



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

GIAC Firewall Perimeter Protection Curriculum Practical Assignment for SANS Security DC2000

Name: Hussam Hamdy Hanafy Eid Aly

Q-1)

Blocking spoofed addresses protect the internal network from a lot of Denial of service attacks, some DOS utilities are used to make an IP conflict with all machines in your network, others are used to flood the network or hosts with ICMP replies. Some spoofed packets may pass through the static filters, which is based on the source IP address in its filtering criteria.

Also we should be sure that our network doesn't send spoofed addresses to the outside world, some internal users could use DOS utilities to send spoofed packets to other networks.

Applying Egress filters could help in regulating the outbound traffic; only real IP could leave your network to the outside world.

Blocking source routing protects your network from responding to a spoofed addresses, and man in the middle attack.

The best way to block the spoofed addresses from coming into your network is the Router configuration itself. All examples shown below are based on the following network configuration,

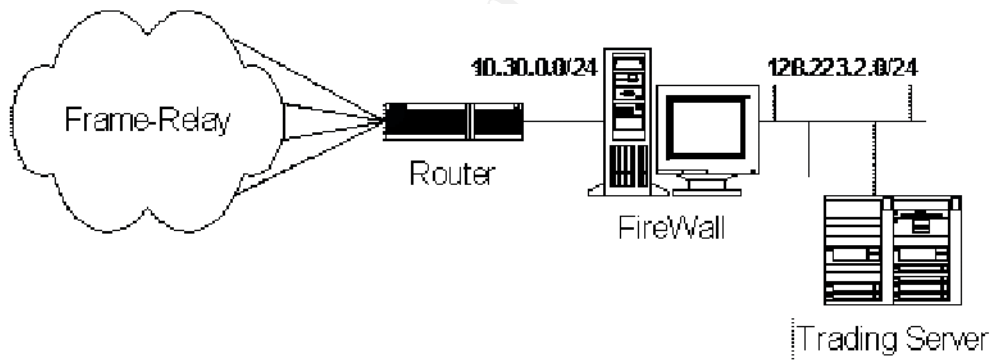


Figure 1 illustrates the current setup.

Using Cisco Router 3640

Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IS56I-M), Version 12.0(5)T1, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 21:16 by cmong

```
Remote_trading#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Remote_trading(config)#access-list 11 deny 10.30.0.0 0.255.255.255
```

```

Remote_trading(config)#access-list 11 deny 128.223.2.0 0.255.255.255
Remote_trading(config)#access-list 11 permit any
Remote_trading(config)#int s1/0
Remote_trading(config-if)#ip access-group 11 in
Remote_trading(config-if)#int s1/1
Remote_trading(config-if)#ip access-group 11 in
Remote_trading(config)#int s2/0
Remote_trading(config-if)#ip access-group 11 in
Remote_trading(config-if)#int s2/1
Remote_trading(config-if)#ip access-group 11 in
Remote_trading(config)#access-list 12 permit 10.30.0.0 0.255.255.255
Remote_trading(config)#access-list 12 permit 128.223.2.0 0.255.255.255
Remote_trading(config)#int fastEthernet 0/0
Remote_trading(config-if)#ip access-group 12 in
Remote_trading(config-if)#no ip source-route
Remote_trading#wr

```

Q-2)

Telnet is used to establish console user sessions with multi-user computer. Telnet could be used to attach to the following services,

- 1- TCP service Echo, Daytime, Chargen
- 2- HTTP & FTP
- 3- POP3, SMTP and NNTP

It is also possible to gain root access that you don't already have via some bugged telnetd in some operating system.

SSH is a protocol for secure remote login and other secure network services over an insecure network. The user authentication protocol is subject to man-in-the-middle attacks if the encryption is disabled. The SSH protocol does not protect against message alteration if no MAC is used.

