Kyle S. Nakamura

GCIA Practical Assignment

Assignment 1 – Network Detects

Detect 1

A:

TIME	EVENTNAME	PROTOCOL	SOURCE PORT	SOURCE ADDRESS	DEST PORT	DESTINATION ADDRESS	Tag Value
…							
09/23/2000 3:35:16 AM	Trace_Route	1	0	10.46.86.0	0	212.158.123.66	Echo request
09/23/2000 3:35:29 AM	Trace_Route	1	0	10.214.111.0	0	216.206.242.75	Echo request
09/23/2000 3:35:52 AM	Trace_Route	1	0	10.190.76.0	0	216.206.242.75	Echo request
09/23/2000 3:35:55 AM	Trace_Route	1	0	10.46.28.0	0	212.158.123.66	Echo request
09/23/2000 3:35:57 AM	Trace_Route	1	0	10.190.93.0	0	216.206.242.75	Echo request
09/23/2000 3:36:24 AM	Trace_Route	1	0	10.6.243.0	0	216.206.242.75	Echo request
09/23/2000 3:36:57 AM	Trace_Route	1	0	10.46.108.0	0	212.158.123.66	Echo request
09/23/2000 3:37:24 AM	Trace_Route	1	0	10.214.100.0	0	212.158.123.66	Echo request
09/23/2000 3:37:24 AM	Trace_Route	1	0	10.46.137.0	0	212.158.123.66	Echo request
09/23/2000 3:37:30 AM	Trace_Route	1	0	10.46.242.0	0	212.158.123.66	Echo request
09/23/2000 3:37:31 AM	Trace_Route	1	0	10.214.114.0	0	212.158.123.66	Echo request
09/23/2000 3:37:35 AM	Trace_Route	1	0	10.137.213.0	0	212.158.123.66	Echo request
…							

B:

```
…
23 9 2000 3:35:43Z : 209.100.86.1: 10.212.109.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:41Z : 207.31.112.33: 10.213.185.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:44Z : 209.100.86.1: 10.214.133.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:44Z : 207.31.112.33: 10.214.111.0:p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:44Z : 207.31.112.33: 10.214.237.0:  p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:49Z : 209.100.86.1: 10.190.63.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:53Z : 207.31.112.33: 10.214.125.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:35:57Z : 209.100.86.1: 10.212.13.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:36:0Z : 209.100.86.1: 10.213.32.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:36:0Z : 209.100.86.1: 10.212.99.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:36:9Z : 209.100.86.1: 10.190.76.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
23 9 2000 3:36:16Z : 207.31.112.33: 10.212.218.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
22 9 2000 20:37:16Z : 207.31.112.33: 10.137.180.0: p 1: pk 1 : size 56 :11/0 ttl exceeded
22 9 2000 20:37:28Z : 207.31.112.33: 10.137.162.0:p 1: pk 1 : size 56 :11/0 ttl exceeded
22 9 2000 20:37:20Z : 209.100.86.1: 10.137.37.0: p  1: pk 1 : size 56 :11/0 ttl exceeded
…
```

1. Source of Trace:
   Own network.

2. Detect was generated by:
   A. Real Secure: These logs were generated with Real Secure version 5.0. They were extracted directly from Real Secures Access database. The table comprises of select fields from the Real Secure database.

a. Time – Date and time of event in Zulu.
b. Eventname – The name of the signature that triggered. In this case "Traceroute."
c. Protocol – The protocol type (1 – ICMP, 6 – TCP, 17 – UDP). In this case ICMP.
d. Source port – Self-explanatory.
e. Source address – Source IP Address.
f. Dest port – Self-explanatory.
g. Dest address – Destination IP Address
h. Tag Value – Depending on the signature, Real Secure will insert important values into this field. Many times this will relate to the "Tag Name" field. In this case, Real Secure is identifying the traceroute as using ICMP echo packets.

B. Netflow is a tool integrated with Cisco routers for the purpose of traffic routing analysis. Netflow records header information on packets being forwarded on the network. Although Netflow can provide all packet header information, this extract only contains the following: Day Month Year Time(Zulu) : Source IP : Destination IP : Protocol type : Number of packets : Total size of packets in bytes : ICMP type/code description.

3. Probability the source address was spoofed:

It is likely this source address was spoofed. The question is more likely if this activity is the initiator or the response. As explained later in this detect, The activity is ICMP ttl exceeded messages from various source IP address to our Network addresses (X.X.X.0). As an initiator, the packets would have to be crafted packets with either spoofed sources or launched from multiple sites concurrently. As a response, it could be resulting packets to a denial of service attack using ICMP echo requests on an outside target using our network addresses as spoofed sources.

