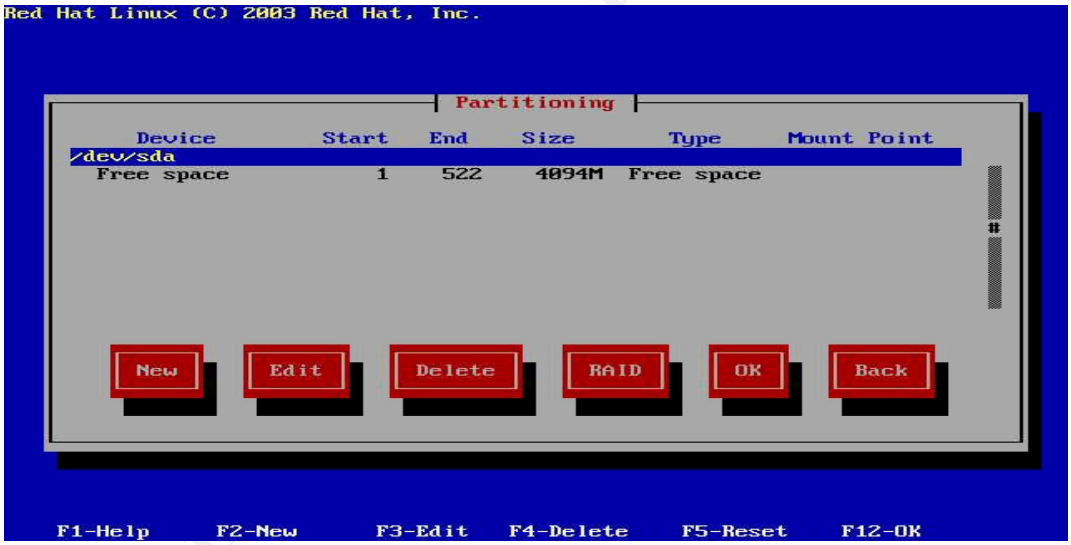
I want to remove all partitions on hard drive, so Select 'Remove all partitions on this system'. And I Clicked the 'Next' Button.

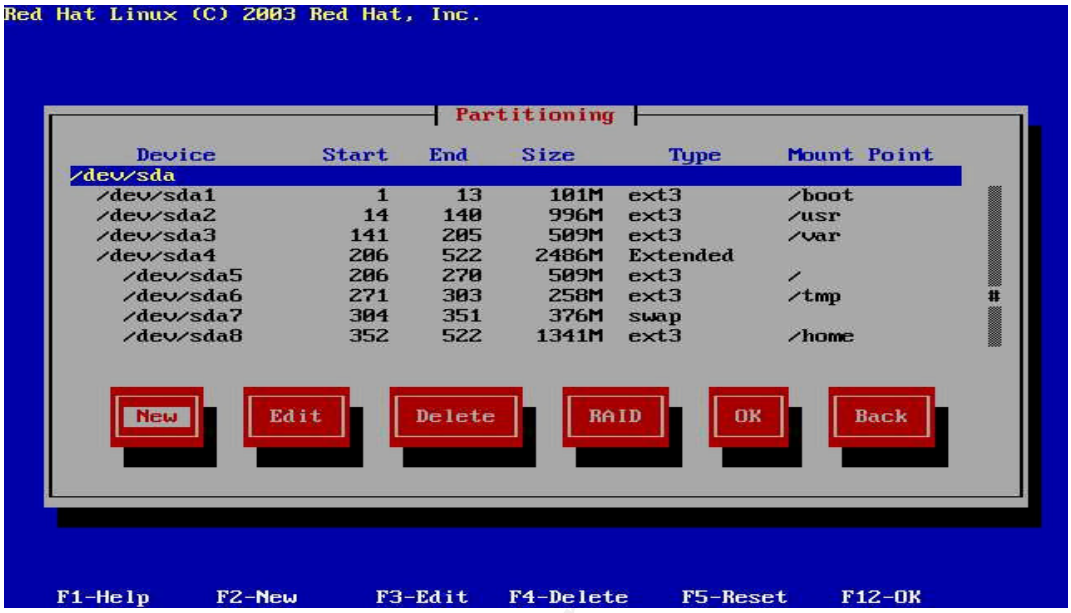


Then warning message box is shown, because selected 'remove all paritions'. Click the 'Yes' button.



I divided this system's HDD partition below:





/boot: Kernel images are kept here

/usr: All Linux binaries programs are installed here. So I allocated about 1GB.

/var: Contains files that change when the system run normally i.e. Log files

/ : root partition

/tmp: Temporary files partition

/home: Normal users' space

Because this server is file exchange server, I allocated a lots for /home. And these multiple partitions strategy enhances security and preventes accidental denial of service or exploit of SUID programs.

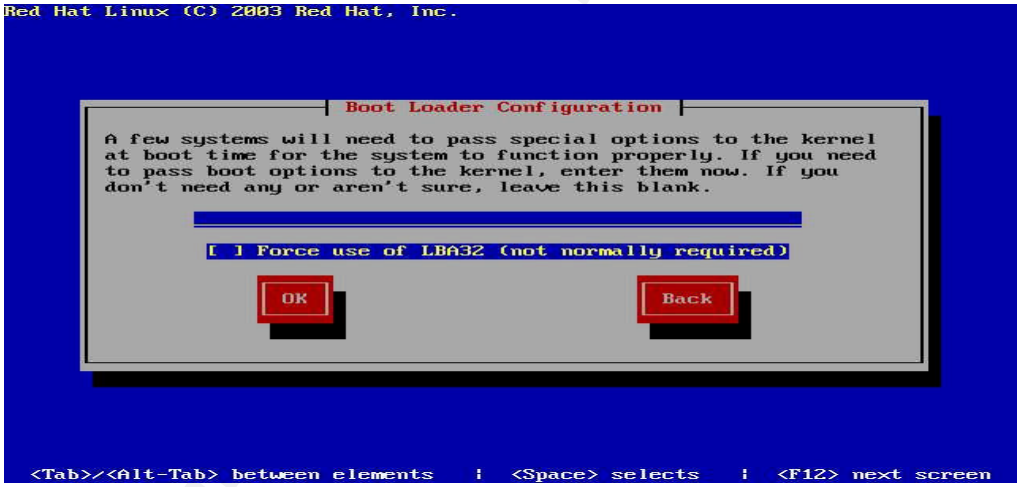
Creating multiple partitions offers the following advantages:

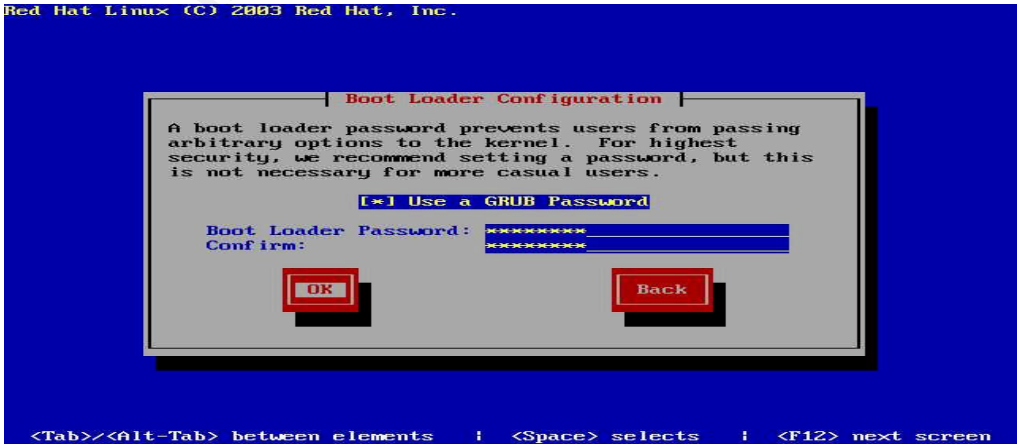
- Protection against denial of service attack
- Protection against SUID programs
- Faster booting
- Easy backup & upgrade management
- Ability for better control of mounted file system
- Limit each file system's ability to grow

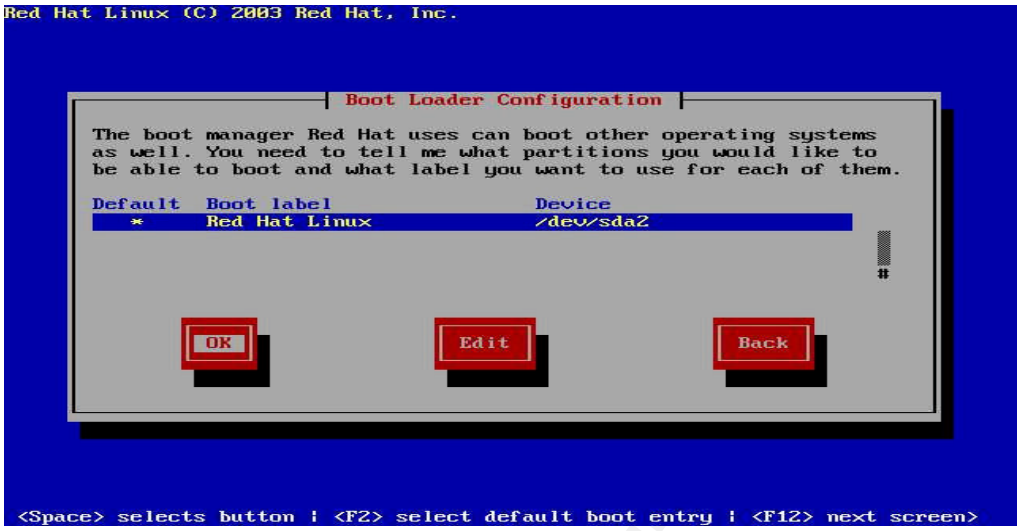
- Boot Loader Configuration

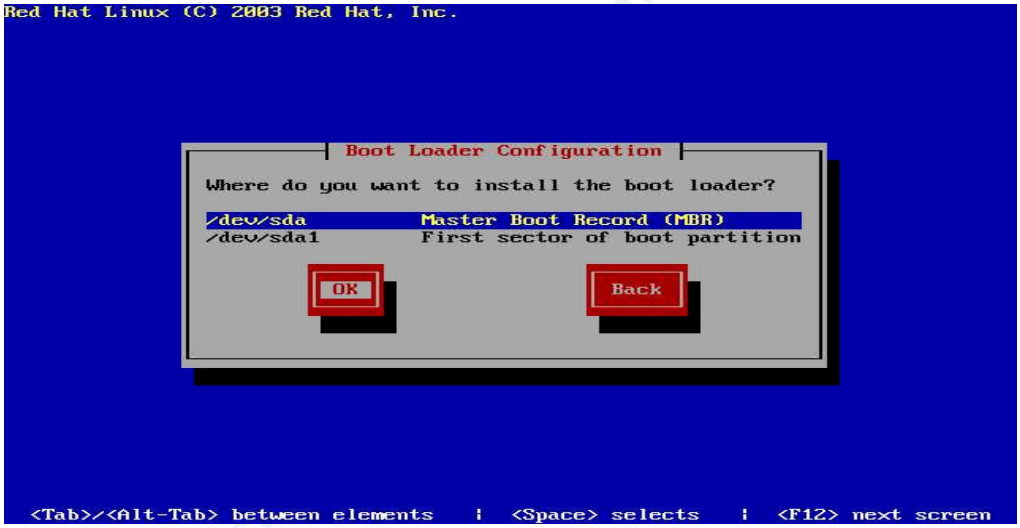
I want to boot by MBR in first HDD disk, I don't change any configuration of

Boot loader. Click ‘Next’ button.



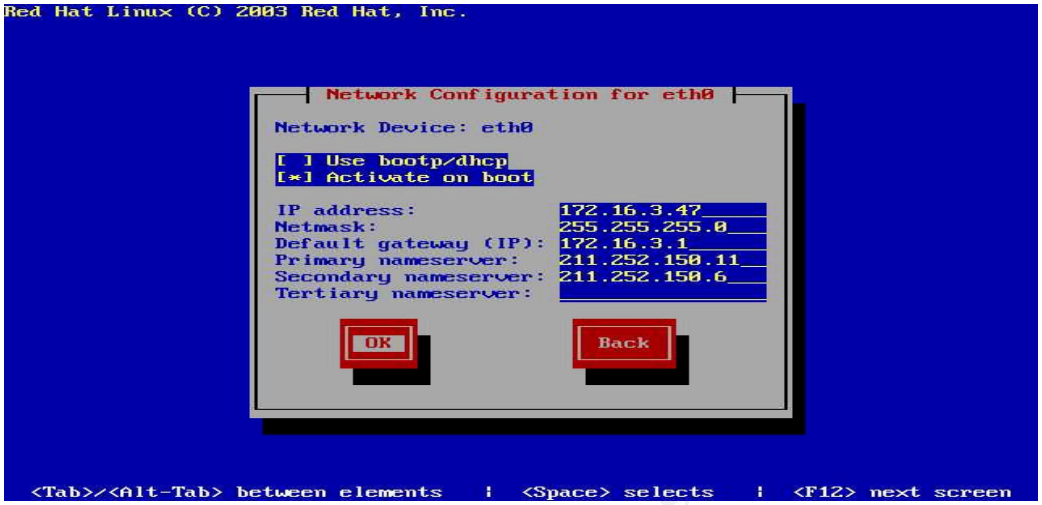






- Network Configuration

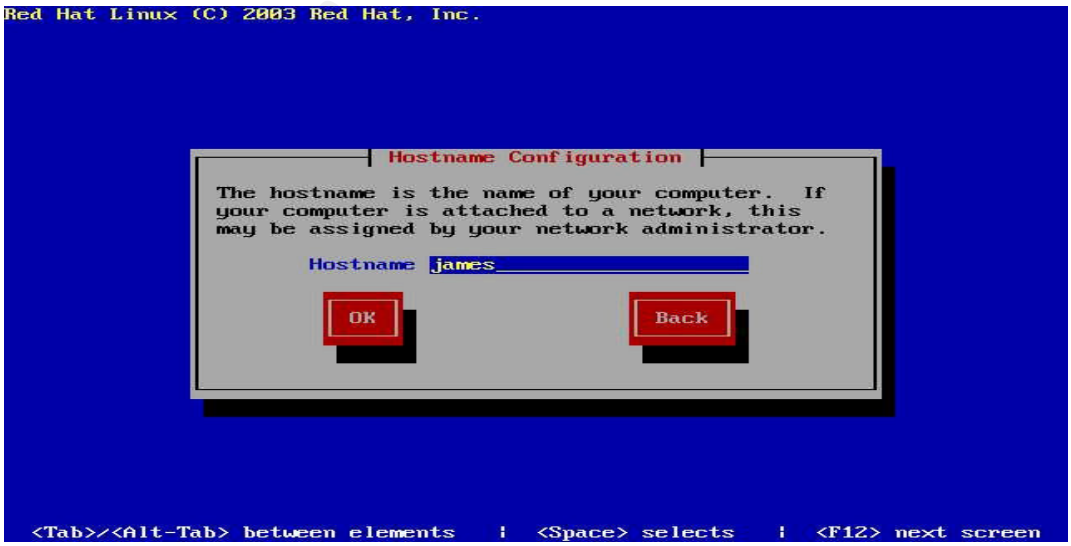
My network configuration is <Figure 1-1>, and my test server's network information is in <Table 1-1>. So I changed network configuration. I activated the interface information on boot. I named the hostname by 'GIAC'.



IP	172.16.3.47
Netmask	255.255.255.0 (C Class)
Gateway	172.16.3.1
Primary Name Server	210.211.150.11
Secondary Name Server	210.211.150.6

And I clicked 'Next' button.

- Hostname configuration



- Firewall Configuration

I will plan to make a secure server. So I need the most secure OS, I

selected ‘High’. Then ‘Next’ button.

For more detailed configuration of firewall, I pushed the ‘Customize’ button. Then I configured ‘Allow incoming’.

- Allow Incoming : Enabling these options allow the specified services to pass through the firewall.

I want to access incoming services by ssh. So I allowed ‘ssh’ service only.

Note) After installation, I can changed the firewall’s access control rules by iptables.

To activate the changes :

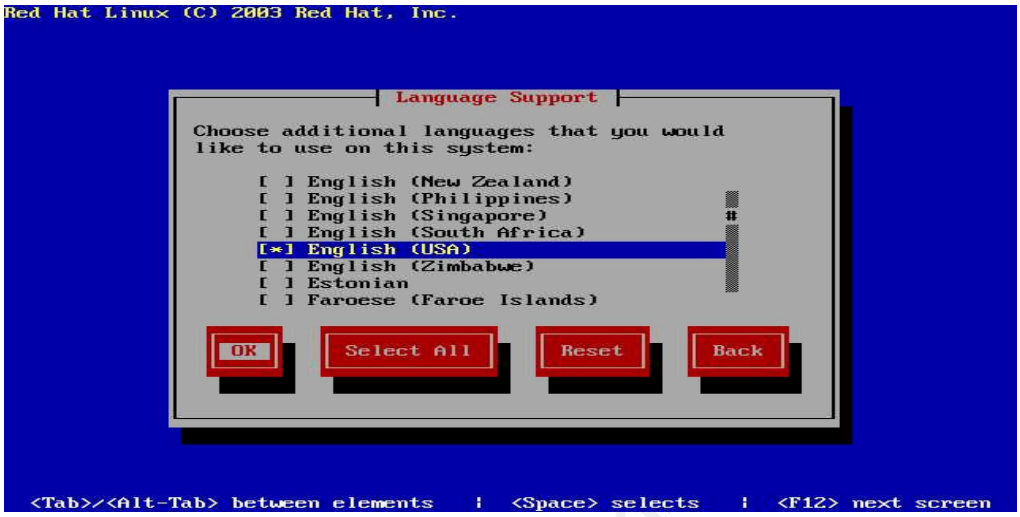
/sbin/service iptables restart

or

/sbin/chkconfig --level 345 iptables on

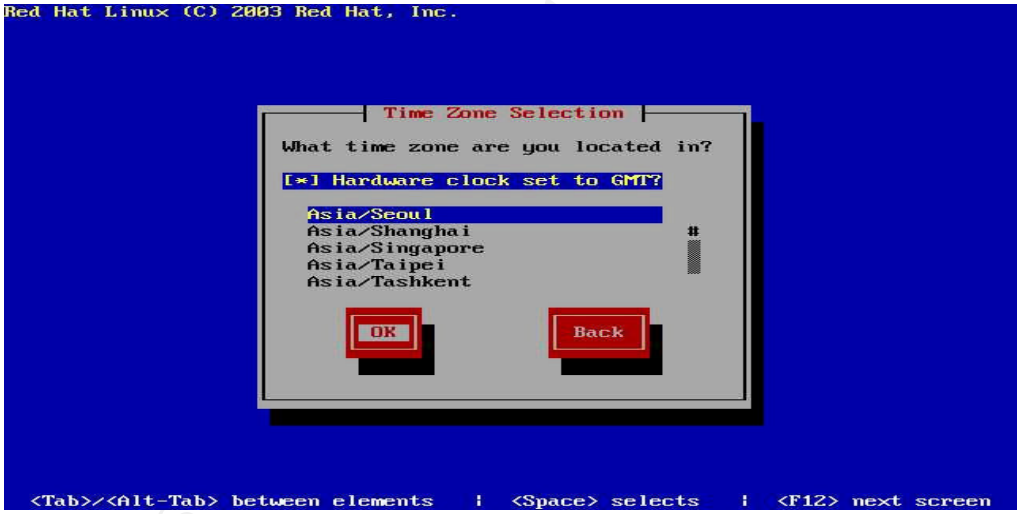
- Additional Language Support

I don’t want another additional language support, so I just click ‘Next’ Button.



Time Zone Selection

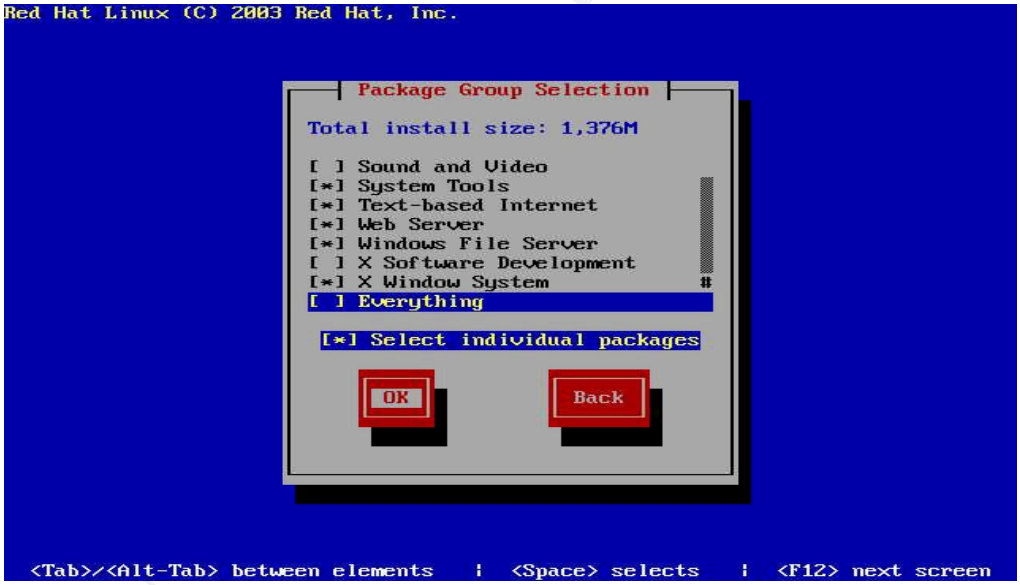
I live in Korea. So I changed location information by 'Asia/Seoul'.



- Set Root Password

I typed twice the root password. If the first password and second password are equal, 'Next' button will be activated. And I clicked the 'Next' button.