FTP has two modes to work with, PASSIVE Mode where the client connect to port TCP/21 for command, then port TCP/20 for data transmission, while ACTIVE mode where client connects to port 21 for commands & any port for data .some old FTP client use port tcp/20 to transmit data (it shouldn't be allowed) .Even if someone access the FTP server as anonymous user the user can gain access to the critical operating system files if the files & directories is not configured properly (Symbolic links).

Net BIOS (138,139,137 TCP/UDP) is the protocol used by Microsoft Windows networking to connect LAN clients to file & Share servers, it will run over IPX, NetBEUI and TCP, it shouldn't be allowed to pass the firewall in either direction, many exploits are available on hacker web site using NetBios protocol.

rlogin , Many UNIX systems provide the rlogin program. rlogin establishes a remote login session from its user's terminal to a remote host computer, rlogin passes the user's current terminal definition as identified by the TERM environment variable to the remote host computer. Many implementations of the rlogin program contain a coding defect where the value of the TERM environment variable is copied without due care to an internal buffer. This means that the buffer holding the copied value of TERM can be overflowed which means denial of service attack.

Now we are going to implement some rules using Axent Raptor firewall Ver 6.0i running over UNIX solaris 5.2, it is an application proxy gateway & stateful inspection packet filter in the same time.

By default it has the rule, deny ANY ANY, so that unless you permit a service it will not work.

After the firewall installation we used a regular port scanner utility to scan the firewall from inside & outside, we found that telnetd, SMTPd, HTTPd, Gopherd & NNTPd by default are listening unless you disable it .

Figure 2 shows the daemons enabled by default in the log file; it is normal responses for port scan the firewall,

