



2001.1.16.  
Copyright (c) 2001 by Clunix, Inc.

\* ( )  
\*

---

- ☞ 1. Linux
- ☞ 1.1 Linux
- ☞ 1.2
- ☞ 1.3
- ☞ 2.
- ☞ 2.1
- ☞ 2.2 SUDO - root
- ☞ 2.3 TCP\_WRAPPER
- ☞ 2.4 SSH - Network Sniffing
- ☞ 2.5 SCAN DETECT
- ☞ 2.6 Libsafe and ETC - Stack Buffer Overflow Attack
- ☞ 2.7 IPSEC VPN
- ☞ 2.8 Host IDS
- ☞ 2.9 Network IDS
- ☞ 2.10 Firewall
- ☞ 3.

---

## 1. Linux

### 1.1 Linux

위로

가 , Linux 가  
가 , 가 가 가 ,  
가 ,

가

(Linux)  
/

가

MS-DOS

, 가

가

, 가

가

?

## 1.2

위도

3가

A.

.

가

(sniffing)

(ethernet)

가  
LAN

가

(wire)

가

"PROMISCUOUS"

가

username

가

가

(scanning)

B.

C.

가 가

### 1.3

위로

(1)

. 가 210.33.\*.\* \*.co.kr

가  
(firewall)

, 가

가

ping

DNS

가

queso, nmap

"IP stack

IP

fingerprinting"

sscan, mscan  
(daemon)

ftpd, telnetd

가

ICMP

firewalk, hping

(2)

가

가 가

(1)

Linux

가 wu-ftpd  
(remote exploit)  
passwd

(buffer overflow) 가  
wu-ftpd (exploit)

, 가

passwd

, crack

rootkit

(3)

(broadcasting)

sniff  
(login)

rlogin, rsh

r-service

(4) 가

K R

R

R

K

sscan

rscan

nmap

10

B가

buffer overflow  
telnet

, sniffer

, rootkit

B

B

B

TFN2k

DoS(Denial of Service)

R

## 2.

### 2.1

위로

(1) init

init AT&T System V , (daemon)  
. MS ,  
(runlevel) .

init .

- : 가 가 .  
- : 가 .  
- : 가 .

\*

(Slackware) BSD init (RedHat),  
(Mandrake), (SuSE), (Caldera) System V init .

## (2) init.d

init.d (daemon) 가  
/etc/rc.d/init.d .

inetd "start" "stop"  
:

/etc/rc.d/init.d/inetd start

, inetd :

/etc/rc.d/init.d/inetd stop

## (3) (runlevel)

Runlevel 0:

Runlevel 1:

Single User mode .

Runlevel 2:

(named, nfs ) 가 .

Runlevel 3:

가 .

Runlevel 4:

3 X 가 가 (Slackware) 4

Runlevel 5:

가 , X 가 .

Runlevel 6:

(4)

init /etc/inittab

LILO:

(default runlevel) /etc/inittab

id:3:initdefault:

id: 가 .

\*

0 6 .

LILO:

LILO: image runlevel

image linux , runlevel

init runlevel

runlevel .

\*

1 가

(5)

init.d 가 가

/etc/rc.d/rc0.d  
/etc/rc.d/rc1.d  
/etc/rc.d/rc2.d  
/etc/rc.d/rc3.d  
/etc/rc.d/rc4.d

/etc/rc.d/rc5.d  
/etc/rc.d/rc6.d

```

S      가      가      가      .
K      .      .

start list(S      init가      kill list(K      )

      .      S      K      lpd
      .      가      init.d
      3      가

```

ln -s /etc/rc.d/init.d/lpd /etc/rc.d/rc3.d/S99lpd

. S lpd , . .

S85gpm -> K85gpm  
S90xfs -> K90xfs  
S99linuxconf -> K99linuxconf  
S60lpd -> K60lpd  
S45pcmcia -> K45pcmcia

```

      .      gpm      X      가      exploit      gpm
      가      root
xfs X      .      X      가      가      .
      linuxconf      linuxconf      가      , lpd
      가      .      pcmcia

```

### (5) PATCH

```

RedHat      RedHat
RedHat      : http://www.redhat.com/apps/support/updates.html
rpm
# rpm -Uvh

```

### (3) inetd.conf

```

inetd      internet super- server      .      inetd      /etc/rc.local
      .      internet socket      .      inetd
      /etc/inetd.conf      가      .
      /etc/inetd.conf      #

```

service name

socket type  
protocol  
wait/nowait[.max]  
user[.group]  
server program  
server program arguments

ftp, telnet . telnet 가  
ssh . ftp tcp\_wrapper

(4) root forwarding 가 root 가 root  
가 root  
가 root  
/etc/mail/aliases /etc/aliases

root: admin@test.test.co.kr

newaliases sendmail

가 sendmail pid가 4039 ,  
kill -HUP 4039 sendmail ,  
#/etc/rc.d/init.d/sendmail restart sendmail service

root admin@test.test.co.kr

(5) kernel variable

/etc/sysctl.conf 가

a. net.ipv4.tcp\_syncookies

CONFIG\_SYNCOOKIES 가 SYN  
가 syncookie . SYN flooding .  
FALSE .  
SYN flooding 가 . 가

net.ipv4.tcp\_max\_syn\_backlog

SYN 가  
가 128 , 가 200 가 256

b. net.ipv4.icmp\_echo\_ignore\_all

ICMP ECHO . 가

c. net.ipv4.icmp\_echo\_ignore\_broadcasts

ICMP ECHO .  
, IDC(Internet Data Center) .