- Package Group Selection



I Selected the necessary Package Group for My server system like these:

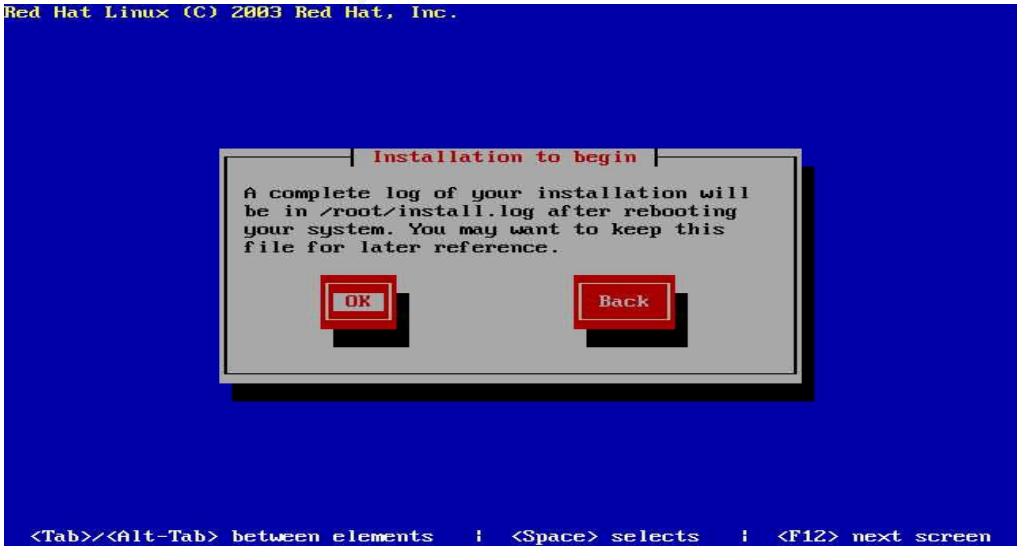
- Text-based internet : To access Internet
- Server configuration Tools : To configure system
- Mail Server : To serve mail server
- FTP Server : To serve of FTP
- Administation Tools : To administrate system
- System Tools : To administrate system
- Development Tools : To compile packages
- Kernel Development : To upgrade of kernel later

- Dependency Check

After selecting packages, Redhat installation process is to check dependency of selected packages.

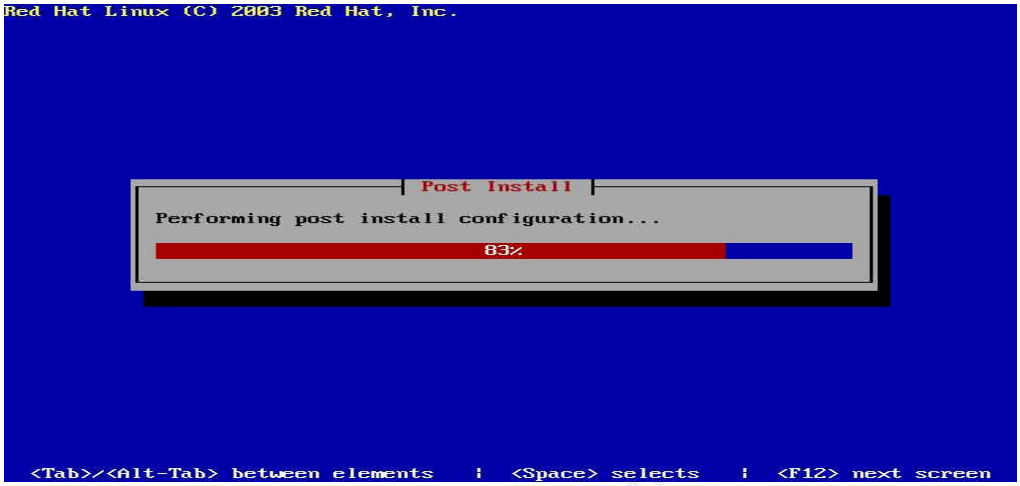
- Installation to begin

After install of Redhat, you can review the install log in /root/install.log.



And then selected packages would be installed.

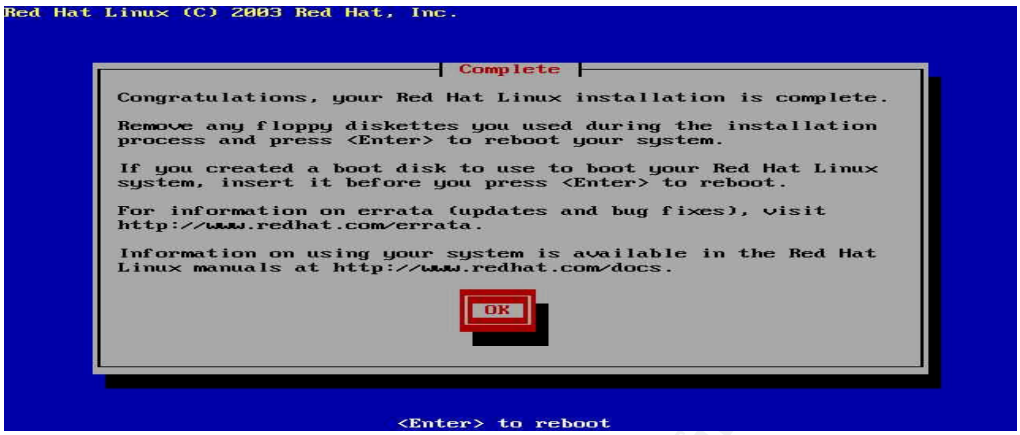
- Post Install

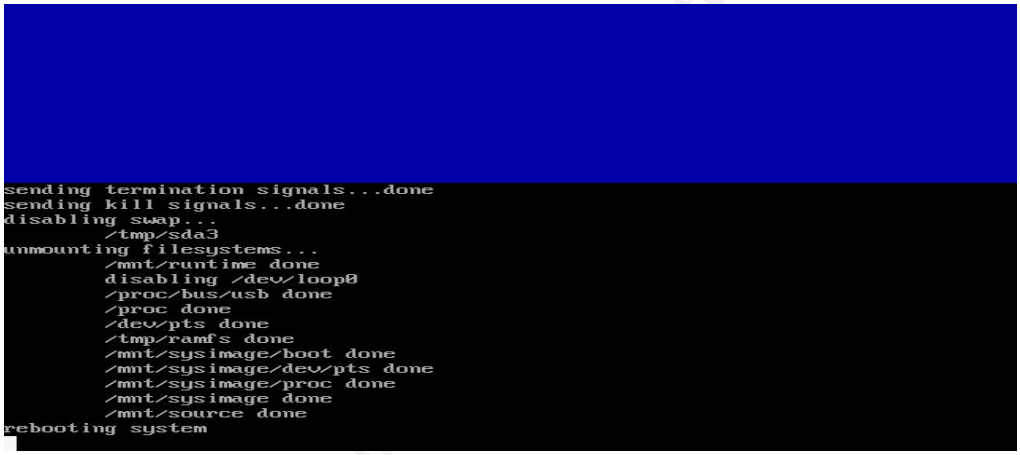


- Boot Diskette

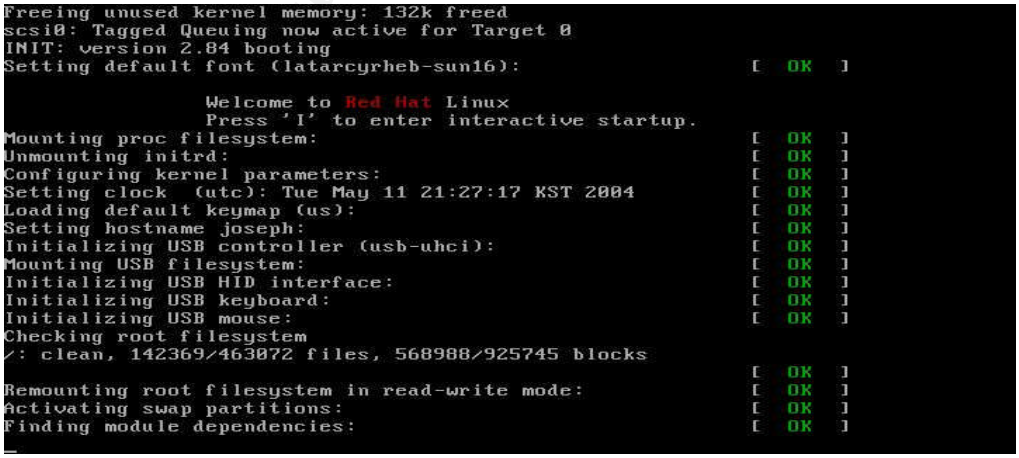
Boot diskette is required later. If boot record was corrupted, it could be recovered by this boot diskette. I made a boot diskette!

- Install Complete & Reboot





- Boot first



IV. Hardening the Redhat 9 installation

A. Preparation

However installation of Redhat 9 was over, OS does not safe. Redhat 9 was released at 2003.

Installation Patch, Check the latest version of Redhat

Install from Redhat Updates Site:

#wget ftp://updates.redhat.com/9/en/os/noarch/*.rpm
#wget ftp://updates.redhat.com/9/en/os/`uname -m`/*.rpm
#wget ftp://updates.redhat.com/9/en/os/i386/*.rpm

- Install Security and other patches regularly

I should check regularly security and other patches above site and the other sites in <Appendix A>.
I can be retrieved security updates
- Download from Red Hat Network
- Downloaded from the Red Hat Linux Errata website

When a security errata (or any type of errata) is released, Red Hat Network will send you an email with a description of the errata as well as which of your systems are affected.

B. Install the latest version of Application program

Application Program Name	The lastest version
OpenSSH	3.8 released Feb. 24, 2004
Sendmail	8.12.11 Jan. 18, 2004

In this server, two major services are openssh, sendmail.
You can get OpenSSH via openssh homepage (http://www.openssh.com/portable.html) and Sendmail via sendmail's homepae (http://www.sendmail.org/8.12.11.html).

But, Openssh package in Redhat 9 is not vulnerable to newest 'Openssh

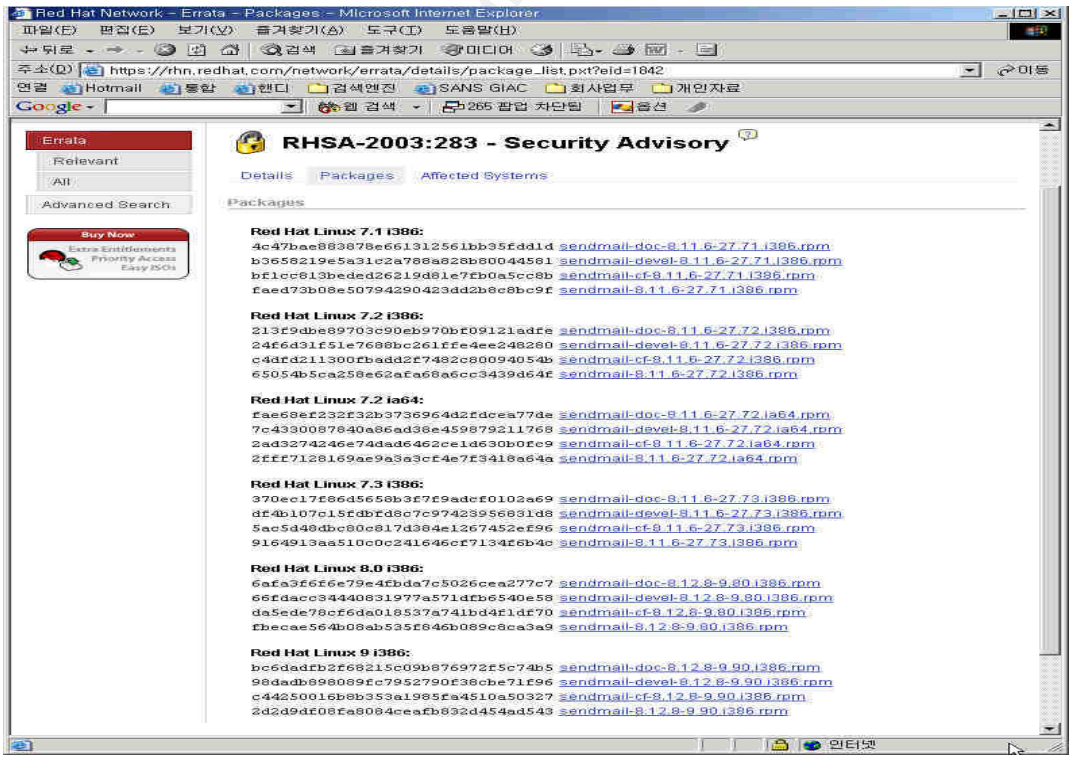
Security advisory'.(http://www.openssh.com/security.html)

OpenSSH 3.7.1 and newer are not vulnerable to "September 16, 2003: OpenSSH Buffer Management bug", OpenSSH Security Advisory and CERT Advisory CA-2003-24.

So, I don't need to the those newest package.

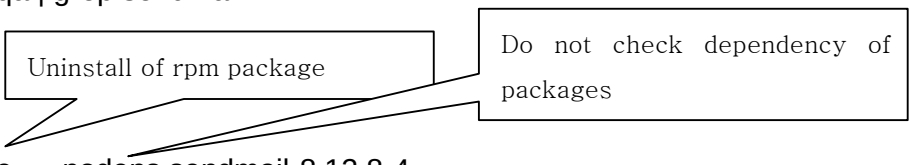
However, the openssh have not vulnerability yet, Sendmail in Redhat 9 have a vulnerability(http://www.cert.org/advisories/CA-2003-25.html, https://rhn.redhat.com/network/errata/details/index.pxt?eid=1842). Version of sendmail in Redhat 9 is 8.12.8. Above vulnerability is resolved in Sendmail 8.12.10.

I've downloaded the news version of sendmail in Redhat site at before step. (& I can download from Redhat Network : https://rhn.redhat.com/network/errata/details/package_list.pxt?eid=1842)



Before installation of the newest sendmail, I've uninstalled old-version sendmail.

rpm -qa | grep sendmail



rpm -e --nodeps sendmail-8.12.8-4
rpm -e sendmail-cf-8.12.8-4

rpm -Uvh sendmail-cf-8.12.8-9.90.i386.rpm
rpm -Uvh sendmail-8.12.8-9.90.i386.rpm

<Installation of sendmail packages>

```
Script started on Thu 03 Jun 2004 07:28:55 PM KST
[root@james packages]#
[root@james packages]# rpm -U_vh send_mail-8.12.8-9.90.i386.rpm
warning: sendmail-8.12.8-9.90.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...
(100%)_____#####################
######################### [100%]
    1:sendmail
( 99%)_____#####################
######################### [100%]
[root@james packages]#
[root@james packages]# rpm -Uvh sen_dmail-cf-8.12.8-9.90.i386.rpm
warning: sendmail-cf-8.12.8-9.90.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...
(100%)_____#####################
######################### [100%]
    1:sendmail-cf
( 99%)_____#####################
######################### [100%]
[root@james packages]#
[root@james packages]#
[root@james packages]# rpm -qa | grep sendmail
sendmail-cf-8.12.8-9.90
sendmail-8.12.8-9.90
[root@james packages]#
```

```
[root@james packages]#
[root@james packages]#
Script done on Thu 03 Jun 2004 07:29:34 PM KST
```

To apply new sendmail daemon, restart sendmail daemon.
#/etc/rc.d/init.d/sendmail restart

C. Shut down un-needed application

The chkconfig command can also be used to activate and deactivate services.
<Before Non-necessary services are deactivated>

```
Script started on Thu 03 Jun 2004 07:35:05 PM KST
[root@james root]#
[root@james root]# chkconfig
chkconfig version 1.3.8 - Copyright (C) 1997-2000 Red Hat, Inc.
This may be freely redistributed under the terms of the GNU Public License.

usage:    chkconfig --list [name]
          chkconfig --add <name>
          chkconfig --del <name>
          chkconfig [--level <levels>] <name> <on|off|reset>)
[root@james root]#
[root@james root]# chkconfig --list
kudzu           0:off   1:off   2:off   3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
random          0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices      0:off   1:off   2:off   3:on    4:on    5:on    6:off
pcmcia          0:off   1:off   2:on    3:on    4:on    5:on    6:off
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
keytable        0:off   1:on    2:on    3:on    4:on    5:on    6:off
apmd                    0:off   1:off   2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
gpm             0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
irda	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
isdn	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
portmap	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
nfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
nfslock	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
httpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
winbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
smb	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
xfs	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
xinetd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
named		0:off	1:off	2:off	3:off	4:off	5:off	6:off
ntpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
snmpd		0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmptrapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
vsftpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
xinetd based services:								
chargen-udp:	off							
rsync:	off							
chargen:	off							
daytime-udp:	off							
daytime:	off							
echo-udp:	off							
echo:	off							
services:	off							
servers:	off							
time-udp:	off							
time:	off							
sgi_fam:	on							
imap:	off							

```
        imaps:    off
        ipop2:    off
        ipop3:    off
        pop3s:    off
[root@james root]#
[root@james root]#
[root@james root]#
Script done on Thu 03 Jun 2004 07:35:39 PM KST
```

In text mode, this system's runlevel is 3. (Confirm by 'runlevel' command)

```
#runlevel
N 3
```

You can get more information of runlevel at /etc/inittab.

This system is operating in runlevel 3. So, I would deactivate unnecessary services at runlevel 3.

Now activating services are :

- kudzu
- syslog
- netfs
- network
- random
- rawdevices
- pcmcia
- keytable
- apmd
- atd
- gpm
- autofs
- iptables
- isdn
- sshd
- portmap
- nfslock

- sendmail
- rhnsd
- crond
- anacron
- xfs
- xinetd

This system does not use X-Windows GUI. So, I would deactivate xfs (X font server) service. And portmap is a server that converts RPC program numbers into DARPA protocol port numbers.

<After Non-necessary services are deactivated>

```
Script started on Thu 03 Jun 2004 08:06:42 PM KST
[root@james root]#
[root@james root]# /sbin/chkconfig --level 2345 xfs off
[root@james root]#
[root@james root]# /sbin/chkconfig --level 345 portmap off
[root@james root]#
[root@james root]#
[root@james root]# chkconfig --list
kudzu           0:off   1:off   2:off   3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
random          0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices      0:off   1:off   2:off   3:on    4:on    5:on    6:off
pcmcia          0:off   1:off   2:on    3:on    4:on    5:on    6:off
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
keytable        0:off   1:on    2:on    3:on    4:on    5:on    6:off
apmd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
gpm             0:off   1:off   2:on    3:on    4:on    5:on    6:off
autofs          0:off   1:off   2:off   3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
irda            0:off   1:off   2:off   3:off   4:off   5:off   6:off
isdn            0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
portmap	0:off	1:off	2:off	3:off	4:off	5:off	6:off
nfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off
nfslock	0:off	1:off	2:off	3:on	4:on	5:on	6:off
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off
rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off
httpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
winbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off
smb	0:off	1:off	2:off	3:off	4:off	5:off	6:off
xfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off
xinetd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
named	0:off	1:off	2:off	3:off	4:off	5:off	6:off
ntpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmptrapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
vsftpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off

xinetd based services:

chargen-udp: off
rsync: off
chargen: off
daytime-udp: off
daytime: off
echo-udp: off
echo: off
services: off
servers: off
time-udp: off
time: off
sgi_fam: on
imap: off
imaps: off
ipop2: off
ipop3: off
pop3s: off

```
[root@james root]#
[root@james root]#
[root@james root]#
Script done on Thu 03 Jun 2004 08:07:41 PM KST
```

ntsysv

The ntsysv utility provides a simple interface for activating or deactivating services, too.

D. Configure network security

Review the current network security settings:

```
# cd /proc/sys/net/ipv4
# cat ip_forward
0
```

: This means that ip forward is not allowed.

To increase overall network security, edit /etc/sysctl.conf

<Original content of /etc/sysctl.conf file>

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.
```

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 0

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
```

<Changed file of /etc/sysctl.conf>

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
# Disable IP Forwarding
net.ipv4.ip_forward = 0

# Disables IP Source Routing
net.ipv4.conf.all.accept_source_route = 0

# Enables SYN flood protection
net.ipv4.tcp_max_syn_backlog = 4096

# Enables TCP SYNC Flood protection
net.ipv4.tcp_syncookies = 1

# Disables the ability to send ICMP Redirect
net.ipv4.conf.all.send_redirects = 0
```

```
# Disables ICMP Redirect acceptance
net.ipv4.conf.all.accept_redirects = 0

# Another parameter that disables ICMP Redirect acceptance
net.ipv4.conf.default.accept_redirects = 0

# Controls source route verification
# Enables IP Spoofing protection
net.ipv4.conf.default.rp_filter = 1

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
```

After change the file, change the file access permission

```
# chown root:root /etc/sysctl.conf
# chmod 0600 /etc/sysctl.conf
```

And apply the changes by restart network service

```
# /etc/rc.d/init.d/network restart
```

E. Configure TCPWrapper to control authentication to SSH

Access will be granted when a match is found in /etc/hosts.allow, otherwise access will be denied when a match is found in /etc/hosts.deny, finally if no matches is found access will be granted.

On this server we use only /etc/hosts.allow in which hosts that are allowed to this system are listed, followed by a global deny statement.