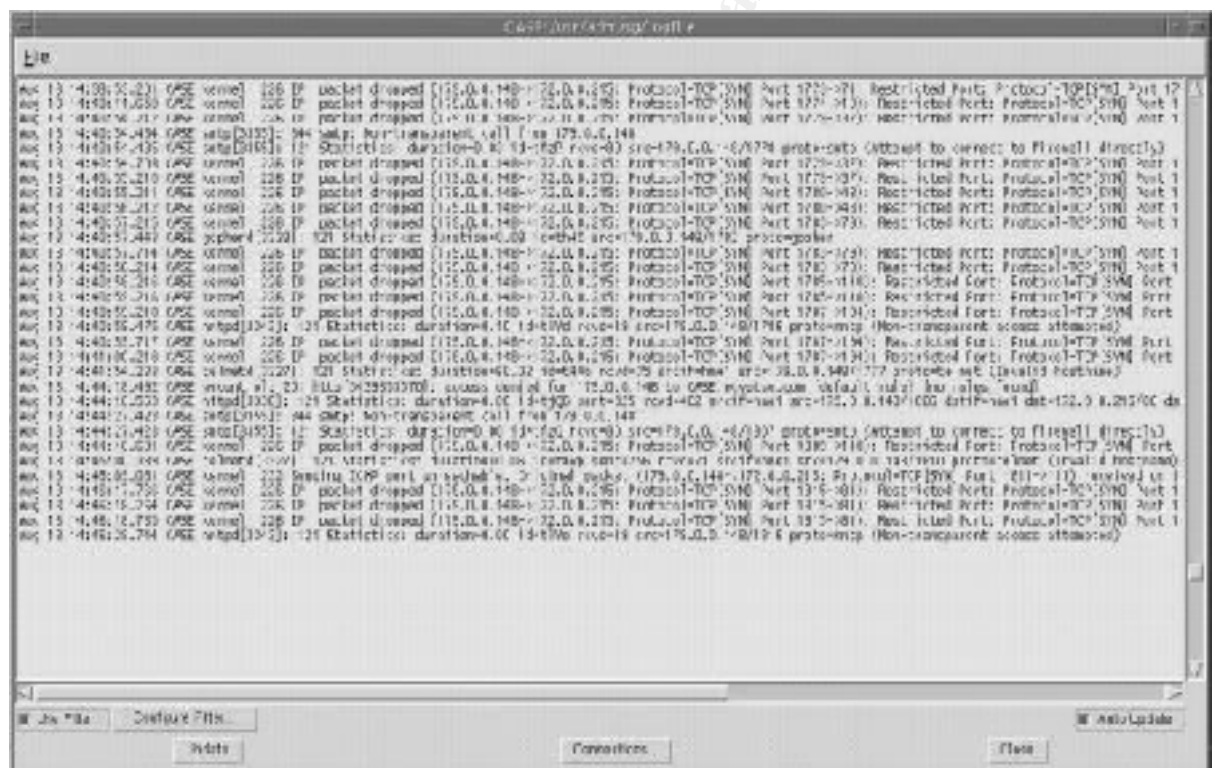


Figure 2 illustrates the log.

The log file says that

Smtplib [3355]: 334 smtp:Non-transparent call from 179.0.0.148

Which means that, the smtp daemon is up and listening, it replies the packet that has been sent by the port scanner software on port 25/TCP, but the smtpd found that the source is trying to connect to the firewall directly which is called non-transparent call, so it gives a warning about that.

Another line in the log file says

Kernel: 226 IP packet dropped (179.0.0.148→ 172.0.0.215) Protocol=TCP [SYN] Port 1779→79): Restricted port.

It means that the firewall see a SYN packet goes to a closed port in the firewall which is 79/TCP, so it drops it and add an entry in the log file.

Now we start define some rules in the rule database, to define a rule you need to permit or deny specific protocol based on the source or destination .By default there are some protocols already defined in the firewall protocol database, so you can use it in the rule definition, but if you could not find a protocol you can define it as follow,

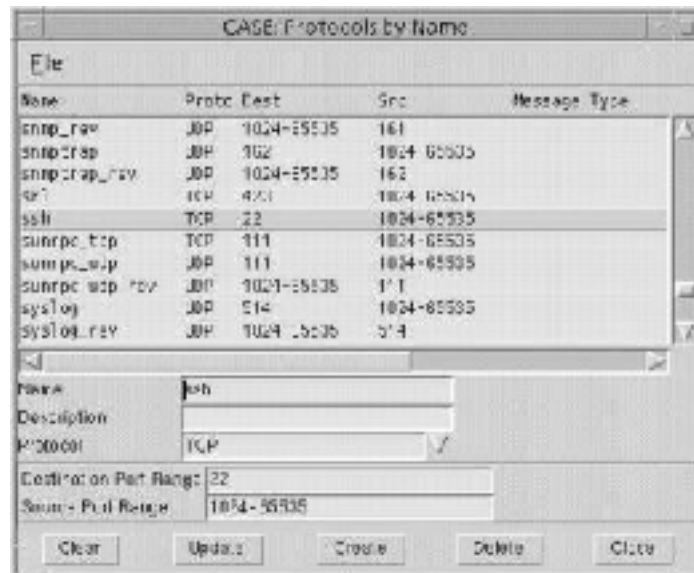


Figure 3

In the previous figure, we are trying to add protocol called SSH, type TCP, and define the dest & Src. ports.

The next step is to create a Generic Services Protocol, Using SSH protocol we have just created.



Figure 4.