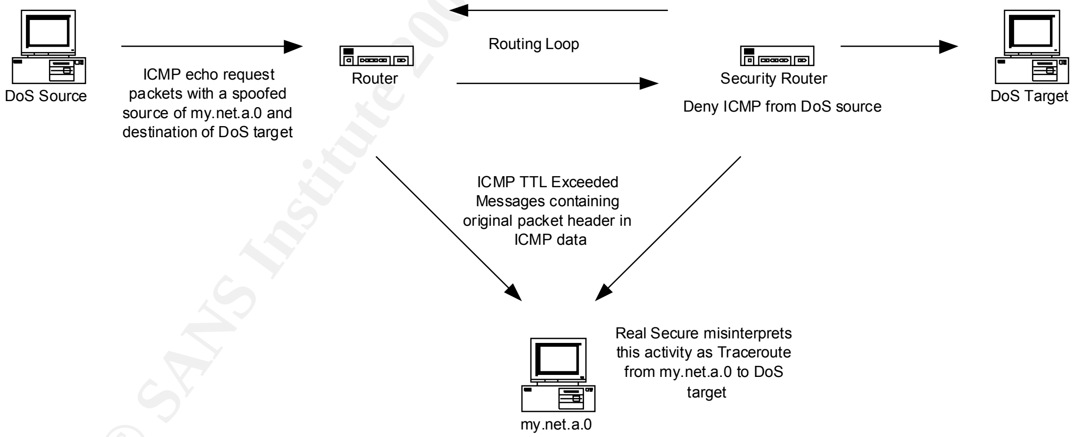
4. Description of attack:

Real Secure recorded numerous traceroutes from our network addresses (X.X.X.0) to a single destination IP on the outside our network. Real Secure reported traceroutes using "echo request". This should be impossible. There would be no device using a network address as its source. Even routers would use their interface IP in sending out traceroutes. Furthermore, only Microsoft traceroute implementations would use ICMP packets. Netflow logs of the activity did not reveal traffic to the traceroute destination IP address. There was activity involving network addresses, however they were the destination IP addresses, not the source. The source addresses were also completely different from the traceroute destination IP addresses. Apparently, Real Secure was triggering on the ttl exceeded messages and interpreting them as a traceroute. Furthermore, Real Secure reads the ICMP ttl exceeded message contents, which contain header information of the packet that generated this message and extracts the original destination IP address and records it as the traceroute destination IP address. This means the traceroute activity was actually misinterpreted ttl exceeded messages. The traceroute signature was triggered without any ICMP echo requests going out. The attack, if any, was ICMP ttl exceeded messages to our network addresses.

5. Attack mechanism:

There were two scenarios I came up with. The first was a denial of service attack using ICMP echo requests on an outside target using our network addresses as spoofed sources. If the target network administrator had reconfigured his or her network to redirect the ICMP echo requests out of the network, the packets would get caught up in a loop and eventually expire. This would generate the expected ICMP time exceeded message. This scenario seems unlikely because I would expect a routing loop would involve a single pair of neighboring routers. Although, the example involved only two IP addresses, it does not appear that these are neighboring routers. To support this further, other logs of similar activity involve several different IP addresses from networks that appear to be very far apart. The second scenario would be crafted ICMP packets. Although the more likely answer, I cannot determine the value for such an activity. In an experiment I duplicated these packets with a packet crafting utility. I received the same records in both Real Secure and Netflow logs. I did not observe any activity returned. (I didn't expect any response to ICMP ttl exceeded messages.) This brings me back to square one. What value does this activity have?

First scenario:


DoS Source
ICMP echo request packets with a spoofed source of my.net.a.0 and destination of DoS target
Router
Routing Loop
Security Router
Deny ICMP from DoS source
DoS Target
ICMP TTL Exceeded Messages containing original packet header in ICMP data
Real Secure misinterprets this activity as Traceroute from my.net.a.0 to DoS target
my.net.a.0

Host Info:

Host name: irc.ins.net.uk
IP address: 212.158.123.66
Alias(es): None

Host name: gots.the.leg-up.net
IP address: 216.206.242.75
Alias(es): 75.242.206.216.in-addr.arpa

```
                75.64/26.242.206.216.in-addr.arpa

          Host name: router.moof.net
          IP address: 209.100.86.1
          Alias(es): None

          No DNS record
          NetRail, Inc. (NETBLK-NETRAIL-BLK2)
            230 Peachtree St., Suite 1700
            Atlanta, GA 30303-1537
            US
            Netname: NETRAIL-BLK2
            Netblock: 207.31.64.0 - 207.31.127.255
            Maintainer: RAIL
```

6. Correlations:

This is a very common detect and was addressed by many analysts. I have also found reference to a book by Stephen Northcut where this has been addressed. These, however, are the correlations I've found on the GIAC website.

