Global Information Assurance Certification Paper

Elizabeth Martin
SANS GIAC Intrusion Detection
Practical Assignment

Note: All non-pertinent traffic has been omitted from each detect

Detect 1

5:02:27 drop firewall > if0 proto udp src 127.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 rule 0 reason: local interface address spoofing
5:03:00 drop firewall >if0 proto udp src 192.168.200.223 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25
5:07:27 drop firewall >if0 proto udp src 127.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 rule 0 reason: local interface address spoofing
5:07:28 drop firewall >if0 proto udp src 192.168.200.224 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25
5:08:13 drop firewall >if0 proto udp src 192.168.200.222 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25 5:08:27 drop firewall >if0 proto udp src 127.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 rule 0 reason: local interface address spoofing
5:09:00 drop firewall >if0 proto udp src 192.168.200.223 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25
5:09:28 drop firewall >if0 proto udp src 127.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 rule 0 reason: local interface address spoofing
5:09:28 drop firewall >if0 proto udp src 192.168.200.224 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25
5:10:13 drop firewall >if0 proto udp src 192.168.200.222 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25
5:10:28 drop firewall >if0 proto udp src 127.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 rule 0 reason: local interface address spoofing
5:11:01 drop firewall >if0 proto udp src 192.168.200.223 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 25

<snip snip; a little while later>

6:01:10 drop firewall >if0 proto udp src 90.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 19
6:05:10 drop firewall >if0 proto udp src 90.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 19
6:07:10 drop firewall >if0 proto udp src 90.0.0.1 dst 255.255.255.255 service 2301 s_port 2301 len 40 rule 19

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields: **5:11:**01[timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto udp** [protocol] **src 192.168.200.3** [source IP address] **dst 255.255.255.255** [destination IP address] **service 2301**[destination port] **s_port 2301** [source port] **len 40** [IP datagram length **rule 25** [firewall rule number]

3. Probability the source address was spoofed
High. Traffic was detected on the internal interface of the firewall, and we do not use 192.168.x.x addresses on our network. In addition the 127.0.0.1 and 90.0.0.1 traffic should never appear on the network. Given this is a denial of service attack and not reconaissance, the attacker loses nothing by spoofing.

4. Description of attack:
Known buffer overflow vulnerability in Compaq Insight Management Agents and Compaq Survey Utility that allows for a Denial of Service.

The source address (possibly spoofed), source port (same as destination port rather than random and incremental), and consistent packet length could indicate forged udp packets.

5. Attack mechanism:
Packets are crafted with a specified length and sent to the network broadcast address. Compaq server responds with a buffer overflow and requires reboot.

6. Correlations:
MS-FOCUS@securityfocus.com Mailing List:
Information regarding this detect was requested by Larry Karantzios (lkarantzios@onmoney.com) in the same timeframe the detects were discovered on my network.

SecurityFocus:
http://www.securityfocus.com/templates/archive.pike?list=1&date=1999-05-22&msg=4125677D.0056351A.00@mailgw.backupcentralen.se

Common Vulnerabilities and Exposures:
CVE-1999-0772
Denial of service in Compaq Management Agents and the Compaq Survey Utility via a long string sent to port 2301.

Compaq:
http://www.compaq.com/products/servers/management/security.html

7. Evidence of active targeting:
Yes - attacker is targeting Compaq servers

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 4 (Compaq is firm standard for all NT servers)
Lethality = 4 (Total lock-out or unrestricted access to server)
Countermeasures: System = 3 (This particular patch is not installed, and as a standard the web agent is enabled);
Net = 5 (No ip directed broadcast enabled on all routers, RFC 1918 IPs blocked at screening router)
Severity = 0

9. Defensive recommendation:
Install patch, identify source of broadcasts and eliminate.

10. The above trace is indicative of:

a) Network Denial of Service attempt
b) NT Version Scan
c) Attempt to exploit system vulnerabilities using spoofed IP address
d) UDP Packet Storm

Answer: c

***Note: Further investigation has led to the conclusion that the 192.x addresses are being used for a dual NIC configuration of Lotus Notes Servers clustering on a 'private' network, indicating IP addresses are not spoofed. The UDP broadcasts are most likely 'legal' but ugly traffic generated by Compaq Insight Manager. Until the source of the 127.0.0.1 and 90.0.0.1 traffic is determined and the Compaq product owners determine the source of the broadcasts research will continue.

Detect 2

16 April
12:13:22 reject ChicagoFirewall11 >ef0 useralert proto udp src 207.59.153.204 dst 256.255.236.27 service SNMP s_port 1529 len 265 rule 2

15 April
10:14:29 reject ChicagoFirewall2 >ef0 useralert proto udp src 207.59.153.204 dst 256.255.244.7 service SNMP s_port 1529 len 265 rule 2

14 April
17:14:42 reject SingaporeFirewall1 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.188.7 service snmp s_port 1042 len 72 rule 13

5:02:48 reject SarasotaFirewall1 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.220.7 service snmp s_port 1042 len 72 rule 12
4:14:15 reject HoustonFirewall1 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.204.7 service snmp s_port 1042 len 72 rule 2
4:02:15 reject ChicagoFirewall11 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.236.27 service snmp s_port 1042 len 72 rule 2
19:04:46 reject SydneyFirewall1 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.212.7 service snmp s_port 1042 len 72 rule 2
3:57:22 reject ChicagoFirewall2 >ef0 useralert proto udp src 194.203.215.204 dst 256.255.244.7 service snmp s_port 1042 len 72 rule 2

13 April
7:54:17 reject ChicagoFirewall2 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.244.7 service snmp s_port 1049 len 72 rule 2
14:00:57 reject LondonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.228.7 service snmp s_port 1049 len 72 rule 13
21:12:06 reject SingaporeFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.188.7 service snmp s_port 1049 len 72 rule 13
15:05:38 reject JohannesburgFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.148.7 service snmp s_port 1049 len 72 rule 2
8:11:30 reject HoustonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.204.7 service snmp s_port 1049 len 72 rule 2
23:01:57 reject SydneyFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.212.7 service snmp s_port 1049 len 72 rule 2
7:59:14 reject ChicagoFirewall11 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.236.27 service snmp s_port 1049 len 72 rule 2
8:59:55 reject SarasotaFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.220.7 service snmp s_port 1049 len 72 rule 12
18:50:51 reject SingaporeFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.188.7 service snmp s_port 1052 len 72 rule 13
12:44:22 reject JohannesburgFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.148.7 service snmp s_port 1052 len 72 rule 2
5:50:13 reject HoustonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.204.7 service snmp s_port 1052 len 72 rule 2
20:40:40 reject SydneyFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.212.7 service snmp s_port 1052 len 72 rule 2
5:33:00 reject ChicagoFirewall2 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.244.7 service snmp s_port 1052 len 72 rule 2
6:38:39 reject SarasotaFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.220.7 service snmp s_port 1052 len 72 rule 12
5:37:57 reject ChicagoFirewall11 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.236.27 service snmp s_port 1052 len 72 rule 2