Define another GSP for Net Bios, rlogin as follow

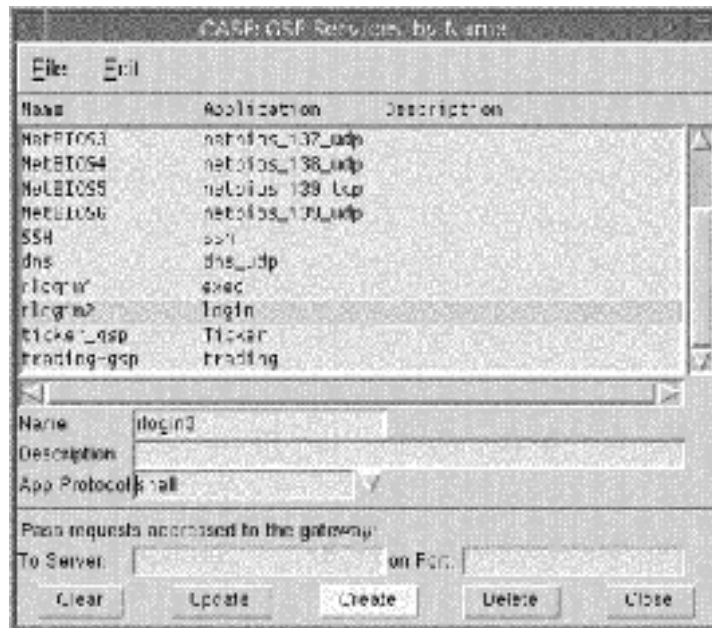


Figure 5

Finally we can define a rule for question No. (2), which prevent the universe, (All Hosts), from sending NetBios , SSH , ftp , rlogin..... inside our internal network .

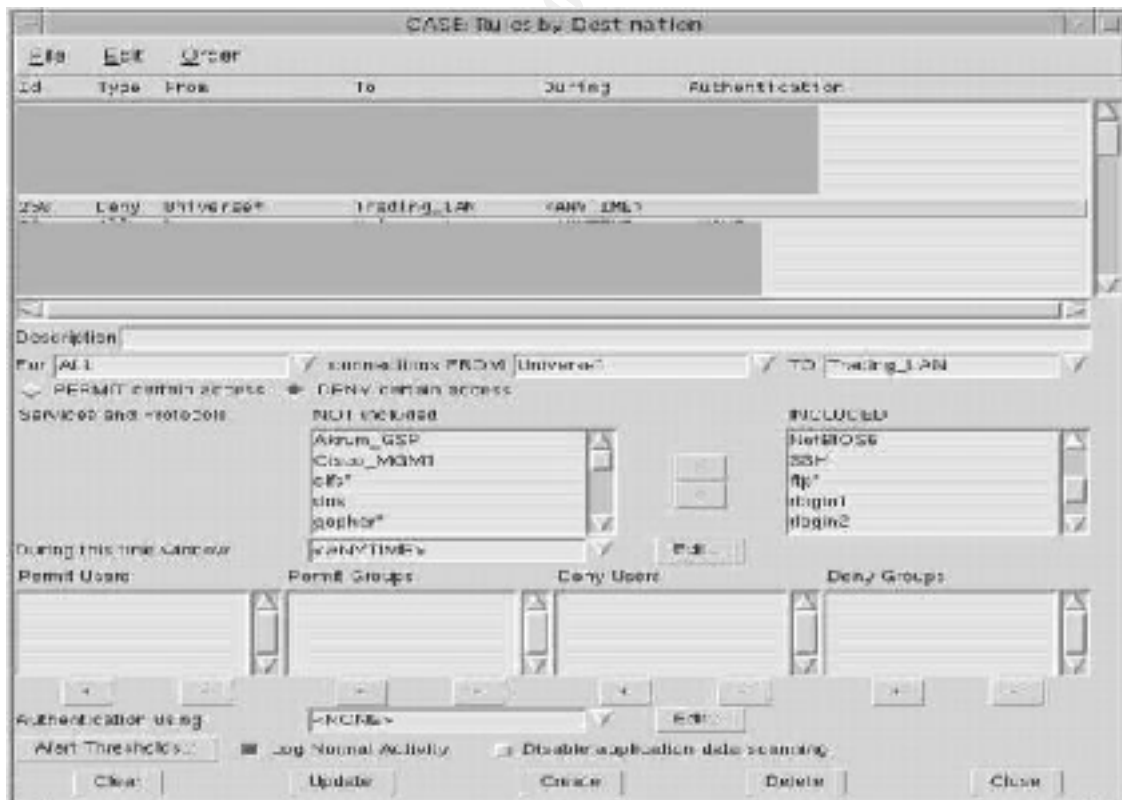


Figure 6.

You can notice the option (disable application data scanning), if we check this option the firewall will work in a packet filter mode. If it is not checked the firewall will work in application proxy mode.