```
[root@james root] # cat /etc/host.deny
cat: /etc/host.deny: No such file or directory
[root@james root] # cat /etc/host.allow
```

```
cat: /etc/host.allow: No such file or directory
[root@james root] # rpm -qa | grep wrapper
tcp_wrappers-7.6-34
[root@james root] # touch /etc/host.deny
[root@james root] # touch /etc/host.allow
[root@james root] # vi /etc/host.deny
[root@james root] # vi /etc/host.allow
[root@james root] # cat /etc/host.deny
ALL : ALL :
[root@james root] # cat /etc/host.allow
ssh : 172.16.3.46 : allow
```

Sending client connections to a service an intimidating banner is a good way to disguise what system the server is running while letting a potential attacker know that system administrator is vigilant.

For ssh, add the following line to the /etc/hosts.allow file

```
sshd : ALL : banners /etc/banners
```

And do the below commands

```
# mkdir /etc/banners
# touch /etc/banners/sshd
& type the banner contents
```

```
220-Hello, %c
220-All activity on james.testserver.or.kr is logged.
220-Act up and you will be banned.
```

%c token supplies a variety of client information, such as the username and hostname, or the username and IP address to make the connection even more intimidating.

To control access to Internet services, use xinetd, which is a secure replacement for inetd. The xinetd daemon conserves system resources, provides access control and logging, and can be used to start special-purpose servers. xinetd can be used to provide access only to particular

hosts, to deny access to particular hosts, to provide access to a service at certain times, to limit the rate of incoming connections and/or the load created by connections, and more xinetd runs constantly and listens on all of the ports for the services it manages.

The configuration file for xinetd is /etc/xinetd.conf, but the file only contains a few defaults and an instruction to include the /etc/xinetd.d directory. To enable or disable an xinetd service, edit its configuration file in the /etc/xinetd.d directory. If the disable attribute is set to yes, the service is disabled. If the disable attribute is set to no, the service is enabled. You can edit any of the xinetd configuration files or change its enabled status using the ntsysv, or chkconfig.

```
# ls /etc/x*
/etc/xinetd.conf

/etc/xinetd.d :
chargen    daytime-udp  imap    ipop3    servers    time
chargen-udp  echo       imaps   pop3s    services   time-udp
daytime    echo-udp     ipop2   rsync    sgi_fam
```

Except sgi_fam, All services was disabled. (You can check the state by chkconfig command: chkconfig --list)
sgi_fam is services that file alteration monitor. This server system doesn't need the ervices.
So, I add "disable = yes" to /etc/xinetd.d/sgi_fam file. And restart the xinetd server by "/etc/rc.d/init.d/xinetd restart".

```
[root@james xinetd.d]# chkconfig --list
kudzu           0:off   1:off   2:off   3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
random          0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices      0:off   1:off   2:off   3:on    4:on    5:on    6:off
pcmcia          0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

saslauthd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
keytable	0:off	1:on	2:on	3:on	4:on	5:on	6:off	
apmd		0:off	1:off	2:on	3:on	4:on	5:on	6:off
atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
gpm	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
irda	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
isdn	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
sshd	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
portmap	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
nfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
nfslock	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off	
httpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
winbind	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
smb	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
xfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
xinetd	0:off	1:off	2:off	3:on	4:on	5:on	6:off	
named		0:off	1:off	2:off	3:off	4:off	5:off	6:off
ntpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
snmpd		0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmptrapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
vsftpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off	
xinetd based services:								
chargen-udp:	off							
rsync:	off							
chargen:	off							
daytime-udp:	off							
daytime:	off							
echo-udp:	off							
echo:	off							
services:	off							

```
        servers:  off
        time-udp:       off
        time:     off
        sgi_fam:        off
        imap:     off
        imaps:    off
        ipop2:    off
        ipop3:    off
        pop3s:    off
[root@james xinetd.d]#
```

F. Secure Console & Root Account

I. Disable network root login

Under normal operating environment, there are no need to remote login in by 'root'. So edit /etc/securetty to reflect disabling network root login.

Edit like this file:

```
[root@james root]# cat /etc/securetty
tty1
tty2
tty3
tty4
tty5
tty6
[root@james root]#
```

Other than logging in from the local console, the only other way of logging into this system is remotely via ssh.

To disable network root login via ssh add 'PermitRootLogin no" to sshd_config and restart sshd.

II. Restrict root login from local console

Require root password when entering "Single User Mode"

Linux provides a “Single User Mode” to perform system maintenance. By default Linux does not require root password to log into single user mode.
To do this, add “~~:S:wait:/sbin/sulogin” to /etc/inittab
Then run ‘/sbin/init q’ to activate the change.

III. Restrict a usage of ‘ctrl+alt+del’

If you type ‘ctrl+alt+del’ simultaneously, linux system would be rebooted. Occasional reboot make non-synchronized file system in memory and HDD. So ‘ctrl+alt+del’ keys would like to be disabled.

- 1st method : This can be that like this, you should change a line to a comment : (in /etc/inittab)

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
->
# ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

- 2nd method : Add a -a option like below. The -a flag tells shutdown to look for the /etc/shutdown.allow file. You can restrict any users who are allowed to shutdown the system using [Ctrl]+[Alt]+[Del].

In /etc/inittabl

```
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
```

In /etc/shutdown.allow

```
james
root
```

I chose the 1st method.

IV. Disabling console program access

If you want to disallow any user at the console to run powerofff, halt, reboot, run the following commands.

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

V. Remove unnecessary system accounts

Some user accounts and groups are not needed for this server to do. It’s

best to keep the /etc/passwd file as small as possible so it's easier to detect unauthorized additions like these:
uucp, operator, games, mail, news, ftp, gopher

</etc/passwd>

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
```

To determine if a user is active or needs access to a shell, run the following command:

find / -user username -print

And verify that no accounts in /etc/passwd have an empty passwd.

I've deleted :
gopher, adm, pcap, rpc, rpcuser , nfsnobody
games, news, uucp, apache, xfs, named, ntp

And I've deleted group id:
news, uucp, adm, games, dip

Above procedure is like these:

Copy original 'passwd, shadow, group' file

Delete users 'gopher, pcap, …, ntp, adm'

```
[root@james root]#
[root@james root]# for file in /etc/{passwd,shadow,group} ; do /bin/cp -p $file
$file.orig ; done
[root@james root]#
[root@james root]# for user in gopher pcap rpc rpcuser nfsnobody games news uucp
 apache xfs named ntp adm ; do /usr/sbin/userdel $user ; done
[root@james root]#
[root@james root]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
```

```
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
[root@james root]#
[root@james root]# for group in news uucp adm games dip; do /sbin/groupdel $group ; done
[root@james root]#
[root@james root]# cat /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
man:x:15:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
rpm:x:37:
floppy:x:19:
vcsa:x:69:
utmp:x:22:
nscd:x:28:
slocate:x:21:
sshd:x:74:
mailnull:x:47:
smmsp:x:51:
[root@james root]# pwck
[root@james root]#
[root@james root]# grpck
 [root@james root]#
```

Delete groups 'news, uucp, adm, games, dip'

Check the integrity of password file

Check the integrity of group file

```
[root@james root]# find / -nouser -exec /bin/chown root {} \;
[root@james root]#
[root@james root]#
[root@james root]# find / -nouser -exec /bin/chgrp root [] \;
[root@james root]#
```

Change owner of the files those owner is deleted

VI. Change default umask

Default mask for the root user should not result in creation of group and world readable files and directories.

Change the files /etc/bashrc, /etc/csh.cshrc

umask 022 → umask 077

umask 002 → umask 007

VII. Password aging

Normal Users may be forgotten that they should change their password. So this system make the normal users should change their password by systemic method.

Change the following lines in the /etc/login.defs

PASS_MAX_DAYS 99999 -> PASS_MAX_DAYS 200

PASS_MIN_DAYS 0 -> PASS_MIN_DAYS 3

PASS_MIN_LEN 5 -> PASS_MIN_LEN 6

<Old file of /etc/login.defs>

```
# *REQUIRED*
#     Directory where mailboxes reside, _or_ name of file, relative to the
#     home directory.   If you _do_ define both, MAIL_DIR takes precedence.
#     QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail


# Password aging controls:
#
#       PASS_MAX_DAYS       Maximum number of days a password may be used.
#       PASS_MIN_DAYS       Minimum number of days allowed between password
```

```
changes.
#       PASS_MIN_LEN  Minimum acceptable password length.
#       PASS_WARN_AGE         Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN 5
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                  500
UID_MAX                60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                  500
GID_MAX                60000

#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD    /usr/sbin/userdel_local

#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is ORed with the -m flag on
# useradd command line.
#
CREATE_HOME yes
```

<Changed file of /etc/login.defs>

```
# *REQUIRED*
#     Directory where mailboxes reside, _or_ name of file, relative to the
#     home directory.    If you _do_ define both, MAIL_DIR takes precedence.
#     QMAIL_DIR is for Qmail
#
#QMAIL_DIR       Maildir
MAIL_DIR         /var/spool/mail
#MAIL_FILE       .mail

# Password aging controls:
#
#           PASS_MAX_DAYS       Maximum number of days a password may be used.
#           PASS_MIN_DAYS       Minimum number of days allowed between password
changes.
#           PASS_MIN_LEN  Minimum acceptable password length.
#           PASS_WARN_AGE       Number of days warning given before a password expires.
#
PASS_MAX_DAYS       200
PASS_MIN_DAYS       3
PASS_MIN_LEN  6
PASS_WARN_AGE       7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                 500
UID_MAX                60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                 500
GID_MAX                60000

#
# If defined, this command is run when removing a user.
```

```
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD            /usr/sbin/userdel_local


#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is ORed with the -m flag on
# useradd command line.
#
CREATE_HOME yes
```

PASS_MAX_DAYS is Maximum number of days a password may be used.
PASS_MIN_DAYS is Minimum number of days allowed between password changes.
PASS_MIN_LEN is Minimum acceptable password length.

Shorter the days that a password may be used, More confidence to the system. And more long password, more secure.

VIII. Secure Cron and at services

Linux allows users to schedule jobs to be run at a regular basis(cron), or once at a specific time. By default, any user can run both cron and at jobs.
For prevention of incidents like Dos(Denial of Service), we can control by /etc/cron.allow and /etc/cron.deny

/etc/cron.allow, /etc/at.allow : contained the users who are allowed to use cron or at.
/etc/cron.deny, /etc/at.deny : contained the users who are denied to use cron or at.
I restricted the user to use cron or at by only root.
- Remove /etc/cron.deny
- /etc/cron.allow contain only root

<Content of /etc/cron.allow>

```
root
```

IX. Create a system Banner

System banner may become useful if a civil or criminal prosecution will be pursued if a hacker breaks into this server.

System banner is in the /etc/issue file.
Write a warning message to hostile user like this :

```
This server is for evaluation of IT product.
Your action is logging.
This server is for authorized use only.
```

/etc/motd, /etc/issue, /etc/issue.net files are used for warning banner.
/etc/motd - Display banner to user has successfully logged into the server system.
/etc/issue - Display to any user that is logging into the system locally.
/etc/issue.net - Display to any users logging in remotely.

So above warning message should be into those files. Edit /etc/motd, /etc/issue, /etc/issue.net.

X. Find and evaluate set-uid / set-gid root programs

To find files that have the set-UID permission.
find / -perm -4000 –user root –print

```
Script started on Fri 04 Jun 2004 04:39:14 PM KST
[root@james root]# find / -type f \( -perm -04000 -o -perm -02000 \) -ls
 32298    36 -rwsr-xr-x    1 root     root        35376 Feb 13   2003 /usr/bin/chage
 32300    36 -rwsr-xr-x    1 root     root        36216 Feb 13   2003 /usr/bin/gpasswd
 32427     8 -r-xr-sr-x    1 root     tty          6908 Feb 11   2003 /usr/bin/wall
 32430    16 -rws--x--x    1 root     root        14140 Feb 25   2003 /usr/bin/chfn
 32431    12 -rws--x--x    1 root     root        11644 Feb 25   2003 /usr/bin/chsh
```

```
 32450      8 -rws--x--x     1 root       root            4728 Feb 25    2003 /usr/bin/newgrp
 32461     44 -rwxr-sr-x     1 root       tty            43593 Feb 25    2003 /usr/bin/write
 32468     16 -r-s--x--x     1 root       root           16336 Feb 14    2003 /usr/bin/passwd
 32499     40 -rwsr-xr-x     1 root       root           37284 Jan 25    2003 /usr/bin/at
 32694     16 -rwxr-sr-x     1 root       mail           12752 Jan 25    2003 /usr/bin/lockfile
 32711     16 -rwsr-xr-x     1 root       root           15324 Jan 25    2003 /usr/bin/rcp
 32713     12 -rwsr-xr-x     1 root       root           11072 Jan 25    2003 /usr/bin/rlogin
 32714      8 -rwsr-xr-x     1 root       root            7740 Jan 25    2003 /usr/bin/rsh
 32718     28 -rwxr-sr-x     1 root       slocate        26368 Feb 20    2003 /usr/bin/slocate
 32724     88 ---s--x--x     1 root       root           84920 Jan 25    2003 /usr/bin/sudo
 32753    112 -rwsr-xr-x     1 root       root          110114 Feb 19    2003 /usr/bin/crontab
242149    152 -rws--x--x     1 root       root          150868 Feb 15    2003
/usr/libexec/openssh/ssh-keysign
129099     28 -rwsr-xr-x     1 root       root           26580 Jan 25    2003 /usr/sbin/ping6
129103     12 -rwsr-xr-x     1 root       root            9988 Jan 25    2003 /usr/sbin/traceroute6
129140     32 -rwsr-xr-x     1 root       root           32674 Mar 13    2003 /usr/sbin/usernetctl
129157     28 -rws--x--x     1 root       root           26680 Feb 25    2003 /usr/sbin/userhelper
129169     12 -rwxr-sr-x     1 root       lock            8800 Feb  4    2003 /usr/sbin/lockdev
129197      8 -rwsr-xr-x     1 root       root            7572 Feb  4    2003 /usr/sbin/userisdnctl
129246    652 -rwxr-sr-x     1 root       smmsp         663232 Sep 18    2003
/usr/sbin/sendmail.sendmail
129253     92 -rwsr-xr-x     1 root       root           86764 Jan 25    2003 /usr/sbin/traceroute
129261     36 -rwxr-sr-x     1 root       utmp           34186 Feb 19    2003 /usr/sbin/utempter
129271     48 -r-s--x---     1 root       48             48741 Feb 25    2003 /usr/sbin/suexec
 42842     29 -rwsr-xr-x     1 root       root           28628 Jan 25    2003 /bin/ping
 42845     32 -rwsr-xr-x     1 root       root           30816 Feb 25    2003 /bin/umount
 42892     95 -rwsr-xr-x     1 root       root           95564 Feb 19    2003 /bin/su
 73548      7 -r-s--x--x     1 root       root            7088 Feb 11    2003
/sbin/pam_timestamp_check
 73549    118 -r-sr-xr-x     1 root       root          119528 Feb 11    2003 /sbin/pwdb_chkpwd
 73550     18 -r-sr-xr-x     1 root       root           17220 Feb 11    2003 /sbin/unix_chkpwd
 73594     29 -rwxr-sr-x     1 root       root           28538 Mar 13    2003 /sbin/netreport
[root@james root]#
```

Above all commands should have the set-UID permission removed for this system except ‘su’ command.

Because this system restrict remote login by root, someone(administrator) might get root ability.

To remove the set-UID bit :
chmod u-s [filename]

To remove the set-GID bit :
chmod g-s [filename]

XI. Configure Syslog to watch the system logs

Syslog is a utility for tracking and logging all manner of system messages from the merely informational to the extremely critical. Each system message sent to the syslog server has two descriptive labels associated with it that makes the message easier to handle.

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical condition
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

<Server system's /etc/syslog.conf>

```
# Log anything (except mail) of level info or higher.
```

```
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure
# Log all the mail messages in one place.
mail.*                                          /var/log/maillog
# Log cron stuff
cron.*                                          /var/log/cron
# Everybody gets emergency messages
*.emerg                                         *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                  /var/log/spooler
# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```

The files to which syslog will write each type of message received is set in the /etc/syslog.conf configuration file. This file consists of two columns, the first lists the facilities and severities of messages to expect and the second lists the files to which they should be logged. By default, RedHat/Fedora's /etc/syslog.conf file is configured to put most of the messages the file /var/log/messages. Here is a sample:

.info;mail.none;authpriv.none;cron.none /var/log/messages

In this case, all messages of severity "info" and above are logged, but none from the mail, cron or authentication facilities/subsystems. You can make this logging even more sensitive by replacing the line above with one that captures all messages from debug severity and above in the /var/log/messages file. This may be more suitable for troubleshooting.

***.debug /var/log/messages**

But, be careful! Very large logs will be in this case.

Changes to /etc/syslog.conf will not take effect until you restart syslog. Issue this command to do so:

[root@james root]# /etc/init.d/syslog restart

XII. Configure OpenSSH

Configuring OpenSSH Server
To run an OpenSSH server, your system should have two packages:
- openssh-server
- openssh

OpenSSH daemon uses the configuration file /etc/ssh/sshd_config.

For this system implementation, SSH2 is only allowed. And Root login via remote host is not allowed. Banner's content is located in /etc/motd file. Edit /etc/ssh/sshd_config file and add/modify the following lines:

```
#Protocol 2,1
Protocol 2
#PermitRootLogin yes
PermitRootLogin no
Banner /etc/motd
```

To start the daemon : # /sbin/service sshd start
To stop that : # /sbin/service sshd stop

To reinstall the OpenSSH, or OS(Redhat), you should keep the host keys (/etc/ssh/ssh_host*key*) files. Restore that files after the reinstallation, and then clients not receive warning message.

Configuring OpenSSH Client
To connect to an OpenSSH server from a client computer, you must install two packages(openssh-clients, openssh).

Content of /etc/ssh/sshd_config

```
#	$OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $
```

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
Protocol 2
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
#PermitRootLogin yes
```

```
PermitRootLogin no
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile    .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no
```

```
# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
#Banner /some/path
Banner /etc/motd
#VerifyReverseMapping no

# override default of no subsystems
Subsystem    sftp    /usr/libexec/openssh/sftp-server
```

XIII. Configure Sendmail

Generate '/etc/mail/sendmail.cf/' by '/etc/mail/sendmail.mc'

```
# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Next modify 'access' file to protect unwant mails.

You can modify accessible/non-accessible host or network by modifying 'access' file.

Example of 'access' file :

```
localhost.localdomain RELAY
localhost RELAY
```

```
127.0.0.1 RELAY
172.16.3.0 RELAY
172.16.11.0 REJECT
```

Above example is
allow from localhost
allow from 172.16.3.0
reject from 172.16.11.0

And next update 'access.db' like this:
makemap hash /etc/mail/access < /etc/mail/access

XIV. Modify firewall configuration

Redhat's default firewall is iptables. Iptables can control input forward packets and output packets.
/etc/sysconfig/iptables

```
# Firewall configuration written by lokkit
# Manual customization of this file is not recommended.
# Note: ifup-post will punch the current nameservers through the
#       firewall; such entries will *not* be listed here.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Lokkit-0-50-INPUT - [0:0]
-A INPUT -j RH-Lokkit-0-50-INPUT
-A FORWARD -j RH-Lokkit-0-50-INPUT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --dport 22 --syn -j ACCEPT
-A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -s 211.252.150.11 --sport 53 -d 0/0 -j
ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --syn -j REJECT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -j REJECT
    COMMIT
```

Port 22 is for ssh, port 53 is for DNS lookup.

So I don’t need any change.
After change, restart iptables daemon to reflect the changes:
/etc/init.d/iptables restart

XV. Mount /usr file system as read-only

For protection against any Trojan binaries being installed by hacker, file system /usr can be mounted as read-only

In /etc/fstab
/usr /usr ext3 ro 1 2

To allow write access before installing rpm or other applications,
mount –o remount,rw /usr

After installation of any programs, change it back to read only
mount –o remount,ro /usr

XVI. Check the system integrity

You can get tripwire package file (tripwire-2.3.1-17.i386.rpm) from Redhat CD #1.

After change the clear text policy file(/etc/tripwire/twpol.txt), you should update the content to real policy file(/etc/tripwire/tw.pol).

In this system, Some files, directories ,that is in clear text policy file, is not. But they don’t need to be deleted, because tripwire database is initialized.
And important files, directories already are included the policy file.

/etc/tripwire/twinstall.sh

To create the tripwire policy file, key files, confguraton file:
    # /etc/tripwire/twinstall.sh
To initialize the tripwire database :
    # /usr/sbin/tripwire --init
To run an integrity check ;

/usr/sbin/tripwire --check | tee > /root/tripwirelog.log

To generate report :

/usr/sbin/tripwire -m r --twrfile /var/lib/tripwire/report/*timestamp.twr* | less

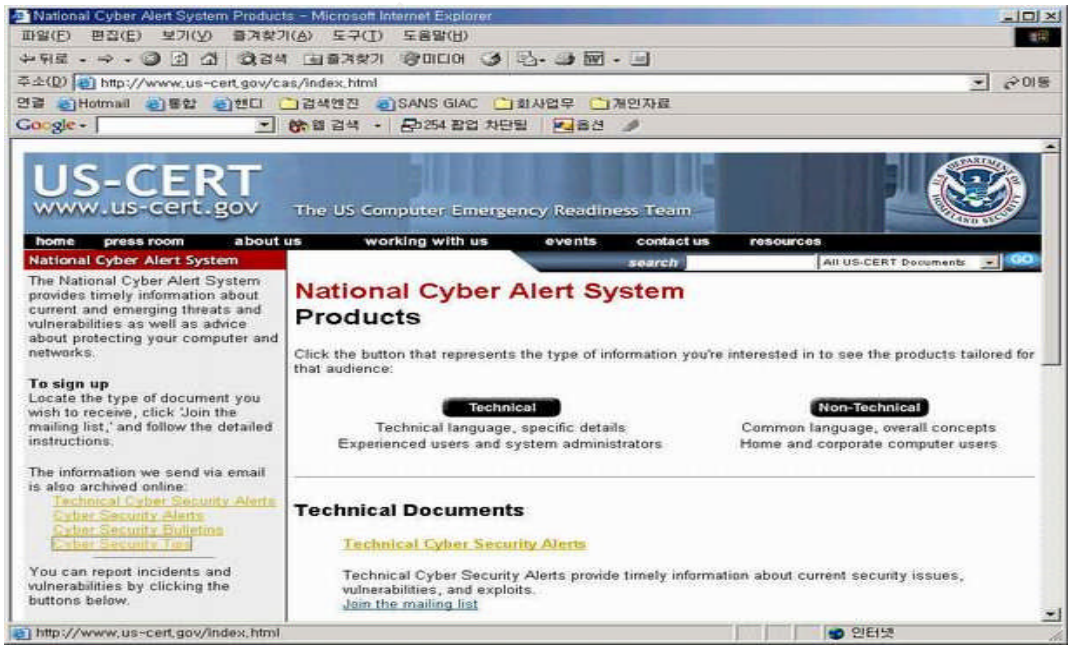
'timestamp.twr' is generated by --check option in /var/lib/tripwire/report directory. timestamp's form is 'hostname-yearmonthday-timestam'.