## 2.2 sudo - root

위로



(1) sudo

UNIX root 가 . root  
UNIX 가 root , , ,  
root , su root가 . 가  
su sudo .  
root passwd , root 가 root  
root가 . root shell  
가 . sudo root filesystem rm - rf  
root  
log . su root 가 , su root가  
. sudo command logging 가  
가 . root 가 ' 가  
. sudo  
shell sudo . ps w command root  
shell root shell . 가 root  
sudo 가 가 sudo sudoers 가  
root shell  
root sudo 가 , sudo 가

(2) sudo

sudo sudo가 .  
가 sudo ,  
sudo가 , sudoers . /etc/sudoers  
가 sudoers  
visudo 가 .

```

sudo /etc/sudoers , 가 sudo
visudo , visudo .

$ visudo

/etc/sudoers ..
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for the details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL) ALL
stevens ALL=(ALL) ALL

user stevens sudo command . sudoers

```

```

dgb boulder = (operator) /bin/lis, (root) /bin/kill, /usr/bin/lprm
, dgb operator ls , root kill lprm

```

```

$ sudo -u operator /bin/lis
sudo command
$ sudo command [argument]
) sudo vi /etc/passwd

```

```

password : ***** <== root 가
root /etc/passwd

```

## 2.3 TCP\_WRAPPER 위로

(1)

```

(tcp_wrapper) SYSTAT, FINGER, FTP, TELNET, RLOGIN,
RSH, EXEC, TFTP, TALK (request)
. 4.3BSD-style socket System V4-style TLI . (inetd.conf)
) 가 가
가
tcp_wrapper ,
inetd.conf root .

```

syslogd

가

(2) wrapper

client program(telnet) - - - - server(in.telnetd) - - - - application(remote login)  
client program(ftp) - - - - server(in.ftpd) - - - - application(file transfer)

telnetd ftpd telnet ftp (protocol)  
server tcp wrapper client 가 가  
log service tcpd( wrapper) overhead가

client(ftp) - - - - tcp wrapper(tcpd) - - - - server(in.ftpd)

(3)

tcpd 가 client 가  
NFS

(4)

/etc/inetd.conf

ftpd dgram udp wait root /usr/sbin/in.ftpd in.ftpd -s /ftpdboot  
tcpd dgram udp wait root /usr/sbin/tcpd in.tcpd -s /tcpdboot

tcpd syslogd log가 /etc/syslog.conf  
log 가 , console @loghost mail

(5) hosts.allow, hosts.deny

hosts.allow , hosts.deny

% vi hosts.allow

/etc/inetd.conf

# , /etc/inetd.conf hosts.allow (line)

/etc/hosts.allow

ALL , DNS name ip address EXCEPT

)

telnetd: ALL \  
EXCEPT 192.168.10. \  
192.168.12.50 \  
192.168.12.51 \  
192.168.11.10

hosts.allow , hosts.deny , hosts.allow EXCEPT

```
% cat hosts.deny
```

```
ALL: ALL : (/usr/sbin/safe_finger -l %@%h | /usr/bin/mail -s %d -%h root ) &
```

```
hosts.deny      hosts.allow      finger      finger
safe_finger     . safe_finger    . safe_finger
가
```

```
hosts.deny      safe_finger      ,
(root)
```

```
hosts.allow  hosts.deny      /etc
```

```
% cp hosts.allow /etc
```

```
% cp hosts.deny /etc
```

```
(6) inetd.conf
```

```
inetd.conf      wrapper      ,
wrapper
```

#ftp	stream	tcp	nowait	root	/usr/sbin/ftpd	ftpd
#telnet	stream	tcp	nowait	root	/usr/sbin/telnetd	telnetd
#shell	stream	tcp	nowait	root	/usr/sbin/rshd	rshd
#login	stream	tcp	nowait	root	/usr/sbin/rlogind	rlogind
#exec	stream	tcp	nowait	root	/usr/sbin/rexecd	rexecd
#						
ftp	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/ftpd
telnet	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/telnetd
shell	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/rshd
login	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/rlogind
exec	stream	tcp	nowait	root	/usr/sbin/tcpd	/usr/sbin/rexecd

```
Wrapper      , #
/usr/sbin/ftpd      /usr/sbin/tcpd (/usr/sbin/tcpd가 )
```

```
(7) tcpdchk      configuration
```

```
wrapper      tcpdchk
```

```
% tcpdchk
```

```
가
```

```
(8) tcpdmatch      configuration
```

```
tcpdmatch
```

```
usage: tcpdmatch [-d] [-i inet_conf] daemon[@host] [user@]host
-d: use allow/deny files in current directory
-i: location of inetd.conf file
```

```
% tcpdmatch ftpd angel.test.co.kr
client:  hostname angel.test.co.kr
client:  address 192.168.14.53
server:  process ftpd
```

```
matched: /etc/hosts.allow line 39
access: granted
```

```
%tcpdmatch telnetd devil.test.co.kr
client: hostname devil.test.co.kr
client: address 192.168.12.51
server: process telnetd
matched: /etc/hosts.deny line 17
command: (/usr/bin/safe_finger -l @%h | /usr/bin/mail -s %d-%h root ) &
access: denied
```

(9) inetd

```
ps          pid          .          inetd          wrapper가          .
% ps -u root | grep inetd
388 ?? | 0:08.56 /usr/sbin/inetd
HUP(hangup)          .
% kill -HUP 388
```

(10)

devil.test.co.kr . 가 가 /var/log/secure

## 2.4 ssh - Network Sniffing

위로

(1) Network Sniffing ?