You can notice that we don't define a telnet or FTP as a GSP because they are already exits via proxy Daemons ftpd, telnetd, but the others will be running using the gateway control.

Q-3)

RPC/UDP, Remote Procedure Call is a protocol that allows two computers to coordinate in executing software. A program in one computer can cause RPC to transfer the execution of a subroutine to another computer, and have the result returned to the first via RPC. So you shouldn't let the RPC traffic through your firewall.

The portmap daemon converts RPC program numbers into Internet port numbers. A lot of hackers are targeting a lot of sites looking for portmapper.

NFS enable LAN clients access to file server storage, it is not recommended to use unless you have encrypted tunnel.

The lockd daemon processes lock requests that are either sent locally by the kernel or remotely by another lock daemon. The lockd daemon forwards lock requests for remote data to the server site lock daemon through the RPC package, it shouldn't pass through the firewall.

all the traffic regarding the 111/TCP, 111/UDP, 2049/TCP, 2049/ UDP, 4045/TCP, &4045/UDP will be denied by the firewall by default , since we found these ports are closed in the port scan result.

Q-4)

Windows 2000 ports 445 /TCP, UDP. Common Internet File System (CIFS). CIFS provides an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the standard Server Message Block (SMB) protocol widely in use by personal computers and workstations running a wide variety of operating systems. When operating CIFS over the NETBIOS transport over TCP, connections are established and messages transferred, message transport is done using NETBIOS session service. After the server name has been resolved to an IP address, a connection to the server needs to be established if one has not already been set up. Connection establishment is done using the NETBIOS session service, which requires the client to provide a "calling name" and a "called name." The calling name is not significant in CIFS, except that an identical name from the same transport address is assumed to represent the same client; the called name is always "*SMBSERVER." Connection establishment results in a "Session Request " packet to port 139 "

Additional rule should be added in our Firewall, deny any any tcp 139. Which is rule (258) shown above in figure 6.

Don't allow logging for this rule because you will get a very big log file at the end of the day.

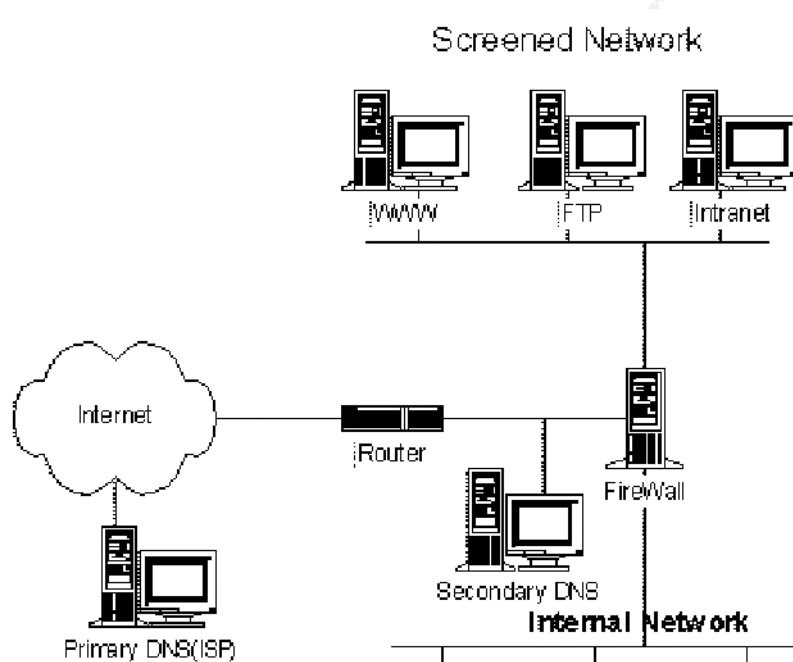
Q-5)

X Windows client may use Server to run a GUI application and receive the application output on the client GUI. Display 0 on port 6000 ~ Display 255 on port 6255. Keystrokes & screen captures could be obtained through Xwindows protocols. By default port 6000/TCP, UDP are closed.