Integrity Checking Process' example using tripwire is appendix B.

V. Ongoing Maintenance

A. Check for Security Alerts

The CERT/CC is no longer accepting subscriptions to the CERT advisory mailing list, and it will eventually be phased out after subscribers have had an opportunity to subscribe to one or more of the US-CERT mailing lists.



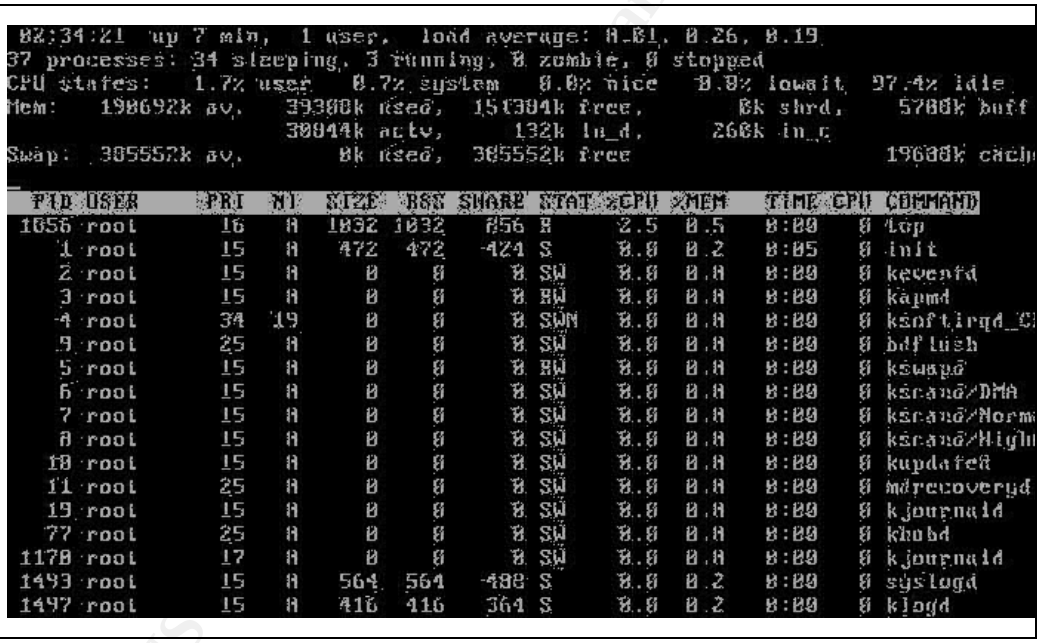
Stay current on vulnerabilities which affect this system
Subscribing mailing lists will help:

US-CERT mailing lists : http://www.us-cert.gov/cas/index.html
OpenSSH mailing lists : http://www.openssh.org/list.html
Redhat mailing lists: http://www.redhat.com
Then they'll send e-mail about vulnerability, advisories. You should check the e-mail message at everyday.
And if the advisories could be adopt this system, you should adapt a patch about that advisory.

B. Monitoring System

Malicious attack(Dos, Virus, etc.) abnormally use system resources. So administrator of system should monitor system resources all the time.

<top command>



If you want more process situation, Use 'ps' command.
#ps -aux | more

<free command>

```
[root@james root]# free
                total       used       free     shared    buffers     cached
Mem:        190692      40008     150684          0       5876
19704
-/+ buffers/cache:      14428     176264
Swap:       385552          0     385552
```

```
[root@james root]#
```

<df command>

```
[root@james root]# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2              3644800   1398788   2060864  41% /
/dev/sda1               101089      9426     86444  10% /boot
none                     95344         0     95344   0% /dev/shm
[root@james root]#
```

C. Review system logs

You can find log files' name in SYSLOG daemon's configuration file (/etc/syslog.conf). In maintenance you should periodically review the system log files. For example :
/var/log/messages
/var/log/cron
/var/log/maillog

'logwatch' tool is system log analyzer and reporter.
You can more easily view the system log.
Defaultly logwatch send a report to root's mail. This can be changed by editing /etc/log.d/logwatch.conf .
MailTo = 'e-mail address' : Write e-mail address to receive log report.
Print = No → If you want to output to screen, change 'Yes'

Above activity should be periodically. So I append the work at cron jobs.
Add file to /etc/cron.daily
<File name: logwatch>

```
#!/bin/sh
/usr/sbin/logwatch --detail med
```

And change that files permission to 755 (chmod 755 logwatch)

Check for updates to key system S/W, OS

Note the Redhat's automatic packages update program "up2date" can be

configured so that no packages that would change configuration data are automatically installed.
But it's good idea that you check the integrity of the configuration after each regular patch updates. This checking can be accomplished by reviewing the tripwire report.

To manually install patches perform the following steps:

Check the firewall's access control policy
iptables –I INPUT –p tcp –m tcp ! --syn -s updates.redhat.com --sport 21 --dport 1024:65535 -j ACCEPT
iptables –I INPUT –p tcp –m tcp -s updates.redhat.com --sport 20 --dport 1024:65535 -j ACCEPT

Remember that these commands does not affect the permanent configuration of firewall's access control policy.

Retrieve all updates for Redhat 9
Redhat provides the automatic update service that run rhnsd daemon every 120 minutes to check for the updates.

Manual method is :
#mkdir /home/admin/patches
#cd /home/admin/patches
#wget ftp://updates.redhat.com/9/en/os/noarch/*.rpm
#wget ftp://updates.redhat.com/9/en/os/`uname -m`/*.rpm
#wget ftp://updates.redhat.com/9/en/os/i386/*.rpm

Install the patches
cd /home/admin/patches
rpm -F *.rpm
(F option means that updates if older version exists and will remove older version.)
Note: You should take care that if the downloaded rpm is for kernel.
For kernel's rpm, you should update by 'i' option.
- Make a directory for that rpm. (#mkdir /home/patches/kernel)

- Move the rpm to the made directory

```
# cd /home/patches
# mv kernel* /home/patches/kernel
# rpm -i kernel*.rpm
```

There are different kernel types such as kernel-smp* for multi-processor, kernel-bigmem* for large physical memory.
Use command 'rpm -qa | grep kernel' to find out what type of kernel was installed on this test server.

D. Consider future need for more advanced tools

- You can restrict users by editing some files in /etc/security

File: /etc/security/limits.conf :
core - limits the core file size (KB)
data - max data size (KB)
fsize - maximum filesize (KB)
memlock - max locked-in-memory address space (KB)
nofile - max number of open files
rss - max resident set size (KB)
stack - max stack size (KB)
cpu - max CPU time (MIN)
nproc - max number of processes
as - address space limit
maxlogins - max number of logins for this user
priority - the priority to run user process with
locks - max number of file locks the user can hold
File: /etc/security/access.conf :
Limit access by network or local console logins.
File: /etc/security/group.conf :
Grant/restrict group device access.
File: /etc/security/time.conf :
Restrict user access by time, day.

VI. Checking the system security

This system have risks that some attacker may penetrate this system. But, this system serve only ssh to outer. So, Should check whether the system have another hole.

A. Nmap

Nmap is a popular program for scanning open port of system.

nmap -sT -P0 -p1-65535 172.16.3.47

-sT is for TCP scan, -P0 is for doing not ping, -p is to specify port range

```
Script started on Sat Jun  5 16:58:58 2004
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]# nmap -sT -P0 -p1-65535 172.16.3.47

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )

Interesting ports on  (172.16.3.47):
(The 65532 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
19063/tcp  filtered    unknown
29521/tcp  filtered    unknown



Nmap run completed -- 1 IP address (1 host up) scanned in 138582 seconds
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
Script done on Tue Jun  8 03:56:02 2004
```

and

nmap -sU -P0 -p1-65535 172.16.3.47

-sU is for UDP scan

```
_]0;root@Matrix2:~_[root@Matrix2 root]# nmap -sU -P0 -p1-65535 172.16.3.47

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
```

```
RTTVAR has grown to over 2.3 seconds, decreasing o 2.0
RTTVAR has grown to over 2.3 seconds, decreasing o 2.0
RTTVAR has grown to over 2.3 seconds, decreasing o 2.0
RTTVAR has grown to over 2.3 seconds, decreasing o 2.0
RTTVAR has grown to over 2.3 seconds, decreasing o 2.0

All 65535 sannedprts    (172.16.3.47) are : closed
Nmap run completed -- 1 IP address (1 host up) scanned in 395923 seconds
_]0;root@Matrix2:~_[root@Matrix2 root]#
```