11:39:41 reject LondonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.228.7 service snmp s_port 1052 len 72 rule 13
11:12:54 reject JohannesburgFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.148.7 service snmp s_port 1027 len 72 rule 2
4:02:27 reject ChicagoFirewall2 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.244.7 service snmp s_port 1027 len 72 rule 2
17:19:44 reject SingaporeFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.188.7 service snmp s_port 1027 len 72 rule 13
5:07:51 reject SarasotaFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.220.7 service snmp s_port 1027 len 72 rule 12
4:19:17 reject HoustonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.204.7 service snmp s_port 1027 len 72 rule 2
4:07:19 reject ChicagoFirewall11 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.236.27 service snmp s_port 1027 len 72 rule 2
19:09:49 reject SydneyFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.212.7 service snmp s_port 1027 len 72 rule 2
10:08:58 reject LondonFirewall1 >ef0 useralert proto udp src 194.203.215.194 dst 256.255.228.7 service snmp s_port 1027 len 72 rule 13

12 April
9:13:07 reject SydneyFirewall1 >ef0 useralert proto icmp src 208.184.232.206 dst 256.255.212.7 rule 2 icmp-type 3 icmp-code 1
1:42:02 reject SydneyFirewall1 >ef0 useralert proto udp src 194.203.215.234 dst 256.255.212.7 service snmp s_port 1053 len 72 rule 2
10:34:37 reject ChicagoFirewall2 >ef0 useralert proto udp src 194.203.215.234 dst 256.255.244.7 service snmp s_port 1053 len 72 rule 2
10:39:29 reject ChicagoFirewall11 >ef0 useralert proto udp src 194.203.215.234 dst 256.255.236.27 service snmp s_port 1053 len 72 rule 2

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
10:39:29 [timestamp] **reject** [action] **ChicagoFirewall11** [hostname] **> ef0** [external interface name] **proto udp** [protocol] **src 194.203.215.234** [source IP address] **dst 256.255.236.27** [destination IP address] **service snmp** [destination service] **s_port 1053** [source port] **len 72** [IP datagram length **rule 2** [firewall rule number]

3. Probability the source address was spoofed
Low. The 194.203.215.234 address is registered to an individual at Worldcom/Uunet via RIPE NCC. The 207.59.153.204 address is registered to Interpath.net (an ASP). In addition this is an attempt to identify unprotected network devices running SNMP, a spoofed IP address would gain nothing.

4. Description of attack:
Attacker is attempting SNMP probe of network device

5. Attack mechanism:
Attacker attempts an SNMP connection via crafted packets (note the time association with the consistent source port and consistent packet length). This may have been a brute force attempt to determine SNMP community strings as individual devices were targeted multiple times at different times. Attacker may have attempted one connection with a device then moved on to another device in order to avoid detection.

In addition to the above, attacker may have been attempting to exploit any number of known SNMP network device related vulnerabilities such as NetApps C630 Netcache default community string "public"; Solaris SNMP subagent default community string; guessable SNMP community string, default SNMP community string; ROUTERmate default community string; etc.

6. Correlations:
securityfocus.com
http://www.securityfocus.com/templates/forum_message.html?forum=2&head=7&id=7
Section: Common Omissions, 11. Network Brute Force Testing

CVE-1999-0472
The SNMP default community name "public" is not properly removed in NetApps C630 Netcache, even if the administrator tries to disable it.

CAN-1999-0186
In Solaris, an SNMP subagent has a default community string that allows remote attackers to execute arbitrary commands as root, or modify system parameters.

CAN-1999-0516 (under review)
An SNMP community name is guessable.

CAN-1999-0792 (under review)
ROUTERmate has a default SNMP community name which allows remote attackers to modify its configuration.

CAN-1999-0517 (under review)
An SNMP community name is the default (e.g. public), null, or missing.

7. Evidence of active targeting:
Yes - attacker is targeting network devices. No logs indicated an attempt to connect to other IP addresses.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 5 (Network device)
Lethality = 4 (Attacker can gain critical network access)
Countermeasures: System = 5 (Operating system up to date, strong SNMP community strings); Net = 5 (SNMP blocked by firewall)
Severity = -1

9. Defensive recommendation:
Block SNMP traffic at firewall, do not use default or easy to guess community strings

10. The source port and packet length of the above trace indicates:
a) Crafted packets
b) Walking the MIB
c) Network mapping via UDP echo request
d) Information gathering via SNMP to broadcast address

Answer: a

**Note: Detect 3 contains lab generated port scans. The purpose of creating these scans is to practice identifying port scanning methods and tools in order to evaluate the severity of the scan.

Detect 3.A
Internet Maniac
http://www.csee.usf.edu/~birla/

18:34:15 drop firewall >if0 proto tcp src 10.255.256.0 dst www.externalhost.com service 1024 s_port 1172 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 21548 xlatedport 1024
18:34:20 drop firewall >if0 proto tcp src 10.255.256.0 dst www.externalhost.com service 1025 s_port 1173 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 21548 xlatedport 1025

Elizabeth Martin
SANS GIAC Intrusion Detection
Practical Assignment

18:34:25 drop firewall >if0 proto tcp src 10.255.256.0 dst www.externalhost.com service 1026 s_port 1174 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 21548 xlatedport 1026

<snip snip, and tcpdump says…>

19:27:17.880794 10.256.255.195.1416 > firewall .2: S 8478825:8478825(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0x84]
19:27:18.184173 10.256.255.195.1418 > firewall.4: S 8488904:8488904(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xc8]

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
18:35:41 [timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto tcp** [protocol] **src 10.255.256.0** [source IP address] **dst www.externalhost.com service** [destination IP address] **1041** [destination service] **s_port 1189** [source port] **len 64** [IP datagram length] **rule 18** [firewall rule number] **xlatesrc 256.192.45.6** [translated source IP address] **xlatedst www.externalhost.com** [translated destination IP address] **xlatesport 21550** [translated source port] **xlatedport 1041** [translated destination port]