(broadcasting media) (ethernet) 가 .
Internet Protocol , 가
, . 가
가 가 , .
가 가 , 가 가
, 가 , plain text 가
, , , sniffing

(2) sniffing

, .
가 200 , 가
, sniffing

가 telnet service, ftp service (login)  
 가 plain text  
 가 ,  
 (exploit)  
 E-mail , NFS 가

sniffing Tcpdump, Sniffit, Hunt, DSniff , MS  
 가 .

(3)

ethernet broadcasting network media  
 Switching Hub , broadcasting 가  
 가 .  
 sniffing .  
 ethernet hub , 가  
 encapsulate 가 .

(3-1) SSH

encrypt telnet, ftp, rsh, rlogin SSH가 . SSH Secure  
 SHell rsh , telnet, ftp, rsh, rlogin,  
 rcp .

SSH non-commercial use only 가 . 1 2  
 가 , encrypt 가 . SSH DES RSA / 가 . telnet

ssh rsh(rlogin) scp rcp .가 ping  
 steven login , .

\$ssh ping -l steven

PASSWORD:\*\*\*\*\*

\* URL : <http://www.ssh.com>

\* : Licence rpm package .  
 URL configure; make; make install .

(3-2) OpenSSH

가 SSH , OpenBSD  
 ( <http://www.openbsd.org> ) OpenSSH가 . SSH

. ( SSH가 redhat .)

SSH .

\* URL : <http://www.openssh.com>

\* : rpm OpenSSH(OpenSSH .  
 OpenBSD Project .) rpm .

) # rpm -Uvh openssl-0.9.5a-1.i386.rpm

openssh , openssh-server openssh-clients .

```
) # rpm -Uvh openssh-2.1.1p4-1.i386.rpm
#rpm -Uvh openssh-server-2.1.1p4-1.i386.rpm
#rpm -Uvh openssh-clients-2.1.1p4-1.i386.rpm
```

### (3-3) scp : ftp

scp SSH OpenSSH rcp , /  
가 ftp . ssh/scp 가

\*

```
$scp ./testfile steven@somehost:/home/steven/
PASSWORD:*****
```

testfile somehost steven

### (3-4) host key generation

host key가 host key .

RSA key generation

```
#ssh-keygen -f /etc/ssh/ssh_host_key
```

DSA key generation

```
#ssh-keygen -d -f /etc/ssh/ssh_host_dsa_key
```

### (4) ssh

ssh ftp, telnet, rlogin, rsh .  
host key identification 가 host ip .  
POP mail service password가 , SSL .

## 2.5 Scan Detect Daemon 위로

### (1) scan detect

(scanning tool) .

pscan , sscan 가 TCP (port) 가 , web, cgi, 가 ,

가 (scanning detect tools)가

가

scanlogd scandetd 가 .

### (2) Scan Detect Tools test

## Scanlogd

<http://www.openwall.com/scanlogd/>

1.

= dependency =

libpcap - 0.5.2.tar.gz

<http://www.tcpdump.org>

./configure;make;make install

sudo mkdir /usr/local/include; sudo mkdir /usr/local/include/net

make install-incl ; make install-man

libnet

<http://www.packetfactory.net/Projects/Libnet/>

./configure;make;make install

libnids

<http://www.packetfactory.net/Projects/Libnids/>

./configure;make;

chmod u+x mkinstalldirs

make install

scanlogd - 2.1

make libnids

cp scanlogd.8 /usr/local/man/man8

useradd scanlogd

=> login

cp scanlogd /usr/local/sbin

2.

scanlogd &

3.

가.

```
scanlogd      scan      syslog      . syslog
demon.alert   , /etc/syslog.conf
```

```
deamon.alert  /var/log/alert
```

```
audit tool    guard   , scanlogd 가      scanning      .      , log
              scanlogd      mail
```

4.

```
atropos      tarzan      nmap
. ( tarzan   scanlogd 가      . ) nmap      가      port scan
. 가      connect()      , SYN scan , Stealth scan
```

```
*****
=      scan.
*****
```

```
[k09@atropos: ~ ]nmap-sT tarzan
```



```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on tarzan.test.co.kr (192.168.12.10):
(The 1515 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
111/tcp   open       sunrpc
113/tcp   open       auth
515/tcp   open       printer
946/tcp   open       unknown
1024/tcp  open       kdm
```

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

tarzan scanning 가 .

```
tarzan]$ sudo tail /var/log/messages
Sep  6 19:14:18 tarzan scanlogd: 192.168.12.10 to 192.168.12.11 ports 80, 587, 3
74, 734, 473, 862, ..., f??p?uxy, TOS 00, TTL 64 @19:14:18
```

```
*****
= SYN scanning.
*****
```

[k09@atropos:/usr/local/man]sudo nmap -sS tarzan

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on tarzan.test.co.kr (192.168.12.10):
(The 1515 ports scanned but not shown below are in state: closed)
Port      State      Service
1024/tcp  open       kdm
. (      ).
```

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

```
[tarzan] tail /var/log/message
Sep  6 19:26:04 tarzan scanlogd: 192.168.12.10:63539 to 192.168.12.11 ports 41,
73, 481, 709, 26208, 1392, 929, ..., fSrpauxy, TOS 00, TTL 45 @19:26:04
```

가 .