During nmap test, I've captured packet by Tcpdump.

```
Script started on Sun Jun    6 02:59:16 2004
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]# tcpdump
tcpdump: listening on eth0
02:59:25.922513 Matrix2.kisain.or.kr.63748 > 172.16.3.47.44694:    udp 0
02:59:25.922714 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 44694
unreachable [tos 0xc0]
02:59:25.923877 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:26.152541 Matrix2.kisain.or.kr.60598 > 172.16.3.47.57773: S
1684369966:1684369966(0) win 5840 <mss 1460,sackOK,timestamp 185913015 0,nop,wscale
0> (DF)
02:59:26.152595 Matrix2.kisain.or.kr.60599 > 172.16.3.47.4982: S 1693449503:1693449503(0)
win 5840 <mss 1460,sackOK,timestamp 185913015 0,nop,wscale 0> (DF)
02:59:26.152634 Matrix2.kisain.or.kr.60600 > 172.16.3.47.51181: S
1685090235:1685090235(0) win 5840 <mss 1460,sackOK,timestamp 185913015 0,nop,wscale
0> (DF)
02:59:26.152672 Matrix2.kisain.or.kr.60601 > 172.16.3.47.56017: S
1684096114:1684096114(0) win 5840 <mss 1460,sackOK,timestamp 185913015 0,nop,wscale
0> (DF)
02:59:26.152711 Matrix2.kisain.or.kr.60602 > 172.16.3.47.36042: S
1684125572:1684125572(0) win 5840 <mss 1460,sackOK,timestamp 185913015 0,nop,wscale
0> (DF)
02:59:26.252522 Matrix2.kisain.or.kr.63748 > 172.16.3.47.3158:    udp 0
02:59:26.361661 0.0.0.0.bootpc > 255.255.255.255.bootps:    xid:0x3d157136 flags:0x8000 file
```

```
""[|bootp]
02:59:26.472524 Matrix2.kisain.or.kr.60603 > 172.16.3.47.57773: S
1691736001:1691736001(0) win 5840 <mss 1460,sackOK,timestamp 185913047 0,nop,wscale
0> (DF)
02:59:26.472568 Matrix2.kisain.or.kr.60604 > 172.16.3.47.4982: S 1682639841:1682639841(0)
win 5840 <mss 1460,sackOK,timestamp 185913047 0,nop,wscale 0> (DF)
02:59:26.472606 Matrix2.kisain.or.kr.60605 > 172.16.3.47.51181: S
1683846280:1683846280(0) win 5840 <mss 1460,sackOK,timestamp 185913047 0,nop,wscale
0> (DF)
02:59:26.472644 Matrix2.kisain.or.kr.60606 > 172.16.3.47.56017: S
1691608644:1691608644(0) win 5840 <mss 1460,sackOK,timestamp 185913047 0,nop,wscale
0> (DF)
02:59:26.472683 Matrix2.kisain.or.kr.60607 > 172.16.3.47.36042: S
1683650886:1683650886(0) win 5840 <mss 1460,sackOK,timestamp 185913047 0,nop,wscale
0> (DF)
02:59:26.582489 Matrix2.kisain.or.kr.63748 > 172.16.3.47.31616:    udp 0
02:59:26.792664 Matrix2.kisain.or.kr.60608 > 172.16.3.47.12404: S
1682948041:1682948041(0) win 5840 <mss 1460,sackOK,timestamp 185913079 0,nop,wscale
0> (DF)
02:59:26.792714 Matrix2.kisain.or.kr.60609 > 172.16.3.47.10496: S
1690016423:1690016423(0) win 5840 <mss 1460,sackOK,timestamp 185913079 0,nop,wscale
0> (DF)
02:59:26.792752 Matrix2.kisain.or.kr.60610 > 172.16.3.47.36222: S
1685809896:1685809896(0) win 5840 <mss 1460,sackOK,timestamp 185913079 0,nop,wscale
0> (DF)
02:59:26.792788 Matrix2.kisain.or.kr.60611 > 172.16.3.47.3972: S 1679354507:1679354507(0)
win 5840 <mss 1460,sackOK,timestamp 185913079 0,nop,wscale 0> (DF)
02:59:26.792824 Matrix2.kisain.or.kr.60612 > 172.16.3.47.62924: S
1682984321:1682984321(0) win 5840 <mss 1460,sackOK,timestamp 185913079 0,nop,wscale
0> (DF)
02:59:26.912503 Matrix2.kisain.or.kr.63748 > 172.16.3.47.64294:    udp 0
02:59:26.912693 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 64294
unreachable [tos 0xc0]
02:59:26.922462 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:27.112517 Matrix2.kisain.or.kr.60613 > 172.16.3.47.12404: S
1685899962:1685899962(0) win 5840 <mss 1460,sackOK,timestamp 185913111 0,nop,wscale
```

```
0> (DF)
02:59:27.112565 Matrix2.kisain.or.kr.60614 > 172.16.3.47.10496: S
1684819288:1684819288(0) win 5840 <mss 1460,sackOK,timestamp 185913111 0,nop,wscale
0> (DF)
02:59:27.112603 Matrix2.kisain.or.kr.60615 > 172.16.3.47.36222: S
1682265686:1682265686(0) win 5840 <mss 1460,sackOK,timestamp 185913111 0,nop,wscale
0> (DF)
02:59:27.112641 Matrix2.kisain.or.kr.60616 > 172.16.3.47.3972: S 1682087597:1682087597(0)
win 5840 <mss 1460,sackOK,timestamp 185913111 0,nop,wscale 0> (DF)
02:59:27.112678 Matrix2.kisain.or.kr.60617 > 172.16.3.47.62924: S
1690108777:1690108777(0) win 5840 <mss 1460,sackOK,timestamp 185913111 0,nop,wscale
0> (DF)
02:59:27.242505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.55146:    udp 0
02:59:27.432525 Matrix2.kisain.or.kr.60618 > 172.16.3.47.12404: S
1689249820:1689249820(0) win 5840 <mss 1460,sackOK,timestamp 185913143 0,nop,wscale
0> (DF)
02:59:27.432568 Matrix2.kisain.or.kr.60619 > 172.16.3.47.10496: S
1691758692:1691758692(0) win 5840 <mss 1460,sackOK,timestamp 185913143 0,nop,wscale
0> (DF)
02:59:27.432607 Matrix2.kisain.or.kr.60620 > 172.16.3.47.36222: S
1678837606:1678837606(0) win 5840 <mss 1460,sackOK,timestamp 185913143 0,nop,wscale
0> (DF)
02:59:27.432645 Matrix2.kisain.or.kr.60621 > 172.16.3.47.3972: S 1682793216:1682793216(0)
win 5840 <mss 1460,sackOK,timestamp 185913143 0,nop,wscale 0> (DF)
02:59:27.432683 Matrix2.kisain.or.kr.60622 > 172.16.3.47.62924: S
1689148590:1689148590(0) win 5840 <mss 1460,sackOK,timestamp 185913143 0,nop,wscale
0> (DF)
02:59:27.572506 Matrix2.kisain.or.kr.63748 > 172.16.3.47.46706:    udp 0
02:59:27.752649 Matrix2.kisain.or.kr.60623 > 172.16.3.47.9305: S 1682965296:1682965296(0)
win 5840 <mss 1460,sackOK,timestamp 185913175 0,nop,wscale 0> (DF)
02:59:27.752699 Matrix2.kisain.or.kr.60624 > 172.16.3.47.56745: S
1692258614:1692258614(0) win 5840 <mss 1460,sackOK,timestamp 185913175 0,nop,wscale
0> (DF)
02:59:27.752736 Matrix2.kisain.or.kr.60625 > 172.16.3.47.43316: S
1689236745:1689236745(0) win 5840 <mss 1460,sackOK,timestamp 185913175 0,nop,wscale
0> (DF)
```

```
02:59:27.752773 Matrix2.kisain.or.kr.60626 > 172.16.3.47.36956: S
1680078978:1680078978(0) win 5840 <mss 1460,sackOK,timestamp 185913175 0,nop,wscale
0> (DF)
02:59:27.752809 Matrix2.kisain.or.kr.60627 > 172.16.3.47.51014: S
1685026181:1685026181(0) win 5840 <mss 1460,sackOK,timestamp 185913175 0,nop,wscale
0> (DF)
02:59:27.902497 Matrix2.kisain.or.kr.63748 > 172.16.3.47.51774:    udp 0
02:59:27.902691 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 51774
unreachable [tos 0xc0]
02:59:27.922462 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:28.072528 Matrix2.kisain.or.kr.60628 > 172.16.3.47.9305: S 1695603041:1695603041(0)
win 5840 <mss 1460,sackOK,timestamp 185913207 0,nop,wscale 0> (DF)
02:59:28.072576 Matrix2.kisain.or.kr.60629 > 172.16.3.47.56745: S
1690101141:1690101141(0) win 5840 <mss 1460,sackOK,timestamp 185913207 0,nop,wscale
0> (DF)
02:59:28.072614 Matrix2.kisain.or.kr.60630 > 172.16.3.47.43316: S
1685144415:1685144415(0) win 5840 <mss 1460,sackOK,timestamp 185913207 0,nop,wscale
0> (DF)
02:59:28.072652 Matrix2.kisain.or.kr.60631 > 172.16.3.47.36956: S
1688507010:1688507010(0) win 5840 <mss 1460,sackOK,timestamp 185913207 0,nop,wscale
0> (DF)
02:59:28.072691 Matrix2.kisain.or.kr.60632 > 172.16.3.47.51014: S
1684047109:1684047109(0) win 5840 <mss 1460,sackOK,timestamp 185913207 0,nop,wscale
0> (DF)
02:59:28.232518 Matrix2.kisain.or.kr.63748 > 172.16.3.47.5475:    udp 0
02:59:28.392524 Matrix2.kisain.or.kr.60633 > 172.16.3.47.9305: S 1690355374:1690355374(0)
win 5840 <mss 1460,sackOK,timestamp 185913239 0,nop,wscale 0> (DF)
02:59:28.392567 Matrix2.kisain.or.kr.60634 > 172.16.3.47.56745: S
1688797237:1688797237(0) win 5840 <mss 1460,sackOK,timestamp 185913239 0,nop,wscale
0> (DF)
02:59:28.392606 Matrix2.kisain.or.kr.60635 > 172.16.3.47.43316: S
1689997473:1689997473(0) win 5840 <mss 1460,sackOK,timestamp 185913239 0,nop,wscale
0> (DF)
02:59:28.392645 Matrix2.kisain.or.kr.60636 > 172.16.3.47.36956: S
1696096699:1696096699(0) win 5840 <mss 1460,sackOK,timestamp 185913239 0,nop,wscale
0> (DF)
```

```
02:59:28.392683 Matrix2.kisain.or.kr.60637 > 172.16.3.47.51014: S
1681196732:1681196732(0) win 5840 <mss 1460,sackOK,timestamp 185913239 0,nop,wscale
0> (DF)
02:59:28.562486 Matrix2.kisain.or.kr.63748 > 172.16.3.47.12920:    udp 0
02:59:28.712647 Matrix2.kisain.or.kr.60638 > 172.16.3.47.10044: S
1690486818:1690486818(0) win 5840 <mss 1460,sackOK,timestamp 185913271 0,nop,wscale
0> (DF)
02:59:28.712696 Matrix2.kisain.or.kr.60639 > 172.16.3.47.32191: S
1685815687:1685815687(0) win 5840 <mss 1460,sackOK,timestamp 185913271 0,nop,wscale
0> (DF)
02:59:28.712733 Matrix2.kisain.or.kr.60640 > 172.16.3.47.15616: S
1680214092:1680214092(0) win 5840 <mss 1460,sackOK,timestamp 185913271 0,nop,wscale
0> (DF)
02:59:28.712769 Matrix2.kisain.or.kr.60641 > 172.16.3.47.48162: S
1680664218:1680664218(0) win 5840 <mss 1460,sackOK,timestamp 185913271 0,nop,wscale
0> (DF)
02:59:28.712806 Matrix2.kisain.or.kr.60642 > 172.16.3.47.44847: S
1695320628:1695320628(0) win 5840 <mss 1460,sackOK,timestamp 185913271 0,nop,wscale
0> (DF)
02:59:28.892504 Matrix2.kisain.or.kr.63748 > 172.16.3.47.83:    udp 0
02:59:28.892695 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 83 unreachable
[tos 0xc0]
02:59:29.032531 Matrix2.kisain.or.kr.60643 > 172.16.3.47.10044: S
1686874089:1686874089(0) win 5840 <mss 1460,sackOK,timestamp 185913303 0,nop,wscale
0> (DF)
02:59:29.032580 Matrix2.kisain.or.kr.60644 > 172.16.3.47.32191: S
1689223302:1689223302(0) win 5840 <mss 1460,sackOK,timestamp 185913303 0,nop,wscale
0> (DF)
02:59:29.032619 Matrix2.kisain.or.kr.60645 > 172.16.3.47.15616: S
1685694325:1685694325(0) win 5840 <mss 1460,sackOK,timestamp 185913303 0,nop,wscale
0> (DF)
02:59:29.032656 Matrix2.kisain.or.kr.60646 > 172.16.3.47.48162: S
1682855514:1682855514(0) win 5840 <mss 1460,sackOK,timestamp 185913303 0,nop,wscale
0> (DF)
02:59:29.032694 Matrix2.kisain.or.kr.60647 > 172.16.3.47.44847: S
1691517504:1691517504(0) win 5840 <mss 1460,sackOK,timestamp 185913303 0,nop,wscale
```

```
0> (DF)
02:59:29.222505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.45674:    udp 0
02:59:29.352526 Matrix2.kisain.or.kr.60648 > 172.16.3.47.10044: S
1683460446:1683460446(0) win 5840 <mss 1460,sackOK,timestamp 185913335 0,nop,wscale
0> (DF)
02:59:29.352568 Matrix2.kisain.or.kr.60649 > 172.16.3.47.32191: S
1683121580:1683121580(0) win 5840 <mss 1460,sackOK,timestamp 185913335 0,nop,wscale
0> (DF)
02:59:29.352607 Matrix2.kisain.or.kr.60650 > 172.16.3.47.15616: S
1683093645:1683093645(0) win 5840 <mss 1460,sackOK,timestamp 185913335 0,nop,wscale
0> (DF)
02:59:29.352645 Matrix2.kisain.or.kr.60651 > 172.16.3.47.48162: S
1695132161:1695132161(0) win 5840 <mss 1460,sackOK,timestamp 185913335 0,nop,wscale
0> (DF)
02:59:29.352684 Matrix2.kisain.or.kr.60652 > 172.16.3.47.44847: S
1685530725:1685530725(0) win 5840 <mss 1460,sackOK,timestamp 185913335 0,nop,wscale
0> (DF)
02:59:29.552503 Matrix2.kisain.or.kr.63748 > 172.16.3.47.39323:    udp 0
02:59:29.672647 Matrix2.kisain.or.kr.60653 > 172.16.3.47.22617: S
1691531169:1691531169(0) win 5840 <mss 1460,sackOK,timestamp 185913367 0,nop,wscale
0> (DF)
02:59:29.672697 Matrix2.kisain.or.kr.60654 > 172.16.3.47.23876: S
1697581182:1697581182(0) win 5840 <mss 1460,sackOK,timestamp 185913367 0,nop,wscale
0> (DF)
02:59:29.672733 Matrix2.kisain.or.kr.60655 > 172.16.3.47.58519: S
1687435346:1687435346(0) win 5840 <mss 1460,sackOK,timestamp 185913367 0,nop,wscale
0> (DF)
02:59:29.672770 Matrix2.kisain.or.kr.60656 > 172.16.3.47.60062: S
1696568606:1696568606(0) win 5840 <mss 1460,sackOK,timestamp 185913367 0,nop,wscale
0> (DF)
02:59:29.672807 Matrix2.kisain.or.kr.60657 > 172.16.3.47.33209: S
1682588838:1682588838(0) win 5840 <mss 1460,sackOK,timestamp 185913367 0,nop,wscale
0> (DF)
02:59:29.882489 Matrix2.kisain.or.kr.63748 > 172.16.3.47.22778:    udp 0
02:59:29.882678 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 22778
unreachable [tos 0xc0]
```

```
02:59:29.992488 Matrix2.kisain.or.kr.60658 > 172.16.3.47.22617: S
1694845948:1694845948(0) win 5840 <mss 1460,sackOK,timestamp 185913399 0,nop,wscale
0> (DF)
02:59:29.992526 Matrix2.kisain.or.kr.60659 > 172.16.3.47.23876: S
1684858088:1684858088(0) win 5840 <mss 1460,sackOK,timestamp 185913399 0,nop,wscale
0> (DF)
02:59:29.992564 Matrix2.kisain.or.kr.60660 > 172.16.3.47.58519: S
1693768527:1693768527(0) win 5840 <mss 1460,sackOK,timestamp 185913399 0,nop,wscale
0> (DF)
02:59:29.992600 Matrix2.kisain.or.kr.60661 > 172.16.3.47.60062: S
1684217758:1684217758(0) win 5840 <mss 1460,sackOK,timestamp 185913399 0,nop,wscale
0> (DF)
02:59:29.992638 Matrix2.kisain.or.kr.60662 > 172.16.3.47.33209: S
1696702628:1696702628(0) win 5840 <mss 1460,sackOK,timestamp 185913399 0,nop,wscale
0> (DF)
02:59:30.212520 Matrix2.kisain.or.kr.63748 > 172.16.3.47.50716:    udp 0
02:59:30.312524 Matrix2.kisain.or.kr.60663 > 172.16.3.47.22617: S
1685739384:1685739384(0) win 5840 <mss 1460,sackOK,timestamp 185913431 0,nop,wscale
0> (DF)
02:59:30.312568 Matrix2.kisain.or.kr.60664 > 172.16.3.47.23876: S
1691721154:1691721154(0) win 5840 <mss 1460,sackOK,timestamp 185913431 0,nop,wscale
0> (DF)
02:59:30.312607 Matrix2.kisain.or.kr.60665 > 172.16.3.47.58519: S
1682271367:1682271367(0) win 5840 <mss 1460,sackOK,timestamp 185913431 0,nop,wscale
0> (DF)
02:59:30.312644 Matrix2.kisain.or.kr.60666 > 172.16.3.47.60062: S
1692753568:1692753568(0) win 5840 <mss 1460,sackOK,timestamp 185913431 0,nop,wscale
0> (DF)
02:59:30.312683 Matrix2.kisain.or.kr.60667 > 172.16.3.47.33209: S
1684201360:1684201360(0) win 5840 <mss 1460,sackOK,timestamp 185913431 0,nop,wscale
0> (DF)
02:59:30.360880 0.0.0.0.bootpc > 255.255.255.255.bootps:    xid:0x3d157136 secs:20468
flags:0x8000 file ""[|bootp]
02:59:30.542488 Matrix2.kisain.or.kr.63748 > 172.16.3.47.55294:    udp 0
02:59:30.632663 Matrix2.kisain.or.kr.60668 > 172.16.3.47.46670: S
1693909450:1693909450(0) win 5840 <mss 1460,sackOK,timestamp 185913463 0,nop,wscale
```

```
0> (DF)
02:59:30.632711 Matrix2.kisain.or.kr.60669 > 172.16.3.47.63475: S
1686825645:1686825645(0) win 5840 <mss 1460,sackOK,timestamp 185913463 0,nop,wscale
0> (DF)
02:59:30.632748 Matrix2.kisain.or.kr.60670 > 172.16.3.47.52333: S
1684671592:1684671592(0) win 5840 <mss 1460,sackOK,timestamp 185913463 0,nop,wscale
0> (DF)
02:59:30.632785 Matrix2.kisain.or.kr.60671 > 172.16.3.47.28199: S
1693988243:1693988243(0) win 5840 <mss 1460,sackOK,timestamp 185913463 0,nop,wscale
0> (DF)
02:59:30.632822 Matrix2.kisain.or.kr.60672 > 172.16.3.47.48189: S
1696041295:1696041295(0) win 5840 <mss 1460,sackOK,timestamp 185913463 0,nop,wscale
0> (DF)
02:59:30.872504 Matrix2.kisain.or.kr.63748 > 172.16.3.47.45059:    udp 0
02:59:30.872695 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 45059
unreachable [tos 0xc0]
02:59:30.932501 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:30.952504 Matrix2.kisain.or.kr.60673 > 172.16.3.47.46670: S
1698568861:1698568861(0) win 5840 <mss 1460,sackOK,timestamp 185913495 0,nop,wscale
0> (DF)
02:59:30.952544 Matrix2.kisain.or.kr.60674 > 172.16.3.47.63475: S
1686208643:1686208643(0) win 5840 <mss 1460,sackOK,timestamp 185913495 0,nop,wscale
0> (DF)
02:59:30.952582 Matrix2.kisain.or.kr.60675 > 172.16.3.47.52333: S
1689132643:1689132643(0) win 5840 <mss 1460,sackOK,timestamp 185913495 0,nop,wscale
0> (DF)
02:59:30.952619 Matrix2.kisain.or.kr.60676 > 172.16.3.47.28199: S
1698166541:1698166541(0) win 5840 <mss 1460,sackOK,timestamp 185913495 0,nop,wscale
0> (DF)
02:59:30.952656 Matrix2.kisain.or.kr.60677 > 172.16.3.47.48189: S
1688959194:1688959194(0) win 5840 <mss 1460,sackOK,timestamp 185913495 0,nop,wscale
0> (DF)
02:59:31.202503 Matrix2.kisain.or.kr.63748 > 172.16.3.47.49442:    udp 0
02:59:31.272526 Matrix2.kisain.or.kr.60678 > 172.16.3.47.46670: S
1692521845:1692521845(0) win 5840 <mss 1460,sackOK,timestamp 185913527 0,nop,wscale
0> (DF)
```

```
02:59:31.272569 Matrix2.kisain.or.kr.60679 > 172.16.3.47.63475: S
1693183564:1693183564(0) win 5840 <mss 1460,sackOK,timestamp 185913527 0,nop,wscale
0> (DF)
02:59:31.272608 Matrix2.kisain.or.kr.60680 > 172.16.3.47.52333: S
1693271993:1693271993(0) win 5840 <mss 1460,sackOK,timestamp 185913527 0,nop,wscale
0> (DF)
02:59:31.272647 Matrix2.kisain.or.kr.60681 > 172.16.3.47.28199: S
1698969889:1698969889(0) win 5840 <mss 1460,sackOK,timestamp 185913527 0,nop,wscale
0> (DF)
02:59:31.272686 Matrix2.kisain.or.kr.60682 > 172.16.3.47.48189: S
1699018706:1699018706(0) win 5840 <mss 1460,sackOK,timestamp 185913527 0,nop,wscale
0> (DF)
02:59:31.532516 Matrix2.kisain.or.kr.63748 > 172.16.3.47.25471:    udp 0
02:59:31.592632 Matrix2.kisain.or.kr.60683 > 172.16.3.47.19343: S
1697214935:1697214935(0) win 5840 <mss 1460,sackOK,timestamp 185913559 0,nop,wscale
0> (DF)
02:59:31.592674 Matrix2.kisain.or.kr.60684 > 172.16.3.47.15914: S
1696276936:1696276936(0) win 5840 <mss 1460,sackOK,timestamp 185913559 0,nop,wscale
0> (DF)
02:59:31.592710 Matrix2.kisain.or.kr.60685 > 172.16.3.47.4666: S 1691508883:1691508883(0)
win 5840 <mss 1460,sackOK,timestamp 185913559 0,nop,wscale 0> (DF)
02:59:31.592746 Matrix2.kisain.or.kr.60686 > 172.16.3.47.20609: S
1682895528:1682895528(0) win 5840 <mss 1460,sackOK,timestamp 185913559 0,nop,wscale
0> (DF)
02:59:31.592782 Matrix2.kisain.or.kr.60687 > 172.16.3.47.20171: S
1686029671:1686029671(0) win 5840 <mss 1460,sackOK,timestamp 185913559 0,nop,wscale
0> (DF)
02:59:31.862498 Matrix2.kisain.or.kr.63748 > 172.16.3.47.32306:    udp 0
02:59:31.912514 Matrix2.kisain.or.kr.60688 > 172.16.3.47.19343: S
1698877283:1698877283(0) win 5840 <mss 1460,sackOK,timestamp 185913591 0,nop,wscale
0> (DF)
02:59:31.912553 Matrix2.kisain.or.kr.60689 > 172.16.3.47.15914: S
1684138345:1684138345(0) win 5840 <mss 1460,sackOK,timestamp 185913591 0,nop,wscale
0> (DF)
02:59:31.912590 Matrix2.kisain.or.kr.60690 > 172.16.3.47.4666: S 1689177412:1689177412(0)
win 5840 <mss 1460,sackOK,timestamp 185913591 0,nop,wscale 0> (DF)
```

```
02:59:31.912629 Matrix2.kisain.or.kr.60691 > 172.16.3.47.20609: S
1695725332:1695725332(0) win 5840 <mss 1460,sackOK,timestamp 185913591 0,nop,wscale
0> (DF)
02:59:31.912668 Matrix2.kisain.or.kr.60692 > 172.16.3.47.20171: S
1697332915:1697332915(0) win 5840 <mss 1460,sackOK,timestamp 185913591 0,nop,wscale
0> (DF)
02:59:31.913825 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 19343
unreachable [tos 0xc0]
02:59:31.932461 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:32.192554 Matrix2.kisain.or.kr.63748 > 172.16.3.47.26176:    udp 0
02:59:32.232528 Matrix2.kisain.or.kr.60693 > 172.16.3.47.15914: S
1698854254:1698854254(0) win 5840 <mss 1460,sackOK,timestamp 185913623 0,nop,wscale
0> (DF)
02:59:32.232575 Matrix2.kisain.or.kr.60694 > 172.16.3.47.4666: S 1693015478:1693015478(0)
win 5840 <mss 1460,sackOK,timestamp 185913623 0,nop,wscale 0> (DF)
02:59:32.232616 Matrix2.kisain.or.kr.60695 > 172.16.3.47.20609: S
1683619532:1683619532(0) win 5840 <mss 1460,sackOK,timestamp 185913623 0,nop,wscale
0> (DF)
02:59:32.232657 Matrix2.kisain.or.kr.60696 > 172.16.3.47.20171: S
1698488558:1698488558(0) win 5840 <mss 1460,sackOK,timestamp 185913623 0,nop,wscale
0> (DF)
02:59:32.522488 Matrix2.kisain.or.kr.63748 > 172.16.3.47.7742:    udp 0
02:59:32.552572 Matrix2.kisain.or.kr.60697 > 172.16.3.47.33544: S
1694595028:1694595028(0) win 5840 <mss 1460,sackOK,timestamp 185913655 0,nop,wscale
0> (DF)
02:59:32.552617 Matrix2.kisain.or.kr.60698 > 172.16.3.47.25855: S
1693225928:1693225928(0) win 5840 <mss 1460,sackOK,timestamp 185913655 0,nop,wscale
0> (DF)
02:59:32.552654 Matrix2.kisain.or.kr.60699 > 172.16.3.47.64814: S
1687620930:1687620930(0) win 5840 <mss 1460,sackOK,timestamp 185913655 0,nop,wscale
0> (DF)
02:59:32.852507 Matrix2.kisain.or.kr.63748 > 172.16.3.47.31342:    udp 0
02:59:32.872517 Matrix2.kisain.or.kr.60700 > 172.16.3.47.33544: S
1699579074:1699579074(0) win 5840 <mss 1460,sackOK,timestamp 185913687 0,nop,wscale
0> (DF)
02:59:32.872558 Matrix2.kisain.or.kr.60701 > 172.16.3.47.25855: S
```

```
1689935749:1689935749(0) win 5840 <mss 1460,sackOK,timestamp 185913687 0,nop,wscale
0> (DF)
02:59:32.872597 Matrix2.kisain.or.kr.60702 > 172.16.3.47.64814: S
1693581674:1693581674(0) win 5840 <mss 1460,sackOK,timestamp 185913687 0,nop,wscale
0> (DF)
02:59:32.872905 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 33544
unreachable [tos 0xc0]
02:59:32.932461 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:33.182516 Matrix2.kisain.or.kr.63748 > 172.16.3.47.23559:    udp 0
02:59:33.192551 Matrix2.kisain.or.kr.60703 > 172.16.3.47.25855: S
1689641174:1689641174(0) win 5840 <mss 1460,sackOK,timestamp 185913719 0,nop,wscale
0> (DF)
02:59:33.192598 Matrix2.kisain.or.kr.60704 > 172.16.3.47.64814: S
1691009679:1691009679(0) win 5840 <mss 1460,sackOK,timestamp 185913719 0,nop,wscale
0> (DF)
02:59:33.512549 Matrix2.kisain.or.kr.60705 > 172.16.3.47.7388: S 1697514601:1697514601(0)
win 5840 <mss 1460,sackOK,timestamp 185913751 0,nop,wscale 0> (DF)
02:59:33.512589 Matrix2.kisain.or.kr.60706 > 172.16.3.47.11326: S
1695272631:1695272631(0) win 5840 <mss 1460,sackOK,timestamp 185913751 0,nop,wscale
0> (DF)
02:59:33.512632 Matrix2.kisain.or.kr.63748 > 172.16.3.47.37338:    udp 0
02:59:33.832522 Matrix2.kisain.or.kr.60707 > 172.16.3.47.7388: S 1694487927:1694487927(0)
win 5840 <mss 1460,sackOK,timestamp 185913783 0,nop,wscale 0> (DF)
02:59:33.832573 Matrix2.kisain.or.kr.60708 > 172.16.3.47.11326: S
1694133142:1694133142(0) win 5840 <mss 1460,sackOK,timestamp 185913783 0,nop,wscale
0> (DF)
02:59:33.842483 Matrix2.kisain.or.kr.63748 > 172.16.3.47.31297:    udp 0
02:59:34.132528 Matrix2.kisain.or.kr.60709 > 172.16.3.47.7388: S 1689145171:1689145171(0)
win 5840 <mss 1460,sackOK,timestamp 185913813 0,nop,wscale 0> (DF)
02:59:34.132763 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 7388
unreachable [tos 0xc0]
02:59:34.152485 Matrix2.kisain.or.kr.60710 > 172.16.3.47.11326: S
1689894997:1689894997(0) win 5840 <mss 1460,sackOK,timestamp 185913815 0,nop,wscale
0> (DF)
02:59:34.172497 Matrix2.kisain.or.kr.63748 > 172.16.3.47.6936:    udp 0
02:59:34.472571 Matrix2.kisain.or.kr.60711 > 172.16.3.47.41107: S
```

```
1701021788:1701021788(0) win 5840 <mss 1460,sackOK,timestamp 185913847 0,nop,wscale
0> (DF)
02:59:34.502493 Matrix2.kisain.or.kr.63748 > 172.16.3.47.4307:    udp 0
02:59:34.792524 Matrix2.kisain.or.kr.60712 > 172.16.3.47.41107: S
1697271692:1697271692(0) win 5840 <mss 1460,sackOK,timestamp 185913879 0,nop,wscale
0> (DF)
02:59:34.832499 Matrix2.kisain.or.kr.63748 > 172.16.3.47.59426:    udp 0
02:59:35.112512 Matrix2.kisain.or.kr.60713 > 172.16.3.47.41107: S
1700822614:1700822614(0) win 5840 <mss 1460,sackOK,timestamp 185913911 0,nop,wscale
0> (DF)
02:59:35.112778 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 41107
unreachable [tos 0xc0]
02:59:35.113676 Matrix2.kisain.or.kr.60714 > 172.16.3.47.31983: S
1692310945:1692310945(0) win 5840 <mss 1460,sackOK,timestamp 185913911 0,nop,wscale
0> (DF)
02:59:35.162485 Matrix2.kisain.or.kr.63748 > 172.16.3.47.31569:    udp 0
02:59:35.432533 Matrix2.kisain.or.kr.60715 > 172.16.3.47.31983: S
1703390589:1703390589(0) win 5840 <mss 1460,sackOK,timestamp 185913943 0,nop,wscale
0> (DF)
02:59:35.492503 Matrix2.kisain.or.kr.63748 > 172.16.3.47.65078:    udp 0
02:59:35.752527 Matrix2.kisain.or.kr.60716 > 172.16.3.47.31983: S
1689530067:1689530067(0) win 5840 <mss 1460,sackOK,timestamp 185913975 0,nop,wscale
0> (DF)
02:59:35.822485 Matrix2.kisain.or.kr.63748 > 172.16.3.47.39616:    udp 0
02:59:35.943468 arp who-has 172.16.3.1 tell Matrix2.kisain.or.kr
02:59:36.072573 Matrix2.kisain.or.kr.60717 > 172.16.3.47.18605: S
1700319472:1700319472(0) win 5840 <mss 1460,sackOK,timestamp 185914007 0,nop,wscale
0> (DF)
02:59:36.072828 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 18605
unreachable [tos 0xc0]
02:59:36.072896 Matrix2.kisain.or.kr.60718 > 172.16.3.47.2718: S 1699248283:1699248283(0)
win 5840 <mss 1460,sackOK,timestamp 185914007 0,nop,wscale 0> (DF)
02:59:36.072935 Matrix2.kisain.or.kr.60719 > 172.16.3.47.3014: S 1692621416:1692621416(0)
win 5840 <mss 1460,sackOK,timestamp 185914007 0,nop,wscale 0> (DF)
02:59:36.072973 Matrix2.kisain.or.kr.60720 > 172.16.3.47.48335: S
1697921131:1697921131(0) win 5840 <mss 1460,sackOK,timestamp 185914007 0,nop,wscale
```

```
0> (DF)
02:59:45.992579 Matrix2.kisain.or.kr.60904 > 172.16.3.47.7705: S 1700041199:1700041199(0)
win 5840 <mss 1460,sackOK,timestamp 185914999 0,nop,wscale 0> (DF)
02:59:45.992638 Matrix2.kisain.or.kr.60905 > 172.16.3.47.37238: S
1702351671:1702351671(0) win 5840 <mss 1460,sackOK,timestamp 185914999 0,nop,wscale
0> (DF)
02:59:45.992678 Matrix2.kisain.or.kr.60906 > 172.16.3.47.50101: S
1701481738:1701481738(0) win 5840 <mss 1460,sackOK,timestamp 185914999 0,nop,wscale
0> (DF)
02:59:45.994147 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 7705
unreachable [tos 0xc0]
02:59:46.052520 Matrix2.kisain.or.kr.63748 > 172.16.3.47.51382:    udp 0
02:59:46.312541 Matrix2.kisain.or.kr.60907 > 172.16.3.47.37238: S
1699180736:1699180736(0) win 5840 <mss 1460,sackOK,timestamp 185915031 0,nop,wscale
0> (DF)
02:59:46.312596 Matrix2.kisain.or.kr.60908 > 172.16.3.47.50101: S
1713502932:1713502932(0) win 5840 <mss 1460,sackOK,timestamp 185915031 0,nop,wscale
0> (DF)
02:59:46.382505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.46806:    udp 0
02:59:46.613584 Matrix2.kisain.or.kr.60909 > 172.16.3.47.16800: S
1701478627:1701478627(0) win 5840 <mss 1460,sackOK,timestamp 185915061 0,nop,wscale
0> (DF)
02:59:46.613641 Matrix2.kisain.or.kr.60910 > 172.16.3.47.52688: S
1707426424:1707426424(0) win 5840 <mss 1460,sackOK,timestamp 185915061 0,nop,wscale
0> (DF)
02:59:46.712518 Matrix2.kisain.or.kr.63748 > 172.16.3.47.12303:    udp 0
02:59:46.932534 Matrix2.kisain.or.kr.60911 > 172.16.3.47.16800: S
1709565412:1709565412(0) win 5840 <mss 1460,sackOK,timestamp 185915093 0,nop,wscale
0> (DF)
02:59:46.932591 Matrix2.kisain.or.kr.60912 > 172.16.3.47.52688: S
1710067740:1710067740(0) win 5840 <mss 1460,sackOK,timestamp 185915093 0,nop,wscale
0> (DF)
02:59:46.932834 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 16800
unreachable [tos 0xc0]
02:59:47.042507 Matrix2.kisain.or.kr.63748 > 172.16.3.47.60422:    udp 0
02:59:47.252540 Matrix2.kisain.or.kr.60913 > 172.16.3.47.52688: S
```

```
1703003668:1703003668(0) win 5840 <mss 1460,sackOK,timestamp 185915125 0,nop,wscale
0> (DF)
02:59:47.372515 Matrix2.kisain.or.kr.63748 > 172.16.3.47.2297:    udp 0
02:59:47.572583 Matrix2.kisain.or.kr.60914 > 172.16.3.47.42937: S
1711030184:1711030184(0) win 5840 <mss 1460,sackOK,timestamp 185915157 0,nop,wscale
0> (DF)
02:59:47.702505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.31343:    udp 0
02:59:47.892537 Matrix2.kisain.or.kr.60915 > 172.16.3.47.42937: S
1713546633:1713546633(0) win 5840 <mss 1460,sackOK,timestamp 185915189 0,nop,wscale
0> (DF)
02:59:47.892780 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 42937
unreachable [tos 0xc0]
02:59:47.892900 Matrix2.kisain.or.kr.60916 > 172.16.3.47.39149: S
1707150567:1707150567(0) win 5840 <mss 1460,sackOK,timestamp 185915189 0,nop,wscale
0> (DF)
02:59:48.032528 Matrix2.kisain.or.kr.63748 > 172.16.3.47.26630:    udp 0
02:59:48.081268 arp who-has Matrix2.kisain.or.kr tell 172.16.3.47
02:59:48.081297 arp reply Matrix2.kisain.or.kr is-at 0:4:76:72:2f:bf
02:59:48.212540 Matrix2.kisain.or.kr.60917 > 172.16.3.47.39149: S
1705825045:1705825045(0) win 5840 <mss 1460,sackOK,timestamp 185915221 0,nop,wscale
0> (DF)
02:59:48.362503 Matrix2.kisain.or.kr.63748 > 172.16.3.47.16647:    udp 0
02:59:48.532546 Matrix2.kisain.or.kr.60918 > 172.16.3.47.39149: S
1715398409:1715398409(0) win 5840 <mss 1460,sackOK,timestamp 185915253 0,nop,wscale
0> (DF)
02:59:48.692517 Matrix2.kisain.or.kr.63748 > 172.16.3.47.54005:    udp 0
02:59:48.852570 Matrix2.kisain.or.kr.60919 > 172.16.3.47.50119: S
1708638468:1708638468(0) win 5840 <mss 1460,sackOK,timestamp 185915285 0,nop,wscale
0> (DF)
02:59:49.022506 Matrix2.kisain.or.kr.63748 > 172.16.3.47.ica:    udp 0
02:59:49.022709 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port ica unreachable
[tos 0xc0]
02:59:49.172539 Matrix2.kisain.or.kr.60920 > 172.16.3.47.50119: S
1710278523:1710278523(0) win 5840 <mss 1460,sackOK,timestamp 185915317 0,nop,wscale
0> (DF)
02:59:49.352516 Matrix2.kisain.or.kr.63748 > 172.16.3.47.20417:    udp 0
```

```
02:59:49.492535 Matrix2.kisain.or.kr.60921 > 172.16.3.47.50119: S
1708334890:1708334890(0) win 5840 <mss 1460,sackOK,timestamp 185915349 0,nop,wscale
0> (DF)
02:59:49.682505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.48452:    udp 0
02:59:49.812578 Matrix2.kisain.or.kr.60922 > 172.16.3.47.30282: S
1714040817:1714040817(0) win 5840 <mss 1460,sackOK,timestamp 185915381 0,nop,wscale
0> (DF)
02:59:50.012517 Matrix2.kisain.or.kr.63748 > 172.16.3.47.42821:    udp 0
02:59:50.012718 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 42821
unreachable [tos 0xc0]
02:59:50.132549 Matrix2.kisain.or.kr.60923 > 172.16.3.47.30282: S
1712060805:1712060805(0) win 5840 <mss 1460,sackOK,timestamp 185915413 0,nop,wscale
0> (DF)
02:59:50.342506 Matrix2.kisain.or.kr.63748 > 172.16.3.47.41274:    udp 0
02:59:50.452538 Matrix2.kisain.or.kr.60924 > 172.16.3.47.30282: S
1702809147:1702809147(0) win 5840 <mss 1460,sackOK,timestamp 185915445 0,nop,wscale
0> (DF)
02:59:50.672516 Matrix2.kisain.or.kr.63748 > 172.16.3.47.36407:    udp 0
02:59:50.752627 Matrix2.kisain.or.kr.60925 > 172.16.3.47.22593: S
1712991962:1712991962(0) win 5840 <mss 1460,sackOK,timestamp 185915475 0,nop,wscale
0> (DF)
02:59:51.002501 Matrix2.kisain.or.kr.63748 > 172.16.3.47.59206:    udp 0
02:59:51.002703 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 59206
unreachable [tos 0xc0]
02:59:51.072536 Matrix2.kisain.or.kr.60926 > 172.16.3.47.22593: S
1702774723:1702774723(0) win 5840 <mss 1460,sackOK,timestamp 185915507 0,nop,wscale
0> (DF)
02:59:51.332518 Matrix2.kisain.or.kr.63748 > 172.16.3.47.47251:    udp 0
02:59:51.392536 Matrix2.kisain.or.kr.60927 > 172.16.3.47.22593: S
1715784304:1715784304(0) win 5840 <mss 1460,sackOK,timestamp 185915539 0,nop,wscale
0> (DF)
02:59:51.662504 Matrix2.kisain.or.kr.63748 > 172.16.3.47.17870:    udp 0
02:59:51.712577 Matrix2.kisain.or.kr.60928 > 172.16.3.47.1064: S 1712710900:1712710900(0)
win 5840 <mss 1460,sackOK,timestamp 185915571 0,nop,wscale 0> (DF)
02:59:51.992514 Matrix2.kisain.or.kr.63748 > 172.16.3.47.12984:    udp 0
02:59:51.992716 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 12984
```