**Note: The firewall translates the source port in order to maintain multiple connections while performing address translation

3. Probability the source address was spoofed
Low. Attacker would gain nothing from spoofing an IP address. This is a reconnaissance attack, attacker is attempting to retrieve information

4. Description of attack:
Attacker is scanning a host for open tcp ports

5. Attack mechanism:
Attacker scans host for open ports, based on the response can attempt to exploit a host based vulnerability. This type of attack is used for reconnaissance, most likely if scan is successful attacker will return later and attempt an exploit. Note the following:

a) Scanning is most likely taking place by a not so robust automated tool
b) Incremental source port
c) 5 second timestamp

d) Destination of the scan is a single host (higher number in the IP range), not a network, broadcast, or low number device IP address.
e) This is a multiscan
f) The only configuration options this tool provides is the port range to scan (as specified by beginning and ending port number) and hosts to scan (single target host or single target domain).

6. Correlations:
securityportal.com
http://www.securityportal.com/topnews/tn19990721.html
http://www.enteract.com/~lspitz/pubs.html
http://phrack.infonexus.com/
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 263

7. Evidence of active targeting:
Yes, scanner is targeting one specific host

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (External host)
Lethality = 1 (Attack is very unlikely to succeed)
Countermeasures: System = 5 (Operating system up to date, no unnecessary services running on host); Net = 5 (All ports blocked by firewall)
Severity = -7

9. Defensive recommendation:
Make a policy statement; that which is not explicitly allowed is denied. Block all ports other than the standard web ports such as http, ftp, telnet. Do not allow the icmps, SNMPs. In addition do not run any unnecessary services on the host. Ensure host operating system and applications are up to date with all required patches, fixes, version upgrades, etc.

10. The timestamps of the packets indicate:
a) This is a manual scan
b) Timeout is set to 5 seconds
c) This is a low and slow scan
d) This is a Mscan on steroids

Answer: b

Detect 3.B
Yaps

http://hotbot.lycos.com/director.asp?target=http%3A%2F%2Fwww%2Etni%2Enet%2F%7Eted%2FYaps%2FYaps%2Ehtml&id=3&userid=48EoiKTi8FAz&query=MT=port

18:18:35 drop firewall >if0 proto udp src 10.256.255.195 dst www.externalhost.com service nbname s_port nbname len 78 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 603 xlatedport nbname
18:18:39 drop firewall >if0 proto icmp src 10.256.255.195 dst www.externalhost.com rule 18 icmp-type 8 icmp-code 0 xlatesrc 256.192.45.6 xlatedst www.externalhost.com
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service echo s_port 1196 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport echo
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service daytime s_port 1197 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport daytime
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service chargen s_port 1198 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport chargen
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service telnet s_port 1200 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport telnet
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service mail s_port 1201 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport mail
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service time s_port 1202 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport time
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service domain s_port 1203 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport domain
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 69 s_port 1204 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 69
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service finger s_port 1205 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport finger
18:19:10 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service http s_port 1206 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport http
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 88 s_port 1207 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 88
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 90 s_port 1209 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 90
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 91 s_port 1210 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 91
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 92 s_port 1211 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 92
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service 94 s_port 1213 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport 94
18:19:40 drop firewall >if0 proto tcp src 10.256.255.195 dst www.externalhost.com service supdup s_port 1214 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 26228 xlatedport supdup

….<snip snip> and a tcpdump says….

19:05:59.711542 10.256.255.195.1367 > www.externalhost.com.telnet: S 7187409:7187409(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xd0]
19:05:59.711563 10.256.255.195.1368 > www.externalhost.com.24: S 7187409:7187409(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xc]
19:06:10.971727 10.256.255.195.1369 > www.externalhost.com.139: S 7218354:7218354(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xb0]

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
18:35:41 [timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto tcp** [protocol] **src 10.255.256.0** [source IP address] **dst www.externalhost.com service** [destination IP address] **1041** [destination service] **s_port 1189** [source port] **len 64** [IP datagram length] **rule 18** [firewall rule number] **xlatesrc 256.192.45.6** [translated source IP address] **xlatedst www.externalhost.com** [translated destination IP address] **xlatesport 21550** [translated source port] **xlatedport 1041** [translated destination port]

**Note: The firewall translates the source port in order to maintain multiple connections while performing address translation

3. Probability the source address was spoofed
Low. Attacker would gain nothing from spoofing an IP address. This is a reconnaissance attack, attacker is attempting to retrieve information

4. Description of attack:
Attacker is scanning a host for open ports

5. Attack mechanism:
Attacker scans host for open ports, based on the response can attempt to exploit a host based vulnerability. This type of attack is used for reconnaissance, most likely if scan is successful attacker will return later and attempt an exploit.

Scanning is most likely taking place by a more robust automated tool than the previous detect (3 A.) Note the following:

a) The pattern, in that initially a number of services are scanned and the order is not related to port numbers, then sequential ports are scanned, then services again. This tool interchanges the services/ports scanned perhaps in an attempt to avoid detection with a not so obvious pattern.
b) Inconsistent sequence number
c) Incremental source port.
d) Scan is not strictly tcp, it interchanges icmp, tcp, and udp.
e) The tool allows for a range of IP addresses to be scanned as specified by beginning and ending host
f) Port numbers, timout, threads, and sockets are configurable.

6. Correlations:
securityportal.com
http://www.securityportal.com/topnews/tn19990721.html
http://www.enteract.com/~lspitz/pubs.html
http://phrack.infonexus.com/
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 263

7. Evidence of active targeting:
Yes, scanner is targeting one specific host

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (External host)
Lethality = 1 (Attack is very unlikely to succeed)
Countermeasures: System = 5 (Operating system up to date, no unnecessary services running on host); Net = 5 (All ports blocked by firewall)
Severity = -7

9. Defensive recommendation:
Make a policy statement; that which is not explicitly allowed is denied. Block all ports outbound other than the standard web ports such as http, ftp, telnet. Do not allow the icmps, SNMPs. In addition do not run any unnecessary services on the host. Ensure host operating system and applications are up to date with all required patches, fixes, version upgrades, etc.