- Jim Webster: GIAC (Detects Analyzed 12/31/99)
- Bill Royds: GIAC (Detects Analyzed 1/5/00)
- Andrew Daviel: GIAC (1/18/01)
- Erik Fichtner: GIAC (Detects Analyzed 5/16/00)

7. Evidence of active targeting:

There is no evidence of active targeting. It appears that this activity was indiscriminant and spanned much of our networks as well as other IP address ranges.

8. Severity:

Severity = (criticality + lethality) – countermeasures (system + net)
-5 = (3 + 1) - (5 + 4)
3 – criticality: an average of all systems.
1 – lethality: no effect on systems.
5 – system countermeasures; modern operating systems w/ patches.
4 – network countermeasures; restrictive firewall.

9. Defensive recommendation:

None, the only defensive measure would be to block ICMP ttl exceeded messages from entering internal networks. Although this would be feasible, the restriction could cause additional barriers in troubleshooting network problems.

10. Multiple choice test question:

TIME	EVENTNAME	PROTOCOL	SOURCE PORT	SOURCE ADDRESS	DEST PORT	DESTINATION ADDRESS	Tag Value
09/23/2000 3:35:16 AM	Trace_Route	1	0	10.46.86.0	0	212.158.123.66	Echo request

In the Real Secure logs above, from where is the address 10.46.86.0 extracted:

a) The source address of the ICMP ttl exceeded message.
b) The destination address of the ICMP ttl exceeded message.
c) The source address in the packet header embedded in the data of the ICMP ttl exceeded message.
d) The destination address in the packet header embedded in the data of the ICMP ttl exceeded message.

c.

Detect 2

A:

TIME	EVENTNAME	PROTOCOL	SOURCE PORT	SOURCE ADDRESS	DEST PORT	DEST ADDRESS
01/30/2001 6:49:44 PM	IPHalfScan	6	111	210.177.11.61	111	10.45.110.109
01/30/2001 6:49:20 PM	IPHalfScan	6	109	210.177.11.61	109	10.45.110.109
01/30/2001 6:49:32 PM	IPHalfScan	6	53	210.177.11.61	53	10.45.110.109
01/30/2001 6:49:12 PM	IPHalfScan	6	21	210.177.11.61	21	10.45.110.109
01/30/2001 6:50:39 PM	IPHalfScan	6	515	210.177.11.61	515	10.45.110.109
01/30/2001 6:50:42 PM	IPHalfScan	6	515	210.177.11.61	515	10.45.111.109
01/30/2001 6:49:48 PM	IPHalfScan	6	111	210.177.11.61	111	10.45.111.109
01/30/2001 6:49:26 PM	IPHalfScan	6	109	210.177.11.61	109	10.45.111.109
01/30/2001 6:49:37 PM	IPHalfScan	6	53	210.177.11.61	53	10.45.111.109
01/30/2001 6:49:17 PM	IPHalfScan	6	21	210.177.11.61	21	10.45.111.109
01/30/2001 6:49:43 PM	IPHalfScan	6	53	210.177.11.61	53	10.45.112.109
01/30/2001 6:49:22 PM	IPHalfScan	6	21	210.177.11.61	21	10.45.112.109
01/30/2001 6:49:31 PM	IPHalfScan	6	109	210.177.11.61	109	10.45.112.109
01/30/2001 6:49:54 PM	IPHalfScan	6	111	210.177.11.61	111	10.45.112.109
01/30/2001 6:49:27 PM	IPHalfScan	6	21	210.177.11.61	21	10.45.113.109
01/30/2001 6:49:47 PM	IPHalfScan	6	53	210.177.11.61	53	10.45.113.109
01/30/2001 6:49:36 PM	IPHalfScan	6	109	210.177.11.61	109	10.45.113.109
01/30/2001 6:49:59 PM	IPHalfScan	6	111	210.177.11.61	111	10.45.113.109