```
*****
= Stealth scanning
*****
```

pos:/usr/local/man]nmap -sF tarzan

.. ( )

```
Sep  6 19:31:52 tarzan scanlogd: 192.168.12.10 to 192.168.12.11 ports 515, 22, 1
7007, 26208, 154, 3049, 812, ..., Fsrpauxy, TOS 00, TTL 44 @19:31:52
```

<http://wizard.ae.krakow.pl/~mike/download/scandetd-1.1.3.tar.gz>

1.

```
gunzip -c scandetd-1.1.3.tar.gz | tar xvf -
cd scandetd-1.1.3
make
make install
```

2.

```
( rpm package 가 source 가 test . )
config.h scan 가 .
, syslog local2.notice log message , root@localhost
, root mail forwarding , /etc/syslog.conf 가
.
```

```
local2.notice /var/log/scandetd_log
```

```
#touch /var/log/scandetd_log
```

3.

```
가
nmap 가
*****
= scanning
*****
```

```
[k09@atropos:/usr/local/man]nmap -sT tarzan
```

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

```
Interesting ports on tarzan.test.co.kr (192.168.12.10):
```

```
(The 1515 ports scanned but not shown below are in state: closed)
```

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
111/tcp	open	sunrpc
113/tcp	open	auth
515/tcp	open	printer
946/tcp	open	unknown
1024/tcp	open	kdm

```
Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

```
#tail /var/log/scandetd_log
```

```
Sep 6 20:28:38 tarzan scandetd: www connection attempt from atropos.test.co.kr
Sep 6 20:28:39 tarzan scandetd: port 681 connection attempt from atropos.test.co.kr
Sep 6 20:28:39 tarzan scandetd: port 135 connection attempt from atropos.test.co.kr
Sep 6 20:28:39 tarzan scandetd: port 402 connection attempt from atropos.test.co.kr
Sep 6 20:28:39 tarzan scandetd: port 1530 connection attempt from atropos.test.co.kr
Sep 6 20:28:39 tarzan scandetd: port 39 connection attempt from atropos.test.co.kr
```

```
root@localhost
```

```
Possible port scanning from atropos.test.co.kr,
I've counted 1009 connections.
```

First connection was made to 80 port at Wed Sep 6 20:37:35 2000  
Last connection was made to 5236 port at Wed Sep 6 20:37:50 2000

Probably it was SYN scan (0 FIN flags and 1009 SYN flags)

\*\*\*\*\*  
= Stealth scanning  
\*\*\*\*\*

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )  
Interesting ports on tarzan.test.co.kr (192.168.12.10):  
(The 1515 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
111/tcp	open	sunrpc
113/tcp	open	auth
515/tcp	open	printer
946/tcp	open	unknown
1024/tcp	open	kdm

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds

detect .

Possible port scanning from atropos.test.co.kr,  
I've counted 1401 connections.

First connection was made to 80 port at Wed Sep 6 20:38:56 2000  
Last connection was made to 205 port at Wed Sep 6 20:42:19 2000

Probably it was FIN stealth scan (1400 FIN flags and 1 SYN flags)

( stealth Port random 가 . )

(3)

scanlogd , scandetd scanning tool ,  
scanlogd mail , scanning guard detect ,  
log auditing tool  
scandetd 가 .

## 2.6 libsafe - Stack Buffer Overflow Attack

위로

(1) stack buffer overflow attack ?

buffer overflow attack , shell code root shell stack buffer  
process suid ,  
strcpy, strcat, sprintf, gets 가 .  
C , C 가

(2)

, DoS(Denial of Service)  
 가 , stack buffer overflow가 .  
 (2000 ) RedHat Linux, S.u.S.E Linux, FreeBSD wu-  
 ftpd 가 , SunOS statd , qpopper  
 imapd .

(3)

가 가 가 가 가 .  
 가 가 가 .  
 가 , 가가 .  
 가 가 .  
 가 , suid가 가 root suid  
 가 .  
 2 StackGuard . StackGuard 가 , StackGuard  
 StackGuard , StackGuard

(4)

, Libsafe  
 Libsafe가 . libsafe Bell Labs  
 ( <http://www.bell-labs.com/org/11356/libsafe.html> ) libsafe library 가  
 strcpy, scanf, sprintf . printf  
 , libsafe sprintf .  
 가 libsafe Linux, FreeBSD ld.so LD\_PRELOAD  
 . 가 bash  
 export LD\_PRELOAD=/lib/libsafe.so.1  
 libsafe . csh, tcsh setenv  
 LD\_PRELOAD /lib/libsafe.so.1 .  
 가 /var/log/secure 가

```
Dec 21 13:57:40 denver libsafe[15704]: Detected an
attempt to write across stack boundary.
Dec 21 13:57:40 denver libsafe[15704]: Terminating
/users/ttsai/work/security.DO_2/test/t91
Dec 21 13:57:40 denver libsafe[15704]: scanf()
```

libsafe  
가 , 가 , 가 ,  
가 가 Bell Labs  
.