10. One of the major differences between trace 3A and 3B is:
a) One tool contains incremental source ports, the other a constant source port
b) One tool negotiates a maximum segment size of 1460, the other a mss of 1024.
c) One tool scans tcp only, the other icmp and udp as well as tcp
d) One tool is automated and one tool is a manual port scan.

Answer: c

Detect 3.C
BlueGlobe
http://www.blueglobe.com/~cliffmcc/portscanner.html

22:21:11 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service ident s_port 1931 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport ident
22:21:19 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service 531 s_port 1932 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport 531
22:21:26 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service courier s_port 1933 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport courier
22:21:33 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service daytime s_port 1934 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport daytime
22:21:41 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service discard s_port 1935 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport discard
22:21:48 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service domain s_port 1936 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport domain
22:21:55 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service echo s_port 1937 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22197 xlatedport echo
22:22:02 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service 520 s_port 1938 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport 520
22:22:10 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service exec s_port 1939 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport exec
22:22:17 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service finger s_port 1940 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport finger
22:22:26 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service hostnames s_port 1942 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport hostnames
22:22:34 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service 8000 s_port 1943 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport 8000
22:22:44 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service ingreslock s_port 1944 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport ingreslock
22:22:48 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service link s_port 1949 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport link
22:22:55 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service login s_port 1950 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22198 xlatedport login
22:23:03 drop firewall >ef0 proto tcp src 10.256.255.195 dst www.externalhost.com service 57 s_port 1951 len 64 rule 18 xlatesrc 256.192.45.6 xlatedst www.externalhost.com xlatesport 22199 xlatedport 57

<snip, tcpdump>
19:59:46.410129 10.256.255.195.1582 > www.externalhost.com.courier: S 10427587:10427587(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0x84]
19:59:47.178489 10.256.255.195.1583 > www.externalhost.com.daytime: S 10434869:10434869(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xc8]

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
18:35:41 [timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto tcp** [protocol] **src 10.255.256.0** [source IP address] **dst www.externalhost.com service** [destination IP address] **1041** [destination service] **s_port 1189** [source port] **len 64** [IP datagram length] **rule 18** [firewall rule number] **xlatesrc 256.192.45.6** [translated source IP address] **xlatedst www.externalhost.com** [translated destination IP address] **xlatesport 21550** [translated source port] **xlatedport 1041** [translated destination port]

**Note: The firewall translates the source port in order to maintain multiple connections while performing address translation

3. Probability the source address was spoofed
Low. Attacker would gain nothing from spoofing an IP address. This is a reconnaissance attack, attacker is attempting to retrieve information

4. Description of attack:
Attacker is scanning a host for open ports

5. Attack mechanism:
Attacker scans host for open ports, based on the response can attempt to exploit a host based vulnerability. This type of attack is used for reconnaissance, most likely if scan is successful attacker will return later and attempt an exploit.

Note the following:
g) The pattern, the ports are scanned in exactly the order in which they are configured and then the scan stops.
h) Inconsistent sequence number
i) Incremental source port.
j) Scan is strictly tcp

k) The tool allows for a range of IP addresses to be scanned (as specified by beginning and ending IP address) as well as Class B and C networks
l) This tool offers the option of incorporating a homegrown script.
m) Only the ports and timeout are configurable

6. Correlations:
securityportal.com
http://www.securityportal.com/topnews/tn19990721.html
http://www.enteract.com/~lspitz/pubs.html
http://phrack.infonexus.com/
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 263

7. Evidence of active targeting:
Yes, scanner is targeting one specific host

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (External host)
Lethality = 1 (Attack is very unlikely to succeed)
Countermeasures: System = 5 (Operating system up to date, no unnecessary services running on host); Net = 5 (All ports blocked by firewall)
Severity = -7

9. Defensive recommendation:
Make a policy statement; that which is not explicitly allowed is denied. Block all ports outbound other than the standard web ports such as http, ftp, telnet. Do not allow the icmps, SNMPs. In addition do not run any unnecessary services on the host. Ensure host operating system and applications are up to date with all required patches, fixes, version upgrades, etc.

10. This tool can be used to:
a) Scan a Class C network for a web farm by specifying only web related ports
b) Scan a network address, then broadcast address, then network, then broadcast
c) Determine version number of a BIND server running DNS
d) Launch a denial of service attack
Answer: a

Detect 3.D

http://www.cl.spb.ru/sparta/ftp/proxyht280.exe

23:41:37 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.52 service 8080 s_port 2693 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.52 xlatesport 23236 xlatedport 8080
23:41:38 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.53 service 8080 s_port 2694 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.53 xlatesport 23236 xlatedport 8080
23:41:40 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.55 service 8080 s_port 2696 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 10.0.248.36 xlatesport 10181 xlatedport 8080
23:41:41 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.56 service 8080 s_port 2697 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.56 xlatesport 23236 xlatedport 8080
23:41:42 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.57 service 8080 s_port 2698 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.57 xlatesport 23236 xlatedport 8080
23:41:44 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.58 service 8080 s_port 2699 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.58 xlatesport 23236 xlatedport 8080
23:41:45 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.59 service 8080 s_port 2700 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.59 xlatesport 23236 xlatedport 8080
23:41:46 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.60 service 8080 s_port 2701 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.60 xlatesport 23236 xlatedport 8080
23:41:47 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.61 service 8080 s_port 2702 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.61 xlatesport 23236 xlatedport 8080
23:41:48 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.62 service 8080 s_port 2703 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 10.253.88.252 xlatesport 10181 xlatedport 8080
23:41:50 drop firewall >ef0 proto tcp src 10.256.255.195 dst 256.252.68.63 service 8080 s_port 2704 len 64 rule 18 xlatesrc 256.252.45.32 xlatedst 256.252.68.63 xlatesport 23236 xlatedport 8080

<snip snip, tcpdump…>

19:45:17.829230 10.256.255.195.1449 > 256.252.68.32 .8080: S 9568655:9568655(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0xc8]
19:45:17.833695 10.256.255.195.1450 > 256.252.68.33.8080: S 9568660:9568660(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos 0x84]

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
18:35:41 [timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto tcp** [protocol] **src 10.255.256.0** [source IP address] **dst www.externalhost.com service** [destination IP address] **1041** [destination

service] **s_port 1189** [source port] **len 64** [IP datagram length] **rule 18** [firewall rule number] **xlatesrc 256.192.45.6** [translated source IP address] **xlatedst www.externalhost.com** [translated destination IP address] **xlatesport 21550** [translated source port] **xlatedport 1041** [translated destination port]

**Note: The firewall translates the source port in order to maintain multiple connections while performing address translation

3. Probability the source address was spoofed
Low. Attacker would gain nothing from spoofing an IP address. This is a reconnaissance attack, attacker is attempting to retrieve information

4. Description of attack:
Attacker is scanning a network for proxy servers

5. Attack mechanism:
Attacker scans network for hosts listening on port 8080 in an attempt to identify proxy servers for the purpose of using the newly discovered proxy server to mask identity, or to exploit a host based vulnerability. This type of attack is used for reconnaissance, most likely if scan is successful attacker will return later and attempt an exploit.