unreachable [tos 0xc0]
02:59:52.032547 Matrix2.kisain.or.kr.60929 > 172.16.3.47.1064: S 1712746888:1712746888(0) win 5840 <mss 1460,sackOK,timestamp 185915603 0,nop,wscale 0> (DF)
02:59:52.322506 Matrix2.kisain.or.kr.63748 > 172.16.3.47.38352: udp 0
02:59:52.332567 Matrix2.kisain.or.kr.60930 > 172.16.3.47.1064: S 1716353362:1716353362(0) win 5840 <mss 1460,sackOK,timestamp 185915633 0,nop,wscale 0> (DF)
02:59:52.652580 Matrix2.kisain.or.kr.60931 > 172.16.3.47.29522: S 1707625978:1707625978(0) win 5840 <mss 1460,sackOK,timestamp 185915665 0,nop,wscale 0> (DF)
02:59:52.652659 Matrix2.kisain.or.kr.63748 > 172.16.3.47.45959: udp 0
02:59:52.972533 Matrix2.kisain.or.kr.60932 > 172.16.3.47.29522: S 1710492041:1710492041(0) win 5840 <mss 1460,sackOK,timestamp 185915697 0,nop,wscale 0> (DF)
02:59:52.972774 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 29522 unreachable [tos 0xc0]
02:59:52.973004 Matrix2.kisain.or.kr.60933 > 172.16.3.47.8826: S 1704427170:1704427170(0) win 5840 <mss 1460,sackOK,timestamp 185915697 0,nop,wscale 0> (DF)
02:59:52.982516 Matrix2.kisain.or.kr.63748 > 172.16.3.47.54803: udp 0
02:59:53.292540 Matrix2.kisain.or.kr.60934 > 172.16.3.47.8826: S 1712739063:1712739063(0) win 5840 <mss 1460,sackOK,timestamp 185915729 0,nop,wscale 0> (DF)
02:59:53.312539 Matrix2.kisain.or.kr.63748 > 172.16.3.47.40662: udp 0
02:59:53.612540 Matrix2.kisain.or.kr.60935 > 172.16.3.47.8826: S 1711531177:1711531177(0) win 5840 <mss 1460,sackOK,timestamp 185915761 0,nop,wscale 0> (DF)
02:59:53.642505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.50587: udp 0
02:59:53.932578 Matrix2.kisain.or.kr.60936 > 172.16.3.47.45476: S 1711899402:1711899402(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.932814 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 45476 unreachable [tos 0xc0]
02:59:53.933001 Matrix2.kisain.or.kr.60937 > 172.16.3.47.63218: S 1711772697:1711772697(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.933049 Matrix2.kisain.or.kr.60938 > 172.16.3.47.34310: S 1721771124:1721771124(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.933089 Matrix2.kisain.or.kr.60939 > 172.16.3.47.24149: S

1718352379:1718352379(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.933128 Matrix2.kisain.or.kr.60940 > 172.16.3.47.54334: S 1712813005:1712813005(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.933167 Matrix2.kisain.or.kr.60941 > 172.16.3.47.3465: S 1707062696:1707062696(0) win 5840 <mss 1460,sackOK,timestamp 185915793 0,nop,wscale 0> (DF)
02:59:53.972520 Matrix2.kisain.or.kr.63748 > 172.16.3.47.20651: udp 0
02:59:54.252537 Matrix2.kisain.or.kr.60942 > 172.16.3.47.63218: S 1709258610:1709258610(0) win 5840 <mss 1460,sackOK,timestamp 185915825 0,nop,wscale 0> (DF)
02:59:54.252593 Matrix2.kisain.or.kr.60943 > 172.16.3.47.34310: S 1719481032:1719481032(0) win 5840 <mss 1460,sackOK,timestamp 185915825 0,nop,wscale 0> (DF)
02:59:54.252632 Matrix2.kisain.or.kr.60944 > 172.16.3.47.24149: S 1716169462:1716169462(0) win 5840 <mss 1460,sackOK,timestamp 185915825 0,nop,wscale 0> (DF)
02:59:54.252670 Matrix2.kisain.or.kr.60945 > 172.16.3.47.54334: S 1707889121:1707889121(0) win 5840 <mss 1460,sackOK,timestamp 185915825 0,nop,wscale 0> (DF)
02:59:54.252707 Matrix2.kisain.or.kr.60946 > 172.16.3.47.3465: S 1720209736:1720209736(0) win 5840 <mss 1460,sackOK,timestamp 185915825 0,nop,wscale 0> (DF)
02:59:54.302505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.40979: udp 0
02:59:54.572541 Matrix2.kisain.or.kr.60947 > 172.16.3.47.63218: S 1721448778:1721448778(0) win 5840 <mss 1460,sackOK,timestamp 185915857 0,nop,wscale 0> (DF)
02:59:54.572594 Matrix2.kisain.or.kr.60948 > 172.16.3.47.34310: S 1705787809:1705787809(0) win 5840 <mss 1460,sackOK,timestamp 185915857 0,nop,wscale 0> (DF)
02:59:54.572633 Matrix2.kisain.or.kr.60949 > 172.16.3.47.24149: S 1707195934:1707195934(0) win 5840 <mss 1460,sackOK,timestamp 185915857 0,nop,wscale 0> (DF)
02:59:54.572671 Matrix2.kisain.or.kr.60950 > 172.16.3.47.54334: S 1721458610:1721458610(0) win 5840 <mss 1460,sackOK,timestamp 185915857 0,nop,wscale 0> (DF)
02:59:54.572709 Matrix2.kisain.or.kr.60951 > 172.16.3.47.3465: S 1718318283:1718318283(0)

```
win 5840 <mss 1460,sackOK,timestamp 185915857 0,nop,wscale 0> (DF)
02:59:54.632540 Matrix2.kisain.or.kr.63748 > 172.16.3.47.63082:    udp 0
02:59:54.892671 Matrix2.kisain.or.kr.60952 > 172.16.3.47.6162: S 1707713557:1707713557(0)
win 5840 <mss 1460,sackOK,timestamp 185915889 0,nop,wscale 0> (DF)
02:59:54.892729 Matrix2.kisain.or.kr.60953 > 172.16.3.47.53685: S
1717869417:1717869417(0) win 5840 <mss 1460,sackOK,timestamp 185915889 0,nop,wscale
0> (DF)
02:59:54.892766 Matrix2.kisain.or.kr.60954 > 172.16.3.47.51421: S
1722406963:1722406963(0) win 5840 <mss 1460,sackOK,timestamp 185915889 0,nop,wscale
0> (DF)
02:59:54.892802 Matrix2.kisain.or.kr.60955 > 172.16.3.47.33000: S
1715744891:1715744891(0) win 5840 <mss 1460,sackOK,timestamp 185915889 0,nop,wscale
0> (DF)
02:59:54.892839 Matrix2.kisain.or.kr.60956 > 172.16.3.47.56131: S
1713266827:1713266827(0) win 5840 <mss 1460,sackOK,timestamp 185915889 0,nop,wscale
0> (DF)
02:59:54.893053 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 tcp port 6162
unreachable [tos 0xc0]
02:59:54.912560 Matrix2.kisain.or.kr.60957 > 172.16.3.47.46783: S
1711686383:1711686383(0) win 5840 <mss 1460,sackOK,timestamp 185915891 0,nop,wscale
0> (DF)
02:59:54.962502 Matrix2.kisain.or.kr.63748 > 172.16.3.47.42099:    udp 0
02:59:55.212540 Matrix2.kisain.or.kr.60958 > 172.16.3.47.53685: S
1720902853:1720902853(0) win 5840 <mss 1460,sackOK,timestamp 185915921 0,nop,wscale
0> (DF)
02:59:55.212595 Matrix2.kisain.or.kr.60959 > 172.16.3.47.51421: S
1712902593:1712902593(0) win 5840 <mss 1460,sackOK,timestamp 185915921 0,nop,wscale
0> (DF)
02:59:55.212634 Matrix2.kisain.or.kr.60960 > 172.16.3.47.33000: S
1716132073:1716132073(0) win 5840 <mss 1460,sackOK,timestamp 185915921 0,nop,wscale
0> (DF)
02:59:55.212672 Matrix2.kisain.or.kr.60961 > 172.16.3.47.56131: S
1714284541:1714284541(0) win 5840 <mss 1460,sackOK,timestamp 185915921 0,nop,wscale
0> (DF)
02:59:55.212710 Matrix2.kisain.or.kr.60962 > 172.16.3.47.46783: S
1711926431:1711926431(0) win 5840 <mss 1460,sackOK,timestamp 185915921 0,nop,wscale
```

```
0> (DF)
02:59:55.292518 Matrix2.kisain.or.kr.63748 > 172.16.3.47.64016:    udp 0
02:59:55.360285 0.0.0.0.bootpc > 255.255.255.255.bootps:    xid:0x3d157136 secs:20468
flags:0x8000 file ""[|bootp]
02:59:55.532553 Matrix2.kisain.or.kr.60963 > 172.16.3.47.53685: S
1721573363:1721573363(0) win 5840 <mss 1460,sackOK,timestamp 185915953 0,nop,wscale
0> (DF)
02:59:55.532608 Matrix2.kisain.or.kr.60964 > 172.16.3.47.51421: S
1707537410:1707537410(0) win 5840 <mss 1460,sackOK,timestamp 185915953 0,nop,wscale
0> (DF)
02:59:55.532648 Matrix2.kisain.or.kr.60965 > 172.16.3.47.33000: S
1708442632:1708442632(0) win 5840 <mss 1460,sackOK,timestamp 185915953 0,nop,wscale
0> (DF)
02:59:55.532687 Matrix2.kisain.or.kr.60966 > 172.16.3.47.56131: S
1720151579:1720151579(0) win 5840 <mss 1460,sackOK,timestamp 185915953 0,nop,wscale
0> (DF)
02:59:55.532726 Matrix2.kisain.or.kr.60967 > 172.16.3.47.46783: S
1712081292:1712081292(0) win 5840 <mss 1460,sackOK,timestamp 185915953 0,nop,wscale
0> (DF)
02:59:55.622593 Matrix2.kisain.or.kr.63748 > 172.16.3.47.5551:    udp 0
02:59:55.852670 Matrix2.kisain.or.kr.60968 > 172.16.3.47.21523: S
1715991172:1715991172(0) win 5840 <mss 1460,sackOK,timestamp 185915985 0,nop,wscale
0> (DF)
02:59:55.852723 Matrix2.kisain.or.kr.60969 > 172.16.3.47.44369: S
1722104210:1722104210(0) win 5840 <mss 1460,sackOK,timestamp 185915985 0,nop,wscale
0> (DF)
02:59:55.852761 Matrix2.kisain.or.kr.60970 > 172.16.3.47.64639: S
1719268216:1719268216(0) win 5840 <mss 1460,sackOK,timestamp 185915985 0,nop,wscale
0> (DF)
02:59:55.852798 Matrix2.kisain.or.kr.60971 > 172.16.3.47.42794: S
1719080872:1719080872(0) win 5840 <mss 1460,sackOK,timestamp 185915985 0,nop,wscale
0> (DF)
02:59:55.852834 Matrix2.kisain.or.kr.60972 > 172.16.3.47.35065: S
1707095930:1707095930(0) win 5840 <mss 1460,sackOK,timestamp 185915985 0,nop,wscale
0> (DF)
02:59:55.952517 Matrix2.kisain.or.kr.63748 > 172.16.3.47.64183:    udp 0
```

```
02:59:55.952719 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 64183
unreachable [tos 0xc0]
02:59:56.172538 Matrix2.kisain.or.kr.60973 > 172.16.3.47.21523: S
1719878050:1719878050(0) win 5840 <mss 1460,sackOK,timestamp 185916017 0,nop,wscale
0> (DF)
02:59:56.172593 Matrix2.kisain.or.kr.60974 > 172.16.3.47.44369: S
1716805508:1716805508(0) win 5840 <mss 1460,sackOK,timestamp 185916017 0,nop,wscale
0> (DF)
02:59:56.172632 Matrix2.kisain.or.kr.60975 > 172.16.3.47.64639: S
1719355759:1719355759(0) win 5840 <mss 1460,sackOK,timestamp 185916017 0,nop,wscale
0> (DF)
02:59:56.172671 Matrix2.kisain.or.kr.60976 > 172.16.3.47.42794: S
1710996860:1710996860(0) win 5840 <mss 1460,sackOK,timestamp 185916017 0,nop,wscale
0> (DF)
02:59:56.172709 Matrix2.kisain.or.kr.60977 > 172.16.3.47.35065: S
1712493729:1712493729(0) win 5840 <mss 1460,sackOK,timestamp 185916017 0,nop,wscale
0> (DF)
02:59:56.282505 Matrix2.kisain.or.kr.63748 > 172.16.3.47.36947:    udp 0
02:59:56.492536 Matrix2.kisain.or.kr.60978 > 172.16.3.47.21523: S
1722591293:1722591293(0) win 5840 <mss 1460,sackOK,timestamp 185916049 0,nop,wscale
0> (DF)
02:59:56.492588 Matrix2.kisain.or.kr.60979 > 172.16.3.47.44369: S
1719990726:1719990726(0) win 5840 <mss 1460,sackOK,timestamp 185916049 0,nop,wscale
0> (DF)
02:59:56.492628 Matrix2.kisain.or.kr.60980 > 172.16.3.47.64639: S
1722785098:1722785098(0) win 5840 <mss 1460,sackOK,timestamp 185916049 0,nop,wscale
0> (DF)
02:59:56.492666 Matrix2.kisain.or.kr.60981 > 172.16.3.47.42794: S
1709940943:1709940943(0) win 5840 <mss 1460,sackOK,timestamp 185916049 0,nop,wscale
0> (DF)
02:59:56.492704 Matrix2.kisain.or.kr.60982 > 172.16.3.47.35065: S
1717593118:1717593118(0) win 5840 <mss 1460,sackOK,timestamp 185916049 0,nop,wscale
0> (DF)
02:59:56.613496 Matrix2.kisain.or.kr.63748 > 172.16.3.47.36209:    udp 0
02:59:56.812617 Matrix2.kisain.or.kr.60983 > 172.16.3.47.23179: S
1723289567:1723289567(0) win 5840 <mss 1460,sackOK,timestamp 185916081 0,nop,wscale
```

```
0> (DF)
02:59:56.812668 Matrix2.kisain.or.kr.60984 > 172.16.3.47.36758: S
1721793265:1721793265(0) win 5840 <mss 1460,sackOK,timestamp 185916081 0,nop,wscale
0> (DF)
02:59:56.812706 Matrix2.kisain.or.kr.60985 > 172.16.3.47.47209: S
1710941679:1710941679(0) win 5840 <mss 1460,sackOK,timestamp 185916081 0,nop,wscale
0> (DF)
02:59:56.812742 Matrix2.kisain.or.kr.60986 > 172.16.3.47.23053: S
1715099925:1715099925(0) win 5840 <mss 1460,sackOK,timestamp 185916081 0,nop,wscale
0> (DF)
02:59:56.812779 Matrix2.kisain.or.kr.60987 > 172.16.3.47.49147: S
1718082535:1718082535(0) win 5840 <mss 1460,sackOK,timestamp 185916081 0,nop,wscale
0> (DF)
02:59:56.942504 Matrix2.kisain.or.kr.63748 > 172.16.3.47.60298:    udp 0
02:59:56.942712 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 60298
unreachable [tos 0xc0]
02:59:57.132546 Matrix2.kisain.or.kr.60988 > 172.16.3.47.23179: S
1716230641:1716230641(0) win 5840 <mss 1460,sackOK,timestamp 185916113 0,nop,wscale
0> (DF)
02:59:57.132601 Matrix2.kisain.or.kr.60989 > 172.16.3.47.36758: S
1709224400:1709224400(0) win 5840 <mss 1460,sackOK,timestamp 185916113 0,nop,wscale
0> (DF)
02:59:57.132640 Matrix2.kisain.or.kr.60990 > 172.16.3.47.47209: S
1714318044:1714318044(0) win 5840 <mss 1460,sackOK,timestamp 185916113 0,nop,wscale
0> (DF)
02:59:57.132679 Matrix2.kisain.or.kr.60991 > 172.16.3.47.23053: S
1722337613:1722337613(0) win 5840 <mss 1460,sackOK,timestamp 185916113 0,nop,wscale
0> (DF)
02:59:57.132717 Matrix2.kisain.or.kr.60992 > 172.16.3.47.49147: S
1714512461:1714512461(0) win 5840 <mss 1460,sackOK,timestamp 185916113 0,nop,wscale
0> (DF)
02:59:57.272524 Matrix2.kisain.or.kr.63748 > 172.16.3.47.17084:    udp 0
02:59:57.452537 Matrix2.kisain.or.kr.60993 > 172.16.3.47.23179: S
1716792241:1716792241(0) win 5840 <mss 1460,sackOK,timestamp 185916145 0,nop,wscale
0> (DF)
02:59:57.452590 Matrix2.kisain.or.kr.60994 > 172.16.3.47.36758: S
```

```
1718683425:1718683425(0) win 5840 <mss 1460,sackOK,timestamp 185916145 0,nop,wscale
0> (DF)
02:59:57.452630 Matrix2.kisain.or.kr.60995 > 172.16.3.47.47209: S
1711451182:1711451182(0) win 5840 <mss 1460,sackOK,timestamp 185916145 0,nop,wscale
0> (DF)
02:59:57.452668 Matrix2.kisain.or.kr.60996 > 172.16.3.47.23053: S
1717901523:1717901523(0) win 5840 <mss 1460,sackOK,timestamp 185916145 0,nop,wscale
0> (DF)
02:59:57.452705 Matrix2.kisain.or.kr.60997 > 172.16.3.47.49147: S
1711305089:1711305089(0) win 5840 <mss 1460,sackOK,timestamp 185916145 0,nop,wscale
0> (DF)
02:59:57.602510 Matrix2.kisain.or.kr.63748 > 172.16.3.47.41657:    udp 0
02:59:57.772628 Matrix2.kisain.or.kr.60998 > 172.16.3.47.65436: S
1719546736:1719546736(0) win 5840 <mss 1460,sackOK,timestamp 185916177 0,nop,wscale
0> (DF)
02:59:57.772684 Matrix2.kisain.or.kr.60999 > 172.16.3.47.29509: S
1725705518:1725705518(0) win 5840 <mss 1460,sackOK,timestamp 185916177 0,nop,wscale
0> (DF)
02:59:57.772721 Matrix2.kisain.or.kr.61000 > 172.16.3.47.38527: S
1711554066:1711554066(0) win 5840 <mss 1460,sackOK,timestamp 185916177 0,nop,wscale
0> (DF)
02:59:57.772758 Matrix2.kisain.or.kr.32768 > 172.16.3.47.30295: S
1722189899:1722189899(0) win 5840 <mss 1460,sackOK,timestamp 185916177 0,nop,wscale
0> (DF)
02:59:57.772795 Matrix2.kisain.or.kr.32769 > 172.16.3.47.31503: S
1709847885:1709847885(0) win 5840 <mss 1460,sackOK,timestamp 185916177 0,nop,wscale
0> (DF)
02:59:57.932517 Matrix2.kisain.or.kr.63748 > 172.16.3.47.30549:    udp 0
02:59:57.932719 172.16.3.47 > Matrix2.kisain.or.kr: icmp: 172.16.3.47 udp port 30549
unreachable [tos 0xc0]
02:59:58.092539 Matrix2.kisain.or.kr.32770 > 172.16.3.47.65436: S
1716141212:1716141212(0) win 5840 <mss 1460,sackOK,timestamp 185916209 0,nop,wscale
0> (DF)
02:59:58.092595 Matrix2.kisain.or.kr.32771 > 172.16.3.47.29509: S
1716571079:1716571079(0) win 5840 <mss 1460,sackOK,timestamp 185916209 0,nop,wscale
0> (DF)
```

```
02:59:58.092633 Matrix2.kisain.or.kr.32772 > 172.16.3.47.38527: S
1712818832:1712818832(0) win 5840 <mss 1460,sackOK,timestamp 185916209 0,nop,wscale
0> (DF)
02:59:58.092671 Matrix2.kisain.or.kr.32773 > 172.16.3.47.30295: S
1718673011:1718673011(0) win 5840 <mss 1460,sackOK,timestamp 185916209 0,nop,wscale
0> (DF)
02:59:58.092710 Matrix2.kisain.or.kr.32774 > 172.16.3.47.31503: S
1720803677:1720803677(0) win 5840 <mss 1460,sackOK,timestamp 185916209 0,nop,wscale
0> (DF)

331 packets received by filter
0 packets dropped by kernel
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
Script done on Sun Jun    6 03:00:00 2004
```