#### (4.1) Libsafe

\* libsafe licence : LGPL

```
rpm libsafe-1.3-4.i386.rpm  
#rpm -Uvh --nodeps libsafe-1.3-4.i386.rpm  
가 , --nodeps  
rpm , dependency가 version 1.3-4,  
가  
 , export LD_PRELOAD=/lib/libsafe.so.1 rc  
csh setenv LD_PRELOAD /lib/libsafe.so.1  
LD_PRELOAD /etc/ld.so.preload /lib/libsafe.so.1  
가 ,  
가 libsafe.so.1 ,  
가 /etc/가
```

#### (5) Libsafe

```
libsafega 가 wu-ftpd 2.6.0 libsafe ,  
libsafega  
ftpd 가 libsafega snprintf() vnprintf  
()가 ,  
libsafe , buffer overflow attack  
libsafega  
libsafe.1.3 , Bell Labs
```

Intel x86 Pentium III 600Mhz  
RedHat 6.2  
wu-ftpd 2.6.0

#### (6)

```

stack
가 SunMicrosystems Solaris8 /etc/system configuration
set noexec_user_stack = 1 stack
openwall project Linux kernel patch가
( http://www.openwall.com/linux/ )
linux-2.2.17-ow1.tar.gz 가 가
2.2.17
Linux 2.2.17 가 /usr/src/linux 가
cd /usr/src/linux ( <== /usr/src/linux .)
patch -p1 < ~/linux/linux2.2.17-ow1/linux-2.2.17-ow1.diff
( <== 2.2.17 .)
kernel configuration Security options
kernel build
/etc/syslog.conf 가
kern.alert /var/log/alert

```

(6.1)

(dynamically shared) 가  
가

(7)

Stack Buffer Overflow 가  
, suid가 가 libsafe

## 2.7 IPsec & VPN 위도

VPN(Virtual Private Network) , IPsec IPsec  
VPN

(1) IPsec

IPsec(IP Security) IP(Internet Protocol)

SSL(Secure Socket Layer) IPsec . SSL IPsec 가  
TCP/IP , IPsec IP .  
, SSL SSL

IPsec IP IPsec

IPSec (subnet) (transport mode) (tunnel mode),  
VPN(Virtual Private Network) IPsec 가

HOST - HOST  
HOST - NETWORK  
NETWORK - NETWORK

(2) IPsec

IP IPsec

가 , 가 ( )

가 , 가 가 가 가

(3) AH, ESP

IPsec AH ESP 가

IPsec ESP(Encapsulated security payload) ESP IP ESP IP  
, ESP ESP

AH(Authentication Header) IP IP AH  
(data) AH

(4) IPsec

IPsec 가 (gateway)  
가

⚡ (transport) 가 AH IP  
IPsec

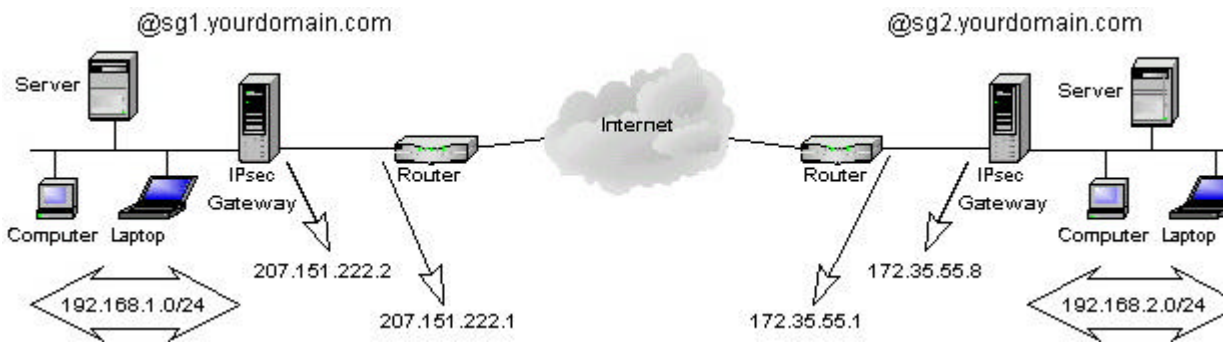
, ESP IP (transport layer)  
 (tunnel) IPsec VPN (gateway)  
 , AH ESP VPN 가  
 IP 가 , IPsec IP-in-IP 가

(5) IPsec

a. subnet-subnet

LAN VPN 192.168.1.0/24 ( )  
 A A B ) 192.168.2.0/24 ( B )  
 A B 207.151.222.2 172.35.55.8 IPsec

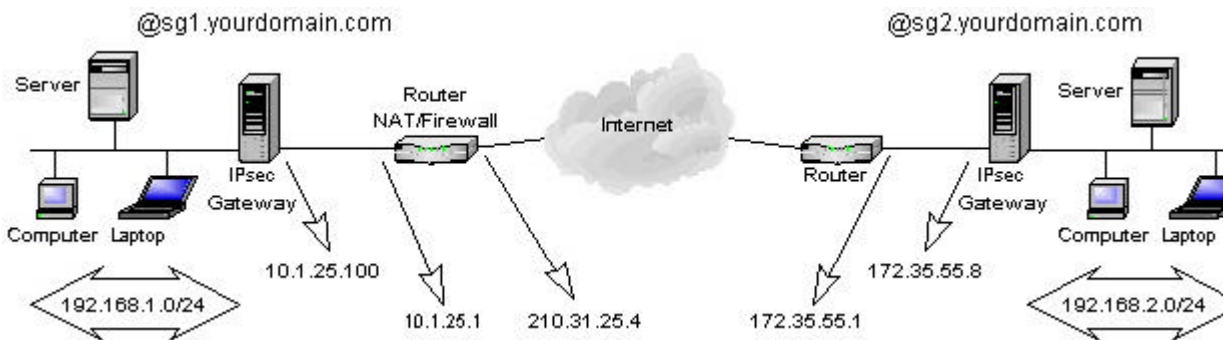
A A IPsec  
 , A B B IPsec  
 가 A B IPsec