Note the following:
a) The pattern, the IP addresses increment while the port remains constant
b) Inconsistent sequence number
c) Incremental source port.
d) Scan is strictly tcp
e) The tool allows for a range of IP addresses to be scanned (as specified by beginning and ending IP address) and also allows for multiple ranges to be scanned
f) This tool offers the option of configuring connect timeout, parallel options, ports to be scanned, and allows a ProxySwitch to be used. In addition it allows for an intranet proxy to be used for scanning (allowing for a little anonymity)
g) As a note this does not appear to be RingZero related as you would see scans for 80, 3128 and 8080 or outbound traffic on one of these ports.

6. Correlations:
securityportal.com
http://www.securityportal.com/topnews/tn19990721.html
http://www.enteract.com/~lspitz/pubs.html
http://phrack.infonexus.com/
http://www.sans.org/y2k/proxy.htm
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 152

CVE-1999-0290
The WinGate telnet proxy allows remote attackers to cause a denial of service via a large number of connections to localhost.

CVE-1999-0291
The WinGate proxy is installed without a password, which allows remote attackers to redirect connections without authentication.

CVE-1999-0471
The remote proxy server in Winroute allows a remote attacker to reconfigure the proxy without authentication through the "cancel" button.

7. Evidence of active targeting:
Not necessarily, attacker is looking for the target proxy server by scanning the network. The attacker can very well not find anything and leave.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (External host)
Lethality = 1 (Attack is very unlikely to succeed)
Countermeasures: System = 5 (Operating system up to date, no unnecessary services running on host); Net = 5 (All ports blocked by firewall)
Severity = -7

9. Defensive recommendation:
Block incoming traffic from the Internet to your proxy server. The proxy server need only to connect outbound, and inbound connections need only come from your internal network. Ensure host operating system and applications are up to date with all required patches, fixes, version upgrades, etc.

10. This tool can be used as the first step in the following process:
   a) Scan a network for any particular service
   b) Identify a proxy server, proxy platform, operating system, then exploit a known vulnerability to poison the cache
   c) Identify a web server, web platform, operating system, then exploit a known vulnerability.
   d) All of the above

   Answer: d

**Note: The above analysis was lab generated, therefore, the analysis of the specific source, destination, and particular ports was not valid and not included. It is understood that with any type of port scan these items are

critical to the analysis as they will determine what the attacker is looking for and whether or not they have a chance of finding it. Again the purpose of this detect was to become familiar with the scanning tools that are easily available and easy to use.

Detect 4

21:27:43 accept firewall >if0 proto tcp src 10.256.255.98 dst 208.184.216.237 service http s_port 1614 len 48 rule 14 xlatesrc 256.252.45.32 xlatedst 208.184.216.237 xlatesport 22049 xlatedport http
21:27:44 accept firewall >if0 proto tcp src 10.256.255.98 dst 208.184.216.223 service 8875 s_port 1615 len 48 rule 14 xlatesrc 256.252.45.32 xlatedst 208.184.216.223 xlatesport 22050 xlatedport 8875
21:27:44 accept firewall >if0 proto tcp src 10.256.255.98 dst 208.184.216.202 service 8888 s_port 1616 len 48 rule 14 xlatesrc 256.252.45.32 xlatedst 208.184.216.202 xlatesport 22051 xlatedport 8888
21:27:46 accept firewall >if0 proto tcp src 10.256.255.98 dst 208.184.216.237 service http s_port 1617 len 48 rule 14 xlatesrc 256.252.45.32 xlatedst 208.184.216.237 xlatesport 22052 xlatedport http
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 1.2.3.4 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 1.2.3.4
21:27:53 drop firewall >ef0 proto icmp src 204.167.134.157 dst 10.256.255.98 rule 18 icmp-type 3 icmp-code 1 xlatesrc 204.167.134.157 xlatedst 10.256.255.98
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 199.240.159.233 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 199.240.159.233
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 212.253.237.14 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 212.253.237.14
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 194.22.193.213 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 194.22.193.213
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 212.16.0.125 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 212.16.0.125
21:27:53 accept firewall >if0 proto icmp src 10.256.255.98 dst 216.15.97.83 rule 14 icmp-type 8 icmp-code 0 xlatesrc 256.252.45.32 xlatedst 216.15.97.83
21:27:53 drop firewall >ef0 proto icmp src 199.240.159.233 dst 10.256.255.98 rule 18 icmp-type 0 icmp-code 0 xlatesrc 199.240.159.233 xlatedst 10.256.255.98

Interesting…..wonder why my user running an automated ping to a bunch of external sources…..let's look at the traffic

10.256.255.98 -> 208.184.216.180 TCP D=7777 S=1612 Ack=3817813115 Seq=2520762
87 Len=50 Win=17500

```
 0: 0800 20a0 1366 0000 863c dfe9 0800 4500    .. ..f...<....E.
16: 005a 945e 4000 8006 9352 0a1e 1f62 d0b8    .Z.^@....R...b..
32: d8b4 064c 1e61 0f06 60ff e38f 347b 5018    ...L.a..`...4{P.
```

```
48: 445c 3d09 0000 2e00 c800 4649 4c45 4e41    D\=.....FILENA
64: 4d45 2043 4f4e 5441 494e 5320 2269 6365    ME CONTAINS "ice
80: 6420 6561 7274 6822 204d 4158 5f52 4553    d earth" MAX_RES
96: 554c 5453 2031 3030                        ULTS 100
```

208.184.216.202.napster.com -> 10.256.255.98 TCP D=1616 S=8888 Ack=281268446 Seq=3949772282 Len=20 Win=16060

```
 0: 0000 863c dfe9 0800 20a0 1366 0800 4500    ...<.... ..f..E.
16: 003c 1bb3 4000 3006 5c06 d0b8 d8ca 0a1e    .<..@.0.\.......
32: 1f62 22b8 0650 eb6c bdfa 10c3 d0de 5018    .b"..P.l......P.
48: 3ebc ed74 0000 1000 0300 616e 6f6e 406e    >..t......anon@n
64: 6170 7374 6572 2e63 6f6d                   apster.com
```