Q-6-7-8)

the previous setup shown in Fig.1 does not support DNS, mail, and http services; there is no Internet traffic in it.

Using the following setup, which is the Internet firewall we can do some DNS, http, mail traffic regulation, the setup is as the following



Unfortunately the Internet router administration is the responsibility of the ISP, so all the configuration could be done in the firewall only.

The policy needed to be configured is as follow,

- DNS 53/UDP is allowed from the screened network (DMZ) & from the Internet Network to the secondary DNS which is as shown above is outside the firewall, while DNS 53TCP/UDP are allowed from the Secondary DNS to the World.
- HTTP & HTTPS are allowed from the internal networks to the DMZ (Mail & Web, intranet) servers and to the universe.
- HTTP & HTTPS are allowed from the universe to the (WWW& Mail) in the DMZ.

- POP, POP3, SMTP are Allowed from the universe to the DMZ mail.
- POP, POP3, SMTP are allowed from the internal to the Mail server in the DMZ& from the internal to the universe through the application gateway proxy since some internal users have personal mail accounts on other internet servers.
- POP, POP3, SMTP are allowed from the MAIL server in the DMZ to the Universe.
As shown in the following figure 10 which is the firewall rule database.

Name	Direction	Source	Destination	Permissions	Services	Time	Substitution
FW-1112-Response-DMZ-250		Response2	DMZ	ALL	SMTP	ANYTIME	ANY
FW-1113-Universal-DMZ		Universal	DMZ	ALL	HTTP	ANYTIME	ANY
FW-1114-Universal-Response2		Universal	Response2	ALL	SMTP	ANYTIME	ANY
FW-1115-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1116-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1117-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1118-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1119-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1120-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1121-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1122-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1123-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1124-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1125-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1126-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1127-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1128-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1129-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1130-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1131-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1132-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1133-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1134-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1135-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1136-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1137-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1138-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1139-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1140-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1141-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1142-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1143-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1144-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1145-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1146-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1147-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1148-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1149-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1150-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1151-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1152-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1153-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1154-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1155-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1156-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1157-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1158-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1159-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1160-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1161-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1162-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1163-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1164-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1165-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1166-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1167-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1168-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1169-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1170-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1171-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1172-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1173-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1174-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1175-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1176-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1177-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1178-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1179-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1180-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1181-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1182-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1183-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1184-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1185-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1186-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1187-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1188-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1189-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1190-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1191-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1192-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1193-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1194-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1195-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1196-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1197-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1198-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY
FW-1199-Universal-Response2		Universal	Response2	ALL	HTTP	ANYTIME	ANY

FIG(10) Axent Raptor firewall ver.6.0 for windows NT, rule base window.

The only outgoing ports available to the internal network is

- 80/TCP
- 53/UDP
- 110,109/TCP
- 1352/TCP

So all Trojans will not work going out, unless it uses the same ports and talking the same protocols.

Q-9)

As example, testing the finger port going from inside to outside, the log said that IP Packet dropped

Note	firewall firelogd	15	17:18:33.303	IP packet dropped (172.0.0.204->163.121.2.5: Protocol=TCP(SYN, Port 2337->73), Restricted Port Pro
Note	firewall firelogd	15	17:18:33.303	IP packet dropped (172.0.0.204->163.121.2.5: Protocol=TCP(SYN, Port 2337->73), Restricted Port Pro

Figure 11.