( 1 )

b. subnet-subnet ( )

A A IPsec 가  
 A 10.1.25.100 IPsec 가  
 210.31.25.4 , IP 가 10.1.25.1  
 AH , IP ESP IP 가 210.31.25.4



( 2 )

c. client-subnet

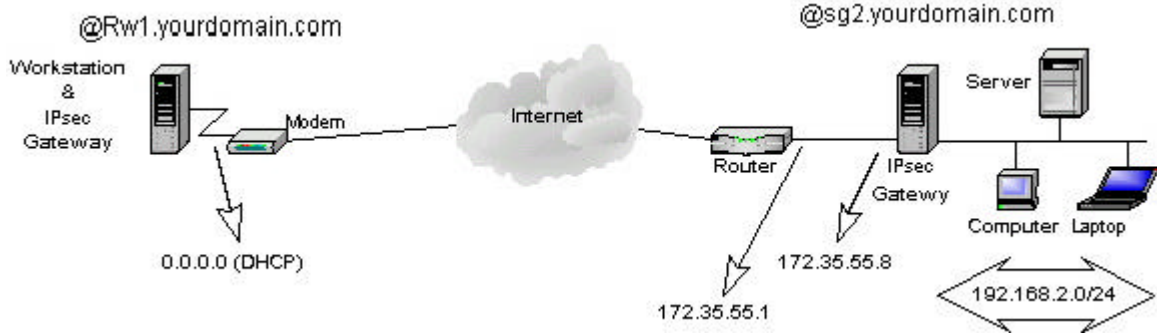
IPsec



(192.168.2.0/24)

(172.35.55.8)

가



( 3)

d. IPsec

IPsec VPN , 1:1 ,

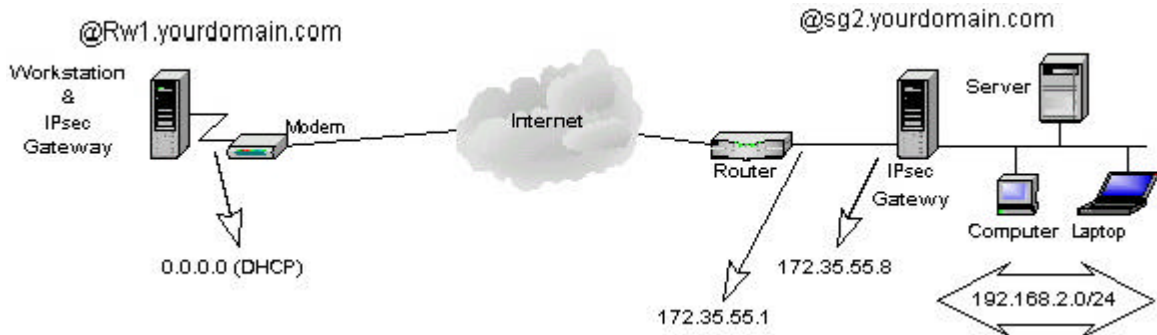
192.168.1.0/24( A), 192.168.2.0/24( B), 192.168.3.0/24( C)가  
 207.151.222.2(IPsec 1), 210.105.32.8(IPsec 2),  
 104.26.85.7(IPsec 3) , 192.168.0.0/16( D)  
 가 172.35.55.8(IPsec 4)

A, B, C, D IPsec 4  
 1 A B 가 A

B , VPN 2  
 2 IPsec 가

가

(CPU



< 4>

(6) FreeS/WAN

FreeS/WAN IPsec , GPL 가 가

<http://www.freeswan.org/>

## 2.8 Host IDS 위조

### (1) Host IDS

Host IDS

root , 가 , 가 ( File Integrity ), log , (port)가 ( Audit Tool ), 가

### (2) File Integrity

tripwire - 2.2.1

[HTTP://www.tripwire.com/downloads/](http://www.tripwire.com/downloads/)

1.

File Integrity 가 , .

#### 2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

You may not rent, lease, distribute, sell, assign, pledge, sublicense, loan, timeshare or otherwise use the Software for the commercial benefit of third parties, but you may transfer the Software on a permanent basis, provided you retain no copies and the recipient agrees to the terms of this EULA.

( Tripwire Linux )  
, 가 (File Integrity Checking Tools)  
가 , .

1. 8 가 Integrity checking algorithm . 2 가

=> 2 가 Checksum .  
cracker .

2. checksum data db , , 가

Fcheck-2.07.512

<http://www.securityfocus.com>

1.

1. md5 CRC check , md5sum file modify Integrity check

2. db , text file checksum ,

, 가 tool  
cron (daemon) ,

2. test

```

/usr/local/fcheck/
/usr/local/fcheck/fcheck -ac : /usr/local/fcheck/fcheck.cfg      checksum
database
/usr/local/fcheck/fcheck -a :      database      integrity

```

samhain -0.9.4

1.