1. Source of trace
My network

2. Detect was generated by:
Checkpoint Firewall-1 v4.0

Explanation of Fields:
18:35:41 [timestamp] **drop** [action] **firewall** [hostname] **>if0** [internal interface name] **proto tcp** [protocol] **src 10.255.256.0** [source IP address] **dst www.externalhost.com service** [destination IP address] **1041** [destination service] **s_port 1189** [source port] **len 64** [IP datagram length] **rule 18** [firewall rule number] **xlatesrc 256.192.45.6** [translated source IP address] **xlatedst www.externalhost.com** [translated destination IP address] **xlatesport 21550** [translated source port] **xlatedport 1041** [translated destination port]

**Note: The firewall translates the source port in order to maintain multiple connections while performing address translation

3. Probability the source address was spoofed
None. This traffic was identifying on a firewall with restricted access, the user was quickly identified.

4. Description of attack:
Initially only the ICMP (echo and echo reply) traffic existed in the logs. The timestamps indicated this traffic was not generated manually, leading to the conclusion some type of utility, tool, application, etc. was sending the echo request. Definitely something to investigate. Verbose snoops of the traffic showed a login at napster.com. Mystery solved.

5. Attack mechanism:

User browses to the napster site over http, logs in over TCP 8888 and 8875, then proceeds to run a search requesting a certain music group. Upon identifying the servers hosting mp3s by this group, it pings each server to determine the best response time, then downloads the music files.

It should be noted that this application can potentially lead to a Denial of Service attack if multiple users within the organization are using Napster. Scores of Napster sites can be responding to each individual user with echo replies, flooding the network.

6. Correlations:
http://napster.cjb.net/

7. Evidence of active targeting:
No

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (End user)
Lethality = 1 (Any potential attacks are very unlikely to succeed)
Countermeasures: System = 5 (Operating system up to date, end user has not opened up sharing on desktop); Net = 4 (All inbound ports blocked by firewall)
Severity = -6

9. Defensive recommendation:
Do not allow ICMPs into your network, do not open up your machine for sharing with the Napster software. Make a policy statement, no Napster, no Gnutella.

10. The ICMP type codes in the above trace indicate:
   a) External host returning a redirect message
   b) Internal host arping for external host
   c) Internal host sends an echo request, and external host replies with echo reply
   d) Major network problems – the Internet must be down

   Answer: c

Detect 5

Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3483
to server1/27374 flags SYN
Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-7-106011:

Deny inbound (No xlate) tcp src outside:216.58.19.218/3487
dst outside:global/27374
Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3488
to server2/27374 flags SYN
Jun 03 00:06:27 [FW1] Jun 03 2000 00:08:01: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3483
to server1/27374 flags SYN
Jun 03 00:06:27 [FW1] Jun 03 2000 00:08:01: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3488
to server2/27374 flags SYN
Jun 03 00:06:28 [FW1] Jun 03 2000 00:08:02: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3488
to server2/27374 flags SYN
Jun 03 00:06:29 [FW1] Jun 03 2000 00:08:03: %PIX-7-106011:
Deny inbound (No xlate) tcp src outside:216.58.19.218/3487
dst outside:global/27374
Jun 03 00:06:29 [FW1] Jun 03 2000 00:08:03: %PIX-2-106001:
Inbound TCP connection denied from 216.58.19.218/3491
to server3/27374 flags SYN

1. Source of trace
http://www.sans.org/y2k/060600.htm

2. Detect was generated by:
Cisco PIX Firewall

Explanation of Fields:
Not available; Assumed as follows:

Jun 03 00:06:29 [timestamp] **[FW1]** [hostname] **Jun 03 2000 00:08:03: %PIX-2-106001:**
Inbound TCP connection denied from 216.58.19.218/3491 [action]
to server3/27374 flags SYN

3. Probability the source address was spoofed
Low. Attacker is looking for a machine infected with SubSeven 2.1 backdoor. Attacker will need return traffic to remotely control infected host

4. Description of attack:
Attacker is attempting to connect to a machine that is thought to be infected with the SubSeven 2.1 Backdoor.

5. Attack mechanism:
Attacker sends an infected file to the target user (usually via email). The end user launches the file and proceeds to infect the host on which the file was launched. The attacker then attempts a connection to the host and uses SubSeven as a backdoor to remotely control the host. SubSeven allows for remotely searching/retrieving/sending files, stealing passwords, changing the colors/resolution, playing sounds and changing the date/time.

6. Correlations:
securityportal.com
http://www.symantec.com/region/uk/avcenter/venc/subseven_20_server.html
http://www.onctek.com/trojanports.html

7. Evidence of active targeting:
No, attacker is looking for an infected machine but does not know of one.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 3 (Assumed a general server, not a DNS, mail server, etc.)
Lethality = 3 (If attacker succeeded, could gain access to network)
Countermeasures: System = 5 (Assumed operating system up to date, no unnecessary services running on host); Net = 5 (This port blocked by firewall)
Severity = -4

9. Defensive recommendation:
Maintain up to date virus definitions on all platforms. Block this port at the firewall, monitor outbound traffic on this port in an effort to identify infected hosts.

1. SubSeven 2.1 is considered to be a:
   a) Worm
   b) Network scanning tool
   c) Trojan providing a backdoor to an infected host
   d) Tool commonly used in the industry to evaluate desktop security

   Answer: c

Detect 6

May 30 16:09:31 [A.B.C.E.35.74] 3135: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.9.29(0) -> 208.48.26.226(0), 1 packet

May 30 16:10:12 [A.B.C.E.35.74] 3136: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.9.165(0) -> 204.202.130.240(0), 2 packets
May 30 16:15:12 [A.B.C.E.35.74] 3137: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.9.29(0) -> 208.48.26.226(0), 1 packet
May 30 16:16:31 [A.B.C.E.35.74] 3138: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.41.64(0) -> 204.216.27.21(0), 1 packet
May 30 16:24:43 [A.B.C.E.35.74] 3139: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.42.84(0) -> 209.173.195.35(0), 1 packet
May 30 16:26:12 [A.B.C.E.35.74] 3140: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.9.29(0) -> 208.48.26.226(0), 1 packet
May 30 16:30:13 [A.B.C.E.35.74] 3141: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.42.84(0) -> 209.173.195.35(0), 23 packets
May 30 16:31:19 [A.B.C.E.35.74] 3142: %SEC-6-IPACCESSLOGP:
list 101 denied tcp X.Y.42.29(0) -> 128.11.45.101(0), 1 packet