B:

D	M	Year	Time	Source IP	Dest IP	Protocol	Packets	Size	Source Port	Dest Port	TCP Flags
30	1	2001	8:40:40	210.177.11.61	10.46.10.109	6	1	40	21	21	SYN/FIN
30	1	2001	8:40:51	210.177.11.61	10.46.10.109	6	1	40	109	109	SYN/FIN
30	1	2001	8:41:02	210.177.11.61	10.46.10.109	6	1	40	53	53	SYN/FIN

30	1	2001	8:41:15	210.177.11.61	10.46.10.109	6	1	40	111	111	SYN/FIN
30	1	2001	8:42:09	210.177.11.61	10.46.10.109	6	1	40	515	515	SYN/FIN
30	1	2001	8:40:47	210.177.11.61	10.46.11.109	6	1	40	21	21	SYN/FIN
30	1	2001	8:40:55	210.177.11.61	10.46.11.109	6	1	40	109	109	SYN/FIN
30	1	2001	8:41:10	210.177.11.61	10.46.11.109	6	1	40	53	53	SYN/FIN
30	1	2001	8:41:18	210.177.11.61	10.46.11.109	6	1	40	111	111	SYN/FIN
30	1	2001	8:42:12	210.177.11.61	10.46.11.109	6	1	40	515	515	SYN/FIN
30	1	2001	8:40:51	210.177.11.61	10.46.12.109	6	1	40	21	21	SYN/FIN
30	1	2001	8:41:02	210.177.11.61	10.46.12.109	6	1	40	109	109	SYN/FIN
30	1	2001	8:41:15	210.177.11.61	10.46.12.109	6	1	40	53	53	SYN/FIN
30	1	2001	8:41:26	210.177.11.61	10.46.12.109	6	1	40	111	111	SYN/FIN
30	1	2001	8:42:21	210.177.11.61	10.46.12.109	6	1	40	515	515	SYN/FIN
30	1	2001	8:40:55	210.177.11.61	10.46.13.109	6	1	40	21	21	SYN/FIN
30	1	2001	8:41:02	210.177.11.61	10.46.13.109	6	1	40	109	109	SYN/FIN
30	1	2001	8:41:18	210.177.11.61	10.46.13.109	6	1	40	53	53	SYN/FIN
30	1	2001	8:41:26	210.177.11.61	10.46.13.109	6	1	40	111	111	SYN/FIN
30	1	2001	8:42:21	210.177.11.61	10.46.13.109	6	1	40	515	515	SYN/FIN
30	1	2001	8:41:02	210.177.11.61	10.46.14.109	6	1	40	21	21	SYN/FIN

1. Source of Trace: Own network.

2. Detect was generated by:

A. Real Secure: These logs were generated with Real Secure version 5.0. They were extracted directly from Real Secures Access database. The table comprises of select fields from the Real Secure database.

a. Time – Date and time of event in Zulu.
b. Eventname – The name of the signature that triggered. In this case “IPHalfscan.”
c. Protocol – The protocol type (1 – ICMP, 6 – TCP, 17 – UDP). In this case TCP.
d. Source port – Self-explanatory.
e. Source address – Source IP Address.
f. Dest port – Self-explanatory.
g. Dest address – Destination IP Address

B. Netflow: These Netflow data outputs were imported to a spreadsheet. The column headings describe the fields.

3. Probability the source address was spoofed:

It is unlikely the source address was spoofed. This activity appeared to be a SYN/FIN scan. If the source were spoofed, the results would not have been gathered unless the scanning host was on a segment along the return route.

4. Description of attack:

This attack was a SYN/FIN scan of numerous IP addresses from and to ports 21, 53, 111, 109 and 515. If sorted by destination IP address, the scan format incremented the third octet of the IP addresses leaving the fourth octet constant.

5. Attack mechanism:

This attack uses SYN/FIN packets as an initiator. The data from the response can be collected and analyzed.