B. Test 1 : remote SSH logins are allowed

```
Script started on Wed May 19 05:11:15 2004
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]# ssh james@172.16.3.47
james@172.16.11.47's password:
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$ ifconfig
-bash: ifconfig: command not found
_]0;james@james:~_[james@james james]$ uname -a
Linux james 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i686 i386
GNU/Linux
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$ exit
```

```
logout
_[H_[2JConnection to 172.16.11.47 closed.
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]# exit_ __ __ __ _
Script done on Wed May 19 05:12:40 2004
```

C. Test 2 : remote SSH logins & su command are allowed

```
Script started on Sat Jun  5 17:01:14 2004
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]# ssh james@172.16.3.47
james@172.16.3.47's password:
This server is for evaluation of IT product.
Your action is logging.
This server is for authorized use only.
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$
_]0;james@james:~_[james@james james]$ whoami
james
_]0;james@james:~_[james@james james]$ uid
-bash: uid: command not found
_]0;james@james:~_[james@james james]$ uname
Linux
_]0;james@james:~_[james@james james]$ ifcofnig__[K__[K__[K__[Knfig
-bash: ifconfig: command not found
_]0;james@james:~_[james@james james]$ ifconfig
-bash: ifconfig: command not found
_]0;james@james:~_[james@james james]$ su
Password:
_]0;james@james:/home/james_[root@james james]#
_]0;james@james:/home/james_[root@james james]#
_]0;james@james:/home/james_[root@james james]# ifconfig
bash: ifconfig: command not found
_]0;james@james:/home/james_[root@james james]# which ifconfig
```

```
/usr/bin/which: no ifconfig in
(/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin:/home/james/bin)
_]0;james@james:/home/james_[root@james james]# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:04:75:C1:2B:D0
          inet addr:172.16.3.47  Bcast:172.16.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4752 errors:0 dropped:0 overruns:1 frame:0
          TX packets:687 errors:0 dropped:0 overruns:0 carrier:0
          collisions:32 txqueuelen:100
          RX bytes:335208 (327.3 Kb)  TX bytes:69328 (67.7 Kb)
          Interrupt:5 Base address:0xe800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:263652 errors:0 dropped:0 overruns:0 frame:0
          TX packets:263652 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12122475 (11.5 Mb)  TX bytes:12122475 (11.5 Mb)

_]0;james@james:/home/james_[root@james james]#
_]0;james@james:/home/james_[root@james james]#
_]0;james@james:/home/james_[root@james james]# exit
exit
_]0;james@james:~_[james@james james]$ exit
logout
_[H_[2JConnection to 172.16.3.47 closed. _]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
Script done on Sat Jun  5 17:03:08 2004
```

D. Test 3 : remote SSH logins as root are disabled

```
Script started on Wed May 19 05:05:23 2004
```

```
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]# ssh 172.16.3.47
The authenticity of host '172.16.3.47 (172.16.3.47)' can't be established.
RSA key fingerprint is 1d:d0:62:72:f1:0a:ca:29:41:1b:4d:bd:da:bc:71:00.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '172.16.3.47' (RSA) to the list of known hosts.
root@172.16.3.47's password:
Permission denied, please try again. root@172.16.3.47's password:
Permission denied, please try again. root@172.16.3.47's password:
Permission denied (publickey,password,keyboard-interactive).
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
_]0;root@Matrix2:~_[root@Matrix2 root]#
Script done on Wed May 19 05:07:27 2004
```

E. Test 4 : SSH v1 is not supported

To test this item, I've changed ssh_config in Client System.

Protocol 2,1

->

Protocol 1 (Only support SSH1)

```
Script started on Wed May 19 05:22:23 2004
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]# ssh_ __ __ ___
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]# ssh james@172.16.3.47
Protocol major versions differ: 1 vs. 2
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]#
_]0;root@Matrix2:/etc/ssh_[root@Matrix2 ssh]# exit
```

Script done on Wed May 19 05:22:40 2004

VII. Reference

SANS, Securing UNIX HandBook

http://www.cert.org/tech_tips/usc20_full.html, UNIX Security Checklist v2.0

http://www.openssh.com, The OpenSSH's homepages

http://www.sendmail.org, The Sendmail's homepages

Red Hat Linux Security Guide, https://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/

Red Hat Linux System Administrator Primer, https://www.redhat.com/docs/manuals/linux/RHL-9-Manual/admin-primer/

Red Hat Linux Reference Guide, https://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/

Red Hat Linux Reference Guide, https://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/

Red Hat Linux x86 Installation Guide,

http://www.xinetd.org, The xinetd webpage

http://www.cert.org, Carnegie Melon's CERT Homepage

http://www.us-cert.gov, US Computer Emergency Readiness Team Homepage

http://cve.mitre.org, Mitre's Vulnerability DB

http://rhn.redhat.com, Redhat Network's homepage

http://www.linuxsecurity.com/advisories/redhat.html, all linux OS's advisories report

http://www.yolinux.com/

http://www.tripwire.org/downloads/index.php

http://www.siliconvalleyccie.com/linux-hn/logging.htm

http://www.linux.duke.edu/projects/yum/, yum package's homepage

http://www.tripwire.com, Tripwire's homepage

http://www.nessus.org, nessus' homepage

SANS Step-by-Step Series Securing Linux Version 1.0

Jacqui Chau, Hardening a Red Hat Linux Apache Web Server with Snort Installed, 19th Dec 2003.

Mike Armstrong, Red Hat Java Application Server Step-by-Step, 15th Feb 2004

C. Cliff Liu, Secure Red Hat 9 to Run a Trouble Ticket System in Chroot Environment, 15th Mar2004

Appendix A: Vulnerability of OpenSSH

http://www.cert.org/

ID	Title	Overview	
CA-2003-24	Buffer Management Vulnerability in OpenSSH	There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7.1.	
CA-2002-36	Multiple Vulnerabilities in SSH Implementations	Multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or cause a denial of service.	
CA-2002-24	Trojan Horse OpenSSH Distribution	some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse.	
CA-2002-18	OpenSSH Vulnerabilities in Challenge Response Handling	There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3.	
CA-2002-07	Double Free Bug in zlib Compression Library	There is a bug in the zlib compression library that may manifest itself as a vulnerability in programs that are linked with zlib.	
CA-2001-35	Recent Activity Against Secure Shell Daemons	There are multiple vulnerabilities in several implementations of the Secure Shell (SSH) protocol.	
CA-1999-15	Buffer Overflows in SSH daemon and RSAREF2 Library	Some versions of sshd are vulnerable to a buffer overflow that can allow an intruder to influence certain variables internal to the program.	

CERT advisories have become a core component of US-CERT's Technical Cyber Security Alerts.

http://www.kb.cert.org/vuls/byid?searchview

ID	Date Public	Name
VU#333628	09/16/2003	OpenSSH contains buffer management errors
VU#209807	09/23/2003	Portable OpenSSH server PAM conversion stack corruption
VU#157447	12/04/2001	OpenSSH UseLogin directive permits privilege escalation
VU#602204	09/23/2003	OpenSSH PAM challenge authentication failure
VU#369347	06/24/2002	OpenSSH vulnerabilities in challenge response handling
VU#363181	12/07/2000	OpenSSH disregards client configuration and allows server access to ssh-agent and/or X11 after session negotiation
VU#408419	03/07/2002	OpenSSH contains a one-off overflow of an array in the channel handling code
VU#797027	06/19/2001	OpenSSH does not initialize PAM session thereby allowing PAM restrictions to be bypassed
VU#40327	06/09/2000	OpenSSH UseLogin option allows remote execution of commands as root
VU#978316	06/04/2003	Vulnerability in OpenSSH daemon (sshd)
VU#905795	09/27/2001	OpenSSH fails to properly apply source IP based access control restrictions
VU#655259	06/12/2001	OpenSSH allows arbitrary file deletion via symlink redirection of temporary file
VU#945216	02/08/2001	SSH CRC32 attack detection code contains remote integer overflow
VU#341187	05/21/2002	SSHD allows users to override "AllowedAuthentications" configuration thereby permitting users to provide any type of authentication
VU#886796	07/28/2003	Cisco Aironet AP1100 fails to provide universal login error messages thereby disclosing validity of user account
VU#442569	03/15/2003	MIT Kerberos vulnerable to ticket splicing when using Kerberos4

		triple DES service tickets
VU#389665	12/16/2002	Multiple vendors' SSH transport layer protocol implementations contain vulnerabilities in key exchange and initialization
VU#623217	03/15/2003	Cryptographic weakness in Kerberos Version 4 protocol
VU#684820	01/18/2001	SSH-1 allows client authentication to be forwarded by a malicious server to another server
VU#565052	01/18/2001	Passwords sent via SSH encrypted with RC4 can be easily cracked

http://cve.mitre.org/

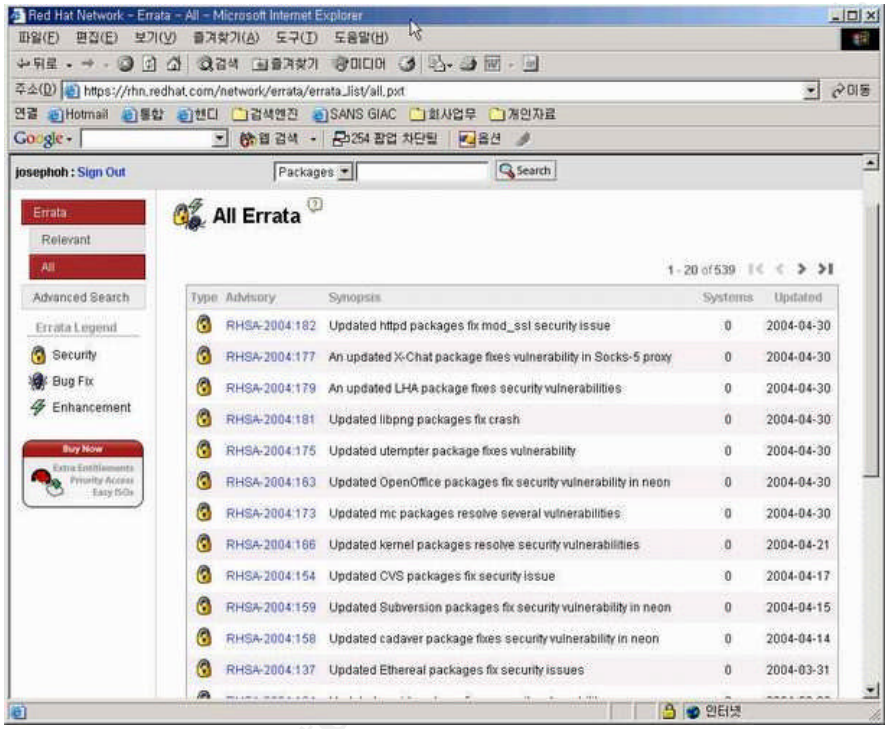
Name	Description
CVE-1999-0013	Stolen credentials from SSH clients via ssh-agent program, allowing other local users to access remote accounts belonging to the ssh-agent user.
CVE-1999-0248	A race condition in the authentication agent mechanism of sshd 1.2.17 allows an attacker to steal another user's credentials.
CVE-1999-0310	SSH 1.2.25 on HP-UX allows access to new user accounts.
CVE-1999-0787	The SSH authentication agent follows symlinks via a UNIX domain socket.
CVE-1999-1010	An SSH 1.2.27 server allows a client to use the "none" cipher, even if it is not allowed by the server policy.
CVE-1999-1085	SSH 1.2.25, 1.2.23, and other versions, when used in in CBC (Cipher Block Chaining) or CFB (Cipher Feedback 64 bits) modes, allows remote attackers to insert arbitrary data into an existing stream between an SSH client and server by using a known plaintext attack and computing a valid CRC-32 checksum for the packet, aka the "SSH insertion attack."
CVE-1999-1159	SSH 2.0.11 and earlier allows local users to request remote forwarding from privileged ports without being root.
CVE-1999-1321	Buffer overflow in ssh 1.2.26 client with Kerberos V enabled could allow remote attackers to cause a denial of service or execute arbitrary commands via a long DNS hostname that is not properly handled during TGT ticket

	passing.
CVE-2000-0217	The default configuration of SSH allows X forwarding, which could allow a remote attacker to control a client's X sessions via a malicious xauth program.
CVE-2000-0525	OpenSSH does not properly drop privileges when the UseLogin option is enabled, which allows local users to execute arbitrary commands by providing the command to the ssh daemon.
CVE-2000-0532	A FreeBSD patch for SSH on 2000-01-14 configures ssh to listen on port 722 as well as port 22, which might allow remote attackers to access SSH through port 722 even if port 22 is otherwise filtered.
CVE-2000-0575	SSH 1.2.27 with Kerberos authentication support stores Kerberos tickets in a file which is created in the current directory of the user who is logging in, which could allow remote attackers to sniff the ticket cache if the home directory is installed on NFS.
CVE-2000-0992	Directory traversal vulnerability in scp in sshd 1.2.xx allows a remote malicious scp server to overwrite arbitrary files via a .. (dot dot) attack.
CVE-2000-1169	OpenSSH SSH client before 2.3.0 does not properly disable X11 or agent forwarding, which could allow a malicious SSH server to gain access to the X11 display and sniff X11 events, or gain access to the ssh-agent.
CVE-2001-0080	Cisco Catalyst 6000, 5000, or 4000 switches allow remote attackers to cause a denial of service by connecting to the SSH service with a non-SSH client, which generates a protocol mismatch error.
CVE-2001-0144	CORE SDI SSH1 CRC-32 compensation attack detector allows remote attackers to execute arbitrary commands on an SSH server or client via an integer overflow.
CVE-2001-0155	Format string vulnerability in VShell SSH gateway 1.0.1 and earlier allows remote attackers to execute arbitrary commands via a user name that contains format string specifiers.
CVE-2001-0156	VShell SSH gateway 1.0.1 and earlier has a default port forwarding rule of 0.0.0.0/0.0.0.0, which could allow local users conduct arbitrary port forwarding to other systems.
CVE-2001-0259	ssh-keygen in ssh 1.2.27 - 1.2.30 with Secure-RPC can allow local attackers to recover a SUN-DES-1 magic phrase generated by another user, which the

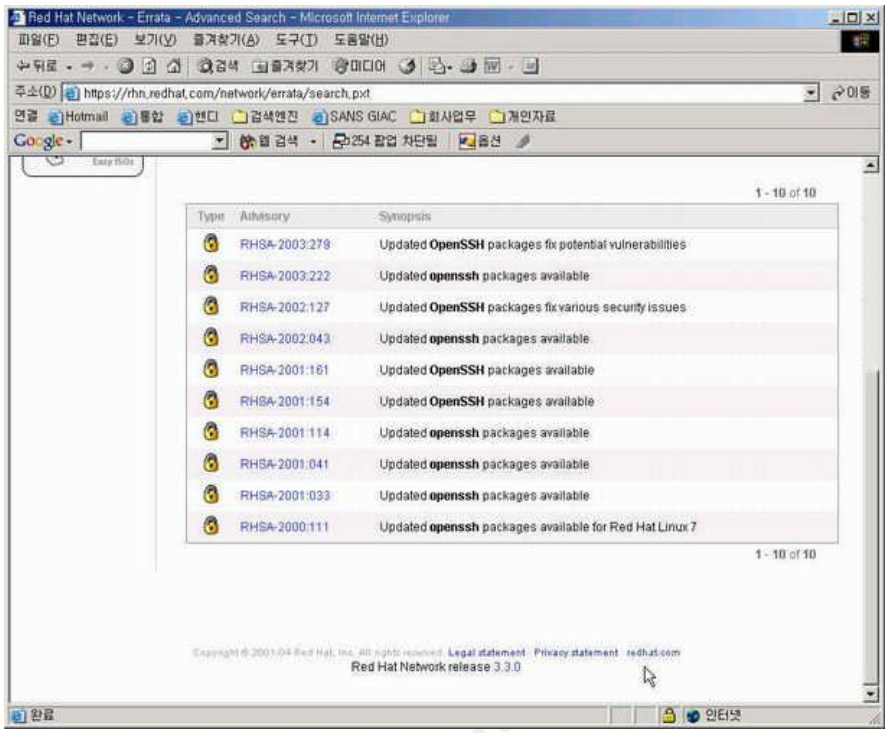
	attacker can use to decrypt that user's private key file.
CVE-2001-0361	Implementations of SSH version 1.5, including (1) OpenSSH up to version 2.3.0, (2) AppGate, and (3) ssh-1 up to version 1.2.31, in certain configurations, allow a remote attacker to decrypt and/or alter traffic via a "Bleichenbacher attack" on PKCS#1 version 1.5.
CVE-2001-0364	SSH Communications Security sshd 2.4 for Windows allows remote attackers to create a denial of service via a large number of simultaneous connections.
CVE-2001-0529	OpenSSH version 2.9 and earlier, with X forwarding enabled, allows a local attacker to delete any file named 'cookies' via a symlink attack.
CVE-2001-0553	SSH Secure Shell 3.0.0 on Unix systems does not properly perform password authentication to the sshd2 daemon, which allows local users to gain access to accounts with short password fields, such as locked accounts that use "NP" in the password field.
CVE-2001-1380	OpenSSH before 2.9.9, while using keypairs and multiple keys of different types in the ~/.ssh/authorized_keys2 file, may not properly handle the "from" option associated with a key, which could allow remote attackers to login from unauthorized IP addresses.
CVE-2002-0639	Integer overflow in sshd in OpenSSH 2.9.9 through 3.3 allows remote attackers to execute arbitrary code during challenge response authentication (ChallengeResponseAuthentication) when OpenSSH is using SKEY or BSD_AUTH authentication.
CVE-2002-0640	Buffer overflow in sshd in OpenSSH 2.3.1 through 3.3 may allow remote attackers to execute arbitrary code via a large number of responses during challenge response authentication when OpenBSD is using PAM modules with interactive keyboard authentication (PAMAuthenticationViaKbdInt).
CVE-2002-0765	sshd in OpenSSH 3.2.2, when using YP with netgroups and under certain conditions, may allow users to successfully authenticate and log in with another user's password.
CVE-2002-1024	Cisco IOS 12.0 through 12.2, when supporting SSH, allows remote attackers to cause a denial of service (CPU consumption) via a large packet that was designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144).