1. Source of trace
http://www.sans.org/y2k/060400.htm

2. Detect was generated by:
Cisco Access Control Log

Explanation of Fields (complements of Mark Thyer obtained from GIAC site) :
Mar 31 13:55:07[Timestamp] **A.B.C.E.35.74** [hostname] **3141: %SEC-6-IPACCESSLOGP:**
list 101 [router ACL responsible for action] **denied** [action] **tcp** [transport protocol] **X.Y.42.84 (0)** [source address and port]**-> 128.11.45.101 (0)** [destination address and port]**, 1 packet**

3. Probability the source address was spoofed
Low. Detects are coming from an internal source

4. Description of attack:
With a lack of information, this is a long shot but a possibility that the firewall has been the victim of a Denial of Service attack, causing sporadic behavior. Also possibly a misconfigured firewall.

5. Attack mechanism:
Attacker targets FW-1 running ISAKMP encryption, and sends crafted UDP packets containing a source port of 0. FW-1 then suffers, leading sporadic behavior. The above traces most likely are not the DoS itself, as they are tcp packets and the target is a general web server on the Internet. In addition, multiple hosts are seeing the same response.

6. Correlations:

CVE #CAN-1999-0675 (under review)

7. Evidence of active targeting:
Yes, if true attacker has targeted FW-1.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 5 (Firewall)
Lethality = 5 (Compromised firewall, misbehaving, pretty lethal)
Countermeasures: System = 3 (Assumed operating system and not up to date and vulnerable); Net = 3 (Port 0 blocked but NAT not working)
Severity = 4

9. Defensive recommendation:
Update operating system and platform with fix to DoS, recreate in a lab environment and identify potential misconfigurations. Continue to monitor and investigate

10. Possible cause of source and destination port 0
    a) Misconfiguration of port translation rules
    b) Corrupt rule base
    c) Successful Denial of Service
    d) All of the Above

    Answer: d

Detect 7

195.76.27.44 > MY.NET.1.1
23:00:08.268287 195.76.27.44.65535 > MY.NET.1.1.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:00:08.271916 195.76.27.44.65535 > MY.NET.1.2.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:00:08.294812 195.76.27.44.65535 > MY.NET.1.3.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:00:08.317808 195.76.27.44.65535 > MY.NET.1.4.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:00:08.330230 195.76.27.44.65535 > MY.NET.1.5.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:21:38.484746 195.76.27.44.65535 > MY.NET.254.246.53:

S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:21:38.497681 195.76.27.44.65535 > MY.NET.254.247.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:21:38.510206 195.76.27.44.65535 > MY.NET.254.248.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:21:38.531702 195.76.27.44.65535 > MY.NET.254.249.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)
23:21:38.548972 195.76.27.44.65535 > MY.NET.254.250.53:
S 2047410176:2047410176(0) win 512 (ttl 241, id 31241)

1. Source of trace
http://www.sans.org/y2k/060300.htm

2. Detect was generated by:
Unknown

Explanation of Fields
Not available, assumption as follows:
23:21:38.548972 [Timestamp] **195.76.27.44.65535)** [source address and port] **> MY.NET.254.250.53**[destination address and port]**: S 2047410176:2047410176(0)** [sequence number]**win 512** [window size] **(ttl 241**[time to live]**, id 31241** [id #]**)**

3. Probability the source address was spoofed
Low. Attacker is scanning for DNS servers and needs the return traffic to find them. IP address is registered to an organization in Spain, obtained from ripe.net.

4. Description of attack:
Attacker is scanning for DNS servers

5. Attack mechanism:
Attacker scans network for DNS servers. Upon identifying the DNS servers will most likely return to attempt to exploit a known vulnerability such as inverse query scans, cache poisoning, or malicious zone transfer attempts. These packets appear to be crafted due to the following:

1. Constant source port of 65535
2. Constant sequence number
3. Constant ttl
4. Constant id #

6. Correlations:

SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 289; Discussion regarding source ports of 0 and 65535
SANS GIAC TCP/IP for Intrusion Detection and Perimeter Defense; 2.1; pages 4-18 through 4-31
http://www.sans.org/y2k/061200.htm

7. Evidence of active targeting:
No, attacker is looking but not sure if DNS servers exist

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 5 (DNS Server)
Lethality = 5 (If entire attack including exploit is successful)
Countermeasures: System = 5 (Assumed operating system up to date, no unnecessary services running on host); Net = 2 Assume this traffic not blocked (otherwise how would the world query their DNS server?)
Severity = 3

9. Defensive recommendation:
Ensure operating system and DNS platform is up to date with all appropriate upgrades, patches, etc. Monitor traffic to this server

10. The above trace illustrates a signature that:
a) Is indicative of an inverse query exploit
b) Is indicative of a bot attempting to determine response times to / from DNS servers on the Internet
c) Is indicative of a Land Attack
d) Is indicative of crafted packets

Answer: d

Detect 8

May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2496 dst xxx.xxx.xxx.0/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2497 dst xxx.xxx.xxx.1/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2498 dst xxx.xxx.xxx.2/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2499 dst xxx.xxx.xxx.3/111
May 12 14:48:58 : Deny inbound tcp src

210.104.234.5/2500 dst xxx.xxx.xxx.4/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2501 dst xxx.xxx.xxx.5/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2502 dst xxx.xxx.xxx.6/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2503 dst xxx.xxx.xxx.7/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2504 dst xxx.xxx.xxx.8/111
May 12 14:48:58 : Deny inbound tcp src
210.104.234.5/2505 dst xxx.xxx.xxx.9/111
May 12 14:48:59 : Deny inbound tcp src
210.104.234.5/2506 dst xxx.xxx.xxx.10/111
May 12 14:48:59 : Deny inbound tcp src
210.104.234.5/2507 dst xxx.xxx.xxx.11/111
May 12 14:48:59 : Deny inbound tcp src
210.104.234.5/2508 dst xxx.xxx.xxx.12/111

1. Source of trace
http://www.sans.org/y2k/060100.htm

2. Detect was generated by:
Unknown

Explanation of Fields
Not available, assumption as follows:
May 12 14:48:59 [Timestamp]**: Deny inbound** [Action] **tcp** [protocol]**src**
210.104.234.5/2508 [source address and port] **dst xxx.xxx.xxx.12/111** [destination address and port]

3. Probability the source address was spoofed
Medium, the low range is questionable, however, attacker gains nothing from a spoofed IP address. IP is registered to Korea Telecom……

4. Description of attack:
Attacker is scanning for servers running Portmapper

5. Attack mechanism:
Attacker scans network for Unix systems running portmapper. Upon identifying the hosts running portmapper, attacker can attempt any number of RPC attacks. If the system is vulnerable, attacker could gain access to the file system as well as obtain information about the system.