For incoming & outgoing application proxy daemons, the daemons, which are enabled by default when finish the firewall installation is

resyncd	138	18:38:54.203	117	Daemon starting
isacmnd	128	18:38:54.343	117	Daemon starting
fpd	175	18:38:54.421	122	Daemon listening on port(s): 21/tcp
udp-dp	115	18:38:54.137	122	Daemon listening on port(s): 53/udp, 4000/udp, 137/udp, 136/udp, 138/udp
pingd	275	18:38:54.477	122	Daemon listening on port(s): 5/icmp
h323d	207	18:38:54.453	122	Daemon listening on port(s): 1720/tcp
stunstd	176	18:38:54.468	117	Daemon starting
upnc	150	18:38:54.484	117	Daemon starting
tcpcatd	144	18:38:54.500	122	Daemon listening on port(s): 49/tcp
httpd	177	18:38:54.571	122	Daemon listening on port(s): 80/tcp, 443/udp
crtd	117	18:38:54.546	122	Daemon listening on port(s): 1038/tcp
nc	150	18:38:54.546	122	Daemon listening on port(s): 7070/tcp, 10000/tcp
rsync	140	18:38:54.562	122	Daemon listening on port(s): 22/tcp
telnetd	100	18:38:54.578	122	Daemon listening on port(s): 23/tcp
tcp-gp	102	18:38:54.009	301	
tcp-gp	162	18:38:54.009	301	
tcp-gp	107	18:38:54.079	122	Daemon listening on port(s): 1521/tcp, 1521/udp, 8080/tcp, 53/tcp, 443/tcp, 5191/tcp, 4100/tcp, 1372/tcp, 1372/udp
isacmnd	128	18:38:54.887	120	isacmnd Info: Successfully logged into the ISAKMP engine with a default profile which has no Certificate support
essential	-	18:38:55.125	101	Raptor Network Security Management System V6.0i starting up
essential	-	18:38:55.125	314	Working in one file (line 27, parse error, expecting NEWLINE)
roadhawk	233	18:38:57.765	121	Statistics: duration=3.691s, ipsec=31, rcvd=62, sent=60, no=62, 0.0.1/1216, success=
stunstd	176	18:38:04.015	120	stunstd Info: Loading twin tunnels
isacmnd	128	18:38:04.015	120	isacmnd Info: Reloading isakmp tunnels
resyncd	138	18:38:04.075	120	resyncd Info: Loading Mobile tunnels

Figure 12.

By editing some files in the firewall & disable some daemons, the enabled daemons will be as follow,

sakmnd	242	18:50:56.203	117	Daemon starting
resyncd	167	18:50:56.218	117	Daemon starting
telnetd	133	18:50:56.296	122	Daemon listening on port(s): 23/tcp
tcp-gp	134	18:50:56.328	301	Internal warning: port_receive_control(5, 39, 2) failed: The network request is not supported.
tcp-gp	134	18:50:56.328	301	Internal warning: port_receive_control(5, 39, 2) failed: The network request is not supported.
tcp-gp	134	18:50:56.343	22	Daemon listening on port(s): 1526/tcp, 1521/tcp, 8080/tcp, 53/tcp, 1352/tcp
tcp-gp	106	18:50:56.343	22	Daemon listening on port(s): 53/udp
pingd	145	18:50:56.389	22	Daemon listening on port(s): 7/icmp
upnc	165	18:50:56.375	117	Daemon starting (tunneling disabled, monitoring config files only)
httpd	118	18:50:56.421	22	Daemon listening on port(s): 80/tcp, 443/tcp
snmp	111	18:50:56.437	22	Daemon listening on port(s): 25/tcp
fpd	102	18:50:56.453	22	Daemon listening on port(s): 21/tcp
sakmnd	242	18:50:56.551	120	sakmnd Info: Successfully logged into the ISAKMP engine with a default profile which has no Certificate support
gwconect	-	18:50:58.200	01	Raptor Network Security Management System V6.0i starting up

Figure 13.

Q-11)

ICMP packets are used for network diagnostics. They could be used to perform DoS attacks or map the network. From the above figure we can notice that

- ICMP is enabled, we can not disable it right now because some network guys uses it as a troubleshooting, but as previous examples showed, we can define a

GSP based on ICMP & message type, then apply the GSP to a deny rule for specific internet or screened network.

- Specific port 8080/tcp is opened for accessing some http servers on 8080 ports for web administration, but it is outgoing only.

© SANS Institute 2000 - 2002, Author retains full rights.