CVE-2002-1059	Buffer overflow in Van Dyke SecureCRT SSH client before 3.4.6, and 4.x before 4.0 beta 3, allows an SSH server to execute arbitrary code via a long SSH1 protocol version string.

http://www.redhat.com



.



Appendix B. Process of Integrity Checking by tripwire

Notice> Here is some control character(for ascii character's color) in this example. And some redundant lines was deleted. I've marked underlined and red commands at integrity checking key point processes. This is generated by 'script' command.

```
Script started on Mon 17 May 2004 12:34:30 PM KST
[root@james root]#
[root@james root]#
[root@james root]# cd /etc/tripwire
[root@james tripwire]# ls
twcfg.txt    twinstall.sh    twpol.txt
  [m[root@james tripwire]#
[root@james tripwire]# ./twinstall.sh

---------------------------------------------
The Tripwire site and local passphrases are used to
sign a variety of files, such as the configuration,
policy, and database files.

Passphrases should be at least 8 characters in length
and contain both letters and numbers.

See the Tripwire manual for more information.

---------------------------------------------
Creating key files...

(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the site keyfile passphrase:
Verify the site keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.
```

```
(When selecting a passphrase, keep in mind that good passphrases typically
have upper and lower case letters, digits and punctuation marks, and are
at least 8 characters in length.)

Enter the local keyfile passphrase:
Verify the local keyfile passphrase:
Generating key (this may take several minutes)...Key generation complete.

---------------------------------------------
Signing configuration file...
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg

A clear-text version of the Tripwire configuration file
/etc/tripwire/twcfg.txt
has been preserved for your inspection.    It is recommended
that you delete this file manually after you have examined it.


---------------------------------------------
Signing policy file...
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

A clear-text version of the Tripwire policy file
/etc/tripwire/twpol.txt
has been preserved for your inspection.    This implements
a minimal policy, intended only to test essential
Tripwire functionality.    You should edit the policy file
to describe your system, and then use twadmin to generate
a new signed copy of the Tripwire policy.

[root@james tripwire]# ls
  [00m   [00mjames-local.key   [00m            [00msite.key   [00m            [00mtw.cfg   [00m
  [00mtwcfg.txt   [00m               [01;32mtwinstall.sh   [00m               [00mtw.pol   [00m
```

```
  [00mtwpol.txt  [00m
  [m[root@james tripwire]# ls -tl
  [00mtotal 100
-rw-r-----    1 root     root         8287 May 17 12:35  [00mtw.pol  [00m
-rw-r-----    1 root     root         4586 May 17 12:35  [00mtw.cfg  [00m
-rw-r-----    1 root     root          931 May 17 12:35  [00mjames-local.key  [00m
-rw-r-----    1 root     root          931 May 17 12:35  [00msite.key  [00m
-rw-r--r--    1 root     root          603 Jan 25  2003  [00mtwcfg.txt  [00m
-rwxr-xr-x    1 root     root        10100 Jan 25  2003  [01;32mtwinstall.sh  [00m
-rw-r--r--    1 root     root        51817 Jan 25  2003  [00mtwpol.txt  [00m
  [m[root@james tripwire]#
[root@james tripwire]#
[root@james tripwire]# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /usr/sbin/fixrmtab
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /usr/bin/vimtutor
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /sbin/accton
### No such file or directory
### Continuing...
### Warning: File system error.

……..


### Warning: File system error.
### Filename: /root/.Xauthority
```

```
### No such file or directory
### Continuing...
Wrote database file: /var/lib/tripwire/james.twd
The database was successfully generated.
[root@james tripwire]#
[root@james tripwire]#
[root@james tripwire]#
[root@james tripwire]# tripwire --check | tee > /root/tripwirelog.log
### Warning: File system error.
### Filename: /root/.esd_auth
### No such file or directory
### Continuing...

……

### Warning: File system error.
### Filename: /bin/ksh
### No such file or directory
### Continuing...
[root@james tripwire]#
[root@james tripwire]#
[root@james tripwire]#
[root@james tripwire]# cd /root
[root@james root]# ls -tl | head
total 3056
-rw-r--r--    1 root     root        15475 May 17 12:45 tripwirelog.log
-rw-r--r--    1 root     root        28672 May 17 12:44 tripwire
-rw-r--r--    1 root     root      3035463 May 17 12:24 tripwire-2.3.1-17.i386.rpm
-rw-r--r--    1 root     root          934 May 17 02:35 free
-rw-r--r--    1 root     root          499 May 14 11:43 set-gid
-rw-r--r--    1 root     root          845 May 14 11:39 set-uid
-rw-r--r--    1 root     root          283 May 14 10:19 typescript
-rw-r--r--    1 root     root         1267 May 14 01:10 anaconda-ks.cfg
-rw-r--r--    1 root     root        15838 May 13 13:45 install.log
[root@james root]#
[root@james root]#
```

```
[root@james root]# twprint -m r --twrfile /var/lib/tripwire/report/james-20040517-124117.twr |
less
  [25;1H   [KNote: Report is not encrypted.
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:              root
Report created on:                Mon 17 May 2004 12:41:17 PM KST
Database last updated on:         Never

================================================================================
==========
Report Summary:
================================================================================
==========

Host name:                          james
Host IP address:                    127.0.0.1
Host ID:                            None
Policy file used:                   /etc/tripwire/tw.pol
Configuration file used:            /etc/tripwire/tw.cfg
Database file used:                 /var/lib/tripwire/james.twd
Command line used:                  tripwire --check

================================================================================
==========
Rule Summary:
================================================================================
==========

--------------------------------------------------------------------------------
  [25;1H   [K:   [25;1H   [25;1H   [K    Section: Unix File System
  [25;1H   [K:   [25;1H   [25;1H   [K--------------------------------------------------------------------------------
--
  [25;1H   [K:   [25;1H   [25;1H   [K
  [25;1H   [K:   [25;1H   [25;1H   [K    Rule  Name                                Severity  Level
Added       Removed    Modified
```

```
  [25;1H  [K:  [25;1H  [25;1H  [K  ---------                    ----------      -----
-------  --------
  [25;1H  [K:  [25;1H  [25;1H  [K  Invariant Directories          66              0
0          0
  [25;1H  [K:  [25;1H  [25;1H  [K  Critical devices               100             0
0          0
  [25;1H  [K:  [25;1H  [25;1H  [K      Temporary  directories                     33
0          0          0
  [25;1H  [K:  [25;1H  [25;1H  [K* Tripwire Data Files            100             1
0          0
  [25;1H  [K:  [25;1H  [25;1H  [K* Root config files              100             1
0          2
   User binaries                  66          0          0          0
   Tripwire Binaries              100         0          0          0
   Critical configuration files   100         0          0          0
   Libraries                      66          0          0          0
   Operating System Utilities     100         0          0          0
   Critical system boot files     100         0          0          0
   File System and Disk Administraton Programs
                                  100         0          0          0
   Kernel Administration Programs 100         0          0          0
   Networking Programs            100         0          0          0
   System Administration Programs 100         0          0          0
   Hardware and Device Control Programs
                                  100         0          0          0
   System Information Programs    100         0          0          0
   Application Information Programs
                                  100         0          0          0
   Shell Related Programs         100         0          0          0
   Critical Utility Sym-Links     100         0          0          0
   Shell Binaries                 100         0          0          0
   System boot changes            100         0          0          0
   OS executables and libraries   100         0          0          0
   Security Control               100         0          0          0
   Login Scripts                  100         0          0          0
  [25;1H  [K:  [25;1H  [25;1H  [K
```

```
Total objects scanned:    18450
Total violations found:    4

================================================================================
==========
Object Detail:
================================================================================
==========

--------------------------------------------------------------------------------
   Section: Unix File System
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
--------------------------------------------------------------------------------
   ----------------------------------------
   Added Objects: 1
   ----------------------------------------

Added object name:    /root/tripwirelog.log

   ----------------------------------------
   Modified Objects: 2
  [25;1H   [K:   [25;1H   [25;1H   [K   ----------------------------------------

Modified object name:    /root

   Property:                 Expected                        Observed
   -------------          -----------                    -----------
* Modify Time               Mon 17 May 2004 12:34:30 PM KST
                                                          Mon 17 May 2004 12:41:17 PM K
ST
* Change Time               Mon 17 May 2004 12:34:30 PM KST
                                                          Mon 17 May 2004 12:41:17 PM K
```

```
ST


Modified object name:    /root/tripwire

   Property:               Expected                    Observed
   -------------          ------------                ------------
* Size                     12288                       16384
* Modify Time              Mon 17 May 2004 12:39:20 PM KST
                                                      Mon 17 May 2004 12:39:37 PM K
ST
* Change Time              Mon 17 May 2004 12:39:20 PM KST
                                                      Mon 17 May 2004 12:39:37 PM K
  [25;1H   [K:   [25;1H   [25;1H   [KST
* Blocks                   24                          32
* CRC32                     BcPbjL                      AAxasp
*    MD5                                                 DfegiyCMBQ30PpcEKPjhO5
DbJ4BcyCCLcZsDXaIm3kU2



--------------------------------------------------------------------------------
Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100
--------------------------------------------------------------------------------
   ---------------------------------------
   Added Objects: 1
   ---------------------------------------

Added object name:    /var/lib/tripwire/james.twd.bak

================================================================================
==========
Error Report:
================================================================================
==========
```

Section: Unix File System

[25;1H [K: [25;1H [25;1H [K

1. File system error.
   Filename: /root/.esd_auth
   No such file or directory

……..

111. File system error.
   Filename: /bin/zsh-4.0.2
   No such file or directory
112. File system error.
   Filename: /bin/ksh
[25;1H [K: [25;1H [25;1H [K No such file or directory

*** End of report ***

[25;1H [K [7m(END) [27m [25;1H [25;1H [K [25;1H [K [7m(END)
[27m [25;1H [25;1H [K [25;1H [K [7m(END)
[27m [25;1H [25;1H [K [25;1H [K [7m(END) [27m [25;1H [K[root@james root]# twprint -m r --twrfile /var/lib/tripwire/report/james-200405517-124117.twr | less [K [K [K [K [K [K> /root/tw [Kripwire.report
[root@james root]#
[root@james root]#
[root@james root]# cd /root
[root@james root]# ls -tl|head
total 3096

```
-rw-r--r--    1 root     root        16869 May 17 12:49 tripwire.report
-rw-r--r--    1 root     root        49152 May 17 12:49 tripwire
-rw-r--r--    1 root     root        15475 May 17 12:45 tripwirelog.log
-rw-r--r--    1 root     root      3035463 May 17 12:24 tripwire-2.3.1-17.i386.rpm
-rw-r--r--    1 root     root          934 May 17 02:35 free
-rw-r--r--    1 root     root          499 May 14 11:43 set-gid
-rw-r--r--    1 root     root          845 May 14 11:39 set-uid
-rw-r--r--    1 root     root          283 May 14 10:19 typescript
-rw-r--r--    1 root     root         1267 May 14 01:10 anaconda-ks.cfg
[root@james root]# vi tripwire.report
  [1;25r [?25h [?8c [?25h [?0c [27m [24m [0;10m [H [J [?25l [?1c [25;1H"tripwir
e.report" 471L, 16869C  [1;1HNote: Report is not encrypted.
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:  [4;31Hroot
Report created on:  [5;31HMon 17 May 2004 12:41:17 PM KST
Database last updated on:       Never

==========================================================================
==========
Report Summary:
==========================================================================
==========

Host name:  [12;31Hjames
Host IP address:  [13;31H127.0.0.1
Host ID:  [14;31HNone
Policy file used:  [15;31H/etc/tripwire/tw.pol
Configuration file used:        /etc/tripwire/tw.cfg
Database file used:  [17;31H/var/lib/tripwire/james.twd
Command line used:  [18;31Htripwire --check

==========================================================================
==========
Rule Summary:
==========================================================================
```

```
==========

---------- [1;1H [?25h [?0c



 [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HSection: Unix File System
 [?25h [?0c [25;1H [K [?25l [?1c [1;24r [24;1H
 [1;25r [24;1H----------
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;1H [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HRule Name [24;35HSeverity Level Added Removed Modified
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3H--------- [24;35H---------- ----- ------- --------
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HInvariant Directories [24;35H66 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HCritical devices [24;35H100 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HTemporary directories [24;35H33 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;1H* Tripwire Data Files [24;35H100 [24;53H1 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;1H* Root config files [24;35H100 [24;53H1 [24;62H0 [24;71H2
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HUser binaries [24;35H66 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HTripwire Binaries [24;35H100 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HCritical configuration files 100 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HLibraries [24;35H66 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
 [1;25r [24;3HOperating System Utilities 100 [24;53H0 [24;62H0 [24;71H0
 [?25h [?0c [?25l [?1c [1;24r [24;1H
```

```
  [1;25r  [24;3HCritical system boot files          100  [24;53H0  [24;62H0  [24;71H0
  [?25h  [?0c  [?25l  [?1c  [1;24r  [24;1H
  [1;25r  [24;3HFile System and Disk Administraton Programs
  [?25h  [?0c  [?25l  [?1c  [1;24r  [1;1H  [12M  [1;25r  [13;35H100  [13;53H0  [13;62H0
[13;71H0
   Kernel Administration Programs   100  [14;53H0  [14;62H0  [14;71H0
   Networking Programs  [15;35H100  [15;53H0  [15;62H0  [15;71H0
   System Administration Programs   100  [16;53H0  [16;62H0  [16;71H0
   Hardware and Device Control Programs  [18;35H100  [18;53H0  [18;62H0  [18;71H0
   System Information Programs        100  [19;53H0  [19;62H0  [19;71H0
   Application Information Programs  [21;35H100  [21;53H0  [21;62H0  [21;71H0
   Shell Related Programs  [22;35H100  [22;53H0  [22;62H0  [22;71H0
   Critical Utility Sym-Links         100  [23;53H0  [23;62H0  [23;71H0
   Shell Binaries  [24;35H100  [24;53H0  [24;62H0  [24;71H0
    [?25h  [?0c  [?25l  [?1c  [1;24r  [1;1H  [12M  [1;25r  [13;3HSystem                boot
changes  [13;35H100  [13;53H0  [13;62H0  [13;71H0
   OS executables and libraries      100  [14;53H0  [14;62H0  [14;71H0
   Security Control  [15;35H100  [15;53H0  [15;62H0  [15;71H0
   Login Scripts  [16;35H100  [16;53H0  [16;62H0  [16;71H0

Total objects scanned:   18450
Total violations found:   4

================================================================
==========
Object Detail:
================================================================
==========
  [?25h  [?0c  [?25l  [?1c  [1;24r  [1;1H  [12M  [1;25r  [13;1H----------------------------------
----------------------------------------
   Section: Unix File System
--------------------------------------------------------------------------------


--------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
```

```
---------------------------------------------------------------------------
   ----------------------------------------
   Added Objects: 1
   ----------------------------------------
  [?25h [?0c [?25l [?1c [1;24r [1;1H [12M [1;25r [13;1HAdded object name:
/root/tripwirelog.log

   ----------------------------------------
   Modified Objects: 2
   ----------------------------------------

Modified object name:  /root

   Property:  [21;24HExpected  [21;52HObserved
   ------------  [22;24H----------  [22;52H----------
* Modify Time  [23;24HMon 17 May 2004 12:34:30 PM KST  [24;52HMon 17 May 2004
12:41:17 PM K [24;1H [1m [34m@
  [23;1H  [?25h  [?0c  [?25l  [?1c  [1;24r  [0;10m  [1;1H  [12M  [1;25r  [12;1H
Mon 17 May 2004 12:41:17 PM K  [13;1HST
* Change Time  [14;24HMon 17 May 2004 12:34:30 PM KST  [15;52HMon 17 May 2004
12:41:17 PM K  [16;1HST


Modified object name:  /root/tripwire

   Property:  [21;24HExpected  [21;52HObserved
   ------------  [22;24H----------  [22;52H----------
* Size  [23;24H12288  [23;52H16384
* Modify Time  [24;24HMon 17 May 2004 12:39:20 PM KST
  [?25h  [?0c  [?25l  [?1c  [1;24r  [1;1H  [11M  [1;25r  [14;52HMon  17  May  2004
12:39:37 PM K  [15;1HST
* Change Time  [16;24HMon 17 May 2004 12:39:20 PM KST  [17;52HMon 17 May 2004
12:39:37 PM K  [18;1HST
* Blocks  [19;24H24  [19;52H32
* CRC32  [20;24HBcPbjL  [20;52HAAxasp
* MD5  [21;24HDfegiyCMBQ30PpcEKPjhO5          DbJ4BcyCCLcZsDXaIm3kU2
```

[?25h [?0c [?25l [?1c [1;24r [1;1H [12M [1;25r [13;1H----------
---

Rule Name: Tripwire Data Files (/var/lib/tripwire)

Severity Level: 100

Added Objects: 1

Added object name: /var/lib/tripwire/james.twd.bak

==========

Error

Report: [22;1H [?25h [?0c [?25l [?1c [1;24r [1;1H [12M [1;25r [13;1H=========
==========
=

Section: Unix File System

---

1. File system error. [20;6HFilename: /root/.esd_auth [21;6HNo such file or directory
2. File system error. [23;6HFilename: /root/.gnome_private [24;6HNo such file or directory [20;6H [?25h [?0c [?25l [?1c [1;24r [1;1H [12M [1;25r [13;1H3. File system error. [14;6HFilename: /root/.gnome-desktop [15;6HNo such file or

……

45. File system error. [20;6HFilename: /var/lock/subsys/bcm5820 [21;6HNo such file or directory
46. File system error. [23;6HFilename: /var/lock/subsys/bgpd [24;6HNo such file or directory [20;6H [?25h [?0c [?25l [?1c [25;1H: [?25h [?0cq
[?25l [?1c [?25h [?0c [25;1H [K [25;1H[root@james root]#

```
[root@james root]#
[root@james root]# ls -tl
  [00mtotal 3112
-rw-r--r--       1 root        root             61440 May 17 12:49    [00mtripwire   [00m
-rw-r--r--       1 root        root             16869 May 17 12:49    [00mtripwire.report   [00m
-rw-r--r--       1 root        root             15475 May 17 12:45    [00mtripwirelog.log   [00m
-rw-r--r--        1   root          root           3035463   May   17   12:24     [01;31mtripwire-2.3.1-
17.i386.rpm   [00m
-rw-r--r--       1 root        root               934 May 17 02:35    [00mfree   [00m
-rw-r--r--       1 root        root               499 May 14 11:43    [00mset-gid   [00m
-rw-r--r--       1 root        root               845 May 14 11:39    [00mset-uid   [00m
-rw-r--r--       1 root        root               283 May 14 10:19    [00mtypescript   [00m
-rw-r--r--       1 root        root              1267 May 14 01:10    [00manaconda-ks.cfg   [00m
-rw-r--r--       1 root        root             15838 May 13 13:45    [00minstall.log   [00m
-rw-r--r--       1 root        root              3865 May 13 13:44    [00minstall.log.syslog   [00m
  [m[root@james root]# ls -tl     [K     [K     [K     [K     [K     [K   e     [Kexit

Script done on Mon 17 May 2004 12:50:14 PM KST
```