The following is the result of my own experiment in order to validate the value of SYN/FIN activity. I used a packet-crafting tool to send SYN/FIN packets to open and closed ports on Solaris, NT Workstation 4.0 and Linux Redhat 6.X. Here are the results:

```
****SOLARIS OPEN PORT****
16:38:50.761362 eth0 > scanner.ftp > solaris.ftp: SF 420:420(0) win 512 (DF) [tos 0x18]
(ttl 254, id 55)
16:38:50.761638 eth0 < solaris.ftp > scanner.ftp: S 3890723562:3890723562(0) ack 421 win
9112 <mss 536> (DF) (ttl 255, id 58151)

****SOLARIS CLOSED PORT****
16:38:59.162646 eth0 > scanner.finger > solaris.finger: SF 420:420(0) win 512 (DF) [tos
0x18]  (ttl 254, id 57)
16:38:59.162819 eth0 < solaris.finger > scanner.finger: R 0:0(0) ack 421 win 0 (DF) [tos
0x18]  (ttl 254, id 58152)

****LINUX_RH OPEN PORT****
16:39:36.945289 eth0 > scanner.www > linux.www: SF 420:420(0) win 512 (DF) [tos 0x18]
(ttl 254, id 58)
16:39:36.945624 eth0 < linux.www > scanner.www: S 1459729196:1459729196(0) ack 421 win
31624 <mss 536> (DF) (ttl 63, id 41530)

****LINUX_RH CLOESED PORT****
16:39:44.421022 eth0 > scanner.finger > linux.finger: SF 420:420(0) win 512 (DF) [tos
0x18]  (ttl 254, id 60)
16:39:44.421345 eth0 < linux.finger > scanner.finger: R 0:0(0) ack 421 win 0 [tos 0x18]
(ttl 254, id 41531)

****WIN_NT OPEN PORT****
16:40:17.213406 eth0 > scanner.135 > 141.190.131.12.135: SF 420:420(0) win 512 (DF) [tos
0x18]  (ttl 254, id 61)
16:40:17.213601 eth0 < 141.190.131.12.135 > scanner.135: S 69105:69105(0) ack 421 win
8576 <mss 1460> (DF) (ttl 128, id 49341)

****WIN_NT CLOSED PORT****
16:40:25.440104 eth0 > scanner.finger > 141.190.131.12.bgp: SF 420:420(0) win 512 (DF)
[tos 0x18]  (ttl 254, id 63)
16:40:25.440358 eth0 < 141.190.131.12.bgp > scanner.finger: R 0:0(0) ack 422 win 0 (ttl
128, id 49853)
```

These results show SYN/FIN as very effective in distinguishing OS and open ports. If a port is open, a SYN/ACK packet will be received and ttl will distinguish between OS (Solaris – 255, Linux – 64, Windows – 128.) If the port is closed, a RST/ACK packet will be received and the don't fragment and acknowledgment number will distinguish between operating systems. The acknowledgment number will be incremented by 2 for only Windows hosts while the DF bit will only be set for Solaris hosts.

Note: I did a quick experiment on Cisco switches and routers. I was not able to solicit a response from an open port, however I was able to notice RST/ACK packets used the same initial sequence numbers as the SYN/FIN packets whereas other OS used 0.

The use of identical source and destination ports could have been an attempt to bypass simple ACLs or firewall rules.

Host Info:
No DNS Records
Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-BLK)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC-CIDR-BLK2
Netblock: 210.0.0.0 - 211.255.255.255

6. Correlations:

SYN/FIN scans are very common detects and have been addressed by many analysts. These, however, are the correlations I've found on the GIAC website.

- Stephan Odak: GIAC (Detects Analyzed 6/25/00)
- Kenneth McKinlay SANS Parliament Hill 2000 Intrusion Detection Practical assignment.
- GIAC (Detects Analyzed 7/7/00)
- JOHN S BEST JR. - GIAC Intrusion Detection Curriculum Practical Assignment for SANS Security DC 2000
- Linkar AB, Stockholm, Sweden (Detects Analyzed 5/4/00)

7. Evidence of active targeting:

There is no indication of active targeting. This appears to be scan of a whole range of IP addresses.

8. Severity:

Severity = (criticality + lethality) – countermeasures (system + net)
-3 = (3 + 1) - (5 + 2)
3 – criticality: an average of all systems.
1 – lethality: no effect on systems.
5 – system countermeasures; modern operating systems w/ patches.
2 – network countermeasures; restrictive firewall.

9. Defensive recommendation:

Increase restriction of firewall policy or implement a stateful inspection firewall. This would prevent SYN/FIN packets from entering the network.