2. test

./configure;make;make install

```

#mkdir /usr/local/var
#mkdir /var/local/var/log
#samhain -t init

```

```

Database initialize
, /usr/local/etc/.samhainrc      checksum
,

```

```

/usr/local/var/log/.samhain_file
/usr/local/var/log/.samhain_log

```

```

( /usr/local/etc/.samhainrc
.)
file/directory integrity check

```

samhain -t check

```

, /etc/inetd.conf /etc/sendmail.cf      , last
modified time

```

```

( )
check

```

```

.....
CRIT : [2000-09-09T18:59:06+0900] Password file entry is NULL for UID 444
CRIT : [2000-09-09T18:59:06+0900] No owner name for file: /etc/inetd.conf
CRIT : [2000-09-09T18:59:06+0900] POLICY [ReadOnly] /etc/inetd.conf
inode ln      mode      ext2flags  owner      group      size      mtime
-----
< 26399 1 -rw-r--r-- -----          root      3933 [2000-09-07T15:31:16
> 26399 1 -rw-r--r-- -----          root      3933 [2000-09-09T18:51:54
CRIT : [2000-09-09T18:59:06+0900] POLICY [ReadOnly] /etc/sendmail.cf
inode ln      mode      ext2flags  owner      group      size      mtime
-----
< 26446 1 -rw-r--r-- -----      root      root      34181 [2000-02-18T07:51:21
> 26446 1 -rw-r--r-- -----      root      root      34181 [2000-09-09T18:54:32

```

3.

```

checksum algorithm      tiger algorithm

```

### (3) Audit Tools

#### Guard -2.6

<http://www.penguin.cz/~ondrej/guard/guard.tar.gz>

1.

```
syslogd          ,          log          syslog.conf
                ,          가          .

Guard  syslogd          log message          ,          log message
      pattern matching          ,          log message          mail
      .          ,          log          .
      ,          syslogd  가  message          .
```

2. test

```
# ./install.sh
```

```
this installation file is pre-alpha version!
it's simple set of commands with default settings and without error checking.
it may help you install guard on fresh system. do not use it to upgrade
from older versions. and do not use it if you don't want default
configuration. when some problems occurs, please read the source code of
this script to know what has been done and how to reverse it.
to prove you have read and understood this now write the 26th word from the
beginning.
: fresh
```

```
making directory /usr/guard
adding user guard
changing shell for user guard to /bin/false
copying files
creating logging FIFO
creating logfile /var/log/security
assigning permissions
chown: root.guard: invalid group
chown: root.guard: invalid group
chgrp: invalid group name `guard'
chgrp: invalid group name `guard'
chgrp: invalid group name `guard'
chgrp: invalid group name `guard'
adding line to /etc/syslog.conf
```

```
*** done
```

```
guard is installed in directory /usr/guard
```

```
these steps have to be done manually now:
```

1. edit /usr/guard/guard.conf and set all variables that have to be set

2. put /usr/guard/g to startup scripts

WARNING: system lockup occurs when syslogd starts writing to FIFO  
and there's no guard process to read from it. always start guard  
before syslogd!

3. start guard and killall -HUP syslogd

```
file
```

```
bash# cp g /etc/rc.d/init.d/
```

```
bash# ln /etc/rc.d/init.d/g /etc/rc.d/rc3.d/
```

```
useradd guard  
cd /usr/guard  
chown -R guard .  
vi guard.conf
```

```
=> OutputDevicec
```

```
Mail  
UID guard
```

```
syslogd g pipe syslogd  
message
```

```
rules/generic - linux pattern match  
/var/log/security , mail report
```

```
** error : Mailer
```

### 3. 가

rule

## logcheck - 1.1.1

### 1.

```
logcheck log , pattern match  
error message , email  
guard  
guard 가 syslog input pipe ,  
logcheck cron  
logcheck log file 가,  
pattern match email
```

### 2. test

```
#make linux  
vi /usr/local/etc/logcheck.sh  
=> SYSADMIN ( email )  
cron /usr/local/etc/logcheck.sh  
log , email
```

#### Security Violations

```
=====
```

```
Sep 9 19:58:15 tarzan PAM_pwdb[10348]: authentication failure; k09(uid=502) -> root f  
Sep 9 19:58:21 tarzan PAM_pwdb[10350]: authentication failure; k09(uid=502) -> root f
```

#### Unusual System Events

```
=====
```

```
Sep 9 19:58:15 tarzan PAM_pwdb[10348]: authentication failure; k09(uid=502) -> root f  
Sep 9 19:58:21 tarzan PAM_pwdb[10350]: authentication failure; k09(uid=502) -> root f
```

### 3. 가

guard , , pattern match syslog audit ,  
 guard 가 , logcheck syslog 가 , pipe  
 guard 가 , reporting logcheck 가

(4) 가

(File Integrity Tool) Audit Tool  
 test 가 , (Intrusion)  
 가  
 File Integrity Fcheck 가, audit guard 가 가

## 2.9 Network IDS 위로

(1)

Network IDS  
 가 matching (segment) , pattern  
 , remote exploit code

(2) Scanning Tools

nmap  
 1. 가 ,  
 (port) , http 80 , telnet 23  
 가 , (port scanning)  
 nmap ,

- ⚡ TCP connect() scanning,
- ⚡ TCP SYN (half open) scanning,
- ⚡ TCP FIN, Xmas, or NULL (stealth) scanning,

- ⌘ TCP ftp proxy (bounce attack) scanning
- ⌘ SYN/FIN scanning using IP fragments (bypasses some packet filters),
- ⌘ ICMP scanning (ping-sweep)
- ⌘ TCP Ping scanning
- ⌘ Remote OS Identification by TCP/IP Fingerprinting, and

2. ( % user , # root )

%nmap -sT foo.bar.com

foo.bar.com connect() system call port scan .