6. Correlations:
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 269;

7. Evidence of active targeting:
No, attacker is looking for Unix systems but is not aware of any

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (Assuming workstations)
Lethality = 3 (Can obtain confidential information, or gain root access)
Countermeasures: System = 5 (Assumed operating system up to date, no unnecessary services running on host); Net = 5 (Traffic is blocked)
Severity = -5

9. Defensive recommendation:
Ensure operating system is up to date with all appropriate upgrades, patches, etc. Block all NFS and portmapper traffic

10. SunRPC attacks could lead to:
a) Compromise of an NT operating system
b) Compromise of a Unix file system
c) Distributed Denial of Service attacks
d) An attempt to SNMP "GetRequest" attack

Answer: b

Detect 9

May 29 12:27:40 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.48.137
May 29 12:27:49 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.49.137
May 29 12:28:01 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.50.137
May 29 12:28:02 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.50.137
May 29 12:28:10 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.51.137

May 29 12:28:19 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.52.137
May 29 12:28:28 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.53.137
May 29 12:28:39 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.54.137
May 29 12:28:42 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.54.137
May 29 12:28:48 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.55.137
May 29 12:29:57 pyramid 28 deny: UDP from
208.21.150.39.137 to 204.245.8.62.137

1. Source of trace
http://www.sans.org/y2k/053100.htm

2. Detect was generated by:
Unknown

Explanation of Fields
Not available; Assumptions as follows
May 29 12:29:57 [Timestamp] **pyramid 28** [hostname] **deny** [Action]**: UDP** [protocol] **from 208.21.150.39.137** [source IP address and port] **to 204.245.8.62.137** [destination IP address and port]

3. Probability the source address was spoofed
Low, again this is an information gathering attack. Attacker gains nothing from a spoofed IP address. IP Address is registered to sprint.net, ISP.

4. Description of attack:
Attacker is scanning for servers running NetBios

5. Attack mechanism:
Attacker scans network for Windows systems in an effort to obtain system information such as user ids and workgroups. Upon identifying the hosts running NetBios attacker can run any slew of Windows based attacks, including name-service attacks.

6. Correlations:
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 293 - 295;

7. Evidence of active targeting:

No, attacker is looking for Windows based systems but is not aware of any

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 2 (Assuming workstations)
Lethality = 5 (Can obtain confidential information, system information, can also obtain access to network)
Countermeasures: System = 5 (Assumed operating system up to date); Net = 5 (Traffic is blocked)
Severity = -3

9. Defensive recommendation:
Ensure operating system is up to date with all appropriate upgrades, patches, etc. Block all NetBios and ports in the 130 – 140 range.

10. Port 137 scans
a) Are indicative of Samba if the source and destination port is 137
b) Are launched in an effort to locate DNS servers running BIND
c) Are always UDP
d) Can lead to compromised Windows NT and 9x systems if allowed in the network

Answer: d

Detect 10

May 25 12:52:10 firewall kernel: Packet log: input DENY eth0 PROTO=6
206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=19973 F=0x4000 T=120 SYN
(#11)
May 25 12:52:13 firewall kernel: Packet log: input DENY eth0 PROTO=6
206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=20997 F=0x4000 T=120 SYN
(#11)
May 25 12:52:19 firewall kernel: Packet log: input DENY eth0 PROTO=6
206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=25093 F=0x4000 T=120 SYN
(#11)
May 25 12:52:31 firewall kernel: Packet log: input DENY eth0 PROTO=6
206.244.48.17:1060 MY.HOST.211:143 L=48 S=0x00 I=35333 F=0x4000 T=120 SYN
(#11)

1. Source of trace
http://www.sans.org/y2k/053000-1000.htm

2. Detect was generated by:
Unknown

Explanation of Fields
Not available; Assumptions as follows:
May 25 12:52:19 [Timestamp]**firewall kernel** [host]**: Packet log: input DENY** [action]**eth0** [interface]
PROTO=6 [protocol]
206.244.48.17:1060 [source address and port]**MY.HOST.211:143** [destination address and port] **L=48** [IP datagram length]**S=0x00 I=25093 F=0x4000 T=120 SYN** [flags]

3. Probability the source address was spoofed
Low, this really looks like a wrong number. IP address is registered to oar.net, ISP.

4. Description of attack:
It appears this 'attacker' is attempting to connect to an IMAP server. This could be a probe for an email server, or a wrong number

5. Attack mechanism:
The following items are indicative of a typical TCP retry:

a) Consistent source port
b) 4 retries, then an exit (unless there are additional log entries)
c) Timestamps are relatively far apart and not consistent
d) Target is a single host
e) Signatures of IMAP scans indicate SYN/FIN flags set, and source port 0

This is leading me to believe this is a wrong number, however, in the event the 'attacker' is scanning for IMAP servers, they could exploit any number of known IMAP vulnerabilities

6. Correlations:
SANS GIAC Network-Based Intrusion Detection Analysis; 2.4; page 281;
www.securityfocus.com

7. Evidence of active targeting:
No, looking for IMAP server but not sure if one exists

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
Criticality = 5 (Assuming email server)
Lethality = 2 (Doesn't appear attacker is trying very hard)
Countermeasures: System = 5 (Assumed operating system up to date); Net = 5 (Traffic is blocked)

Severity = -3

9. Defensive recommendation:
Ensure operating system and IMAP platform is up to date with all appropriate upgrades, patches, etc. Block all unnecessary 143 traffic.

10. The IMAP protocol:

a) Is typically used for bulletin board messages and email; stands for Internet Message Access Protocol
b) Is typically used for network mapping
c) Is frequently used in implementing a web proxy server
d) Can be used to exercise a DNS zone transfer attack

Answer: a