#nmap -sS foo.bar.com

foo.bar.com SYN scan , host , 3-way handshake connection .

#nmap -sF foo.bar.com

Stealth scan. 가 IDS(Intrusion Detection System, ) .

#nmap -O foo.bar.com

TCP/IP fingerprint .

saint

1.

saint , (port) , 가 , .

가 Web , 가 .

2.

, root

#./saint

Web target host scan , 가 .

### (3) IDS Tools

tcpdump- 3.5.2

1.

Network Monitoring Tools .

TCP / UDP / ICMP

packet

## 2. test

```
= dependency
libpcap-0.5.2.tar.gz
http://www.tcpdump.org
./configure;make;make install
sudo mkdir /usr/local/include; sudo mkdir /usr/local/include/net
make install-incl ; make install-man
```

" 가 "

```
# tcpdump src not 192.168 and tcp and not port 80
tcpdump: listening on eth0
17:31:03.762427 cracker.test.co.kr.3312 > atropos.test.co.kr.ssh: . ack 2348842403
win 16268 (DF)
```

## 3.

tcpdump , (filtering) 가

snort- 1.6.2.2

⚡

snort tcpdump , IP , remote exploit

가

⚡ test

```
./configure;make;make install
make /var/log/snort
http://www.snort.org -> Rules Database rule
Rule file
```

Rule File , network level

```
# Backdoors - Signature Based
# Denial of Service
# Finger Rules
# FTP Rules
# Overflows
# ICMP / PING
# Scan / Probe
# SMTP
# TELNET
# Mail Virus
```



(3) 가

Network IDS

(Packet Sniffer)

, 가  
, 가

. snort  
가

pattern matching rule

. <http://www.snort.org>

## 2.10 Firewall -

위로

(1) Firewall

, 가

, 가

firewall

(Port)

. firewall IP

가 telnet  
IP

, telnet

, 가

가 , firewall

rullset

tcp\_wrapper

. 가 가

firewall

firewall

(2) firewall

firewall

firewall

(2-1) ipchains

- rpm package  
RedHat package

<ftp://ftp.freshmeat.net/pub/rpms/>

-

IP masquerading, packet filtering (firewall)

ACCEPT, DENY, REJECT, MASQ  
masquerade

input packet, forward packet, output packet

-

1)

```
ipchains -I forward -s 192.168.1.0/24 -d 147.47.0.0/255.255.0.0 -j MASQ
```

source 192.168.1.\* 147.47.\*.\* packet forwarding  
가 가 .

192.168.1.\* IP masquerade 가 .

2)

```
ipchains -A forward -s 192.168.0.0/24 -d 0.0.0.0/0 -p tcp -j MASQ
```

source 192.168.0.\* destination tcp packet forwarding 가  
, 가 append .

3)

```
ipchains -P forward DENY
```

가 packet , 가

4)

```
ipchains -A forward -p tcp -s 0.0.0.0/0 -d 0.0.0.0/0 telnet -j ACCEPT
```

가 telnet packet .

5)

```
ipchains -A input -j DENY
```

!!! !!!

. ipchains

6)

==>

```
ipchains --list
```

```
Chain input (policy ACCEPT):
Chain forward (policy DENY):
target prot opt source destination ports
MASQ tcp ----- 192.168.0.0/24 anywhere any -> any
ACCEPT tcp ----- anywhere anywhere any -> telnet
Chain output (policy ACCEPT):
```

7)

```
ipchains --flush
```

8)

```
ipchains -D forward 1
```

```
forward 1 .
```

-

1) ping icmp

```
ipchains -A input -p icmp -j DENY
```

```
ping 0
```

)

```
PING 0 (0.0.0.0) from 127.0.0.1 : 56(84) bytes of data.
```

```
--- 0 ping statistics ---
```

```
3 packets transmitted, 0 packets received, 100% packet loss
```

2) telnet

```
telnet
```

```
telnet 0
```

)

```
Trying 0.0.0.0...
```

```
telnet: Unable to connect to remote host: Connection refused
```

(3) firewall

가?

```
firewall
```

```
. firewall
```

가

3.

위로

가

root

sudo

가

, root

su

tcp\_wrapper

TCP  
libwrap

, inetd

.tcp\_wrapper

(console)

, sniffing

가

. ssh

가

. scandetd  
(scanning)

가

가 buffer overflow

libsafe

가

가

telnet rsh, rlogin, ftp

IPsec

. IPsec IP

IPsec

security gateway

, 가 가

가

network -IDS(

)가

host -IDS(

)

. host -IDS

가

network -IDS

ipchains가

. ipchains

(firewall)

가

가

. ipchains

가

가

가

( )

( )

Copyright (c) 2001 by Clunix, Inc.