10. Multiple choice test question:

D	M	Year	Time	Source IP	Dest IP	Protocol	Packets	Size	Source Port	Dest Port	TCP Flags
30	1	2001	8:40:47	210.177.11.61	10.46.11.109	6	1	40	21	21	SYN/FIN
30	1	2001	8:40:55	210.177.11.61	10.46.11.109	6	1	40	109	109	SYN/FIN
30	1	2001	8:41:10	210.177.11.61	10.46.11.109	6	1	40	53	53	SYN/FIN

30	1	2001	8:41:18	210.177.11.61	10.46.11.109	6	1	40	111	111	SYN/FIN
30	1	2001	8:42:12	210.177.11.61	10.46.11.109	6	1	40	515	515	SYN/FIN

The scan above is likely targeting….

a) Microsoft NT systems.
b) Routers
c) UNIX or LINUX systems.
d) Switches

c.

Detect 3

A:

TIME	EVENTNAME	PROTOCOL	SOURCE PORT	SOURCE ADDRESS	DEST PORT	DEST ADDRESS
02/11/2001 14:09:28	IPHalfScan	6	53	208.156.1.100	53	10.201.4.1
02/11/2001 14:09:33	IPHalfScan	6	53	208.156.1.100	53	10.201.5.1
02/11/2001 14:09:38	IPHalfScan	6	53	208.156.1.100	53	10.201.6.1
02/11/2001 14:27:06	IPHalfScan	6	53	208.156.1.100	53	10.201.4.1
02/11/2001 14:27:11	IPHalfScan	6	53	208.156.1.100	53	10.201.5.1
02/11/2001 14:27:16	IPHalfScan	6	53	208.156.1.100	53	10.201.6.1
02/11/2001 14:48:47	IPHalfScan	6	53	208.156.1.100	53	10.201.4.2
02/11/2001 14:48:52	IPHalfScan	6	53	208.156.1.100	53	10.201.5.2
02/11/2001 14:48:57	IPHalfScan	6	53	208.156.1.100	53	10.201.6.2
02/11/2001 15:10:27	IPHalfScan	6	53	208.156.1.100	53	10.201.4.3
02/11/2001 15:10:32	IPHalfScan	6	53	208.156.1.100	53	10.201.5.3
02/11/2001 15:10:37	IPHalfScan	6	53	208.156.1.100	53	10.201.6.3
02/11/2001 15:32:08	IPHalfScan	6	53	208.156.1.100	53	10.201.4.4
02/11/2001 15:32:13	IPHalfScan	6	53	208.156.1.100	53	10.201.5.4
02/11/2001 15:32:18	IPHalfScan	6	53	208.156.1.100	53	10.201.6.4
02/11/2001 15:53:49	IPHalfScan	6	53	208.156.1.100	53	10.201.4.5
02/11/2001 15:53:54	IPHalfScan	6	53	208.156.1.100	53	10.201.5.5
02/11/2001 15:53:59	IPHalfScan	6	53	208.156.1.100	53	10.201.6.5
02/11/2001 16:15:30	IPHalfScan	6	53	208.156.1.100	53	10.201.4.6
02/11/2001 16:15:35	IPHalfScan	6	53	208.156.1.100	53	10.201.5.6
02/11/2001 16:15:40	IPHalfScan	6	53	208.156.1.100	53	10.201.6.6

B:

```
11 02 2001 14:09:31Z 208.156.1.100 10.201.4.1 p 6  pk 2 size  80 sp  53 dp 53 flg  0x7
11 02 2001 14:09:34Z 208.156.1.100 10.201.5.1 p 6  pk 1 size  40 sp  53 dp 53 flg  0x3
11 02 2001 14:09:41Z 208.156.1.100 10.201.6.1 p 6  pk 1 size  40 sp  53 dp 53 flg  0x3
11 02 2001 14:09:41Z 208.156.1.100 10.201.4.1 p 6  pk 4 size 216 sp 1455 dp 53 flg  0x13
11 02 2001 14:09:55Z 208.156.1.100 10.201.4.1 p 17 pk 1 size  55 sp 1241 dp 53
11 02 2001 14:09:55Z 208.156.1.100 10.250.180.194 p 1 pk 1 size  83 3/3 port unreachable
11 02 2001 14:27:08Z 208.156.1.100  10.201.4.1 p 6 pk 2 size  80 sp 53 dp 53 flg  0x7
11 02 2001 14:27:08Z 208.156.1.100  10.201.4.1 p 6 pk 4 size 216 sp 1855 dp 53 flg  0x13
11 02 2001 14:27:13Z 208.156.1.100  10.201.5.1 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
```

```
11 02 2001 14:27:18Z 208.156.1.100  10.201.6.1 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 14:27:21Z 208.156.1.100  10.201.4.1 p 17 pk 1 size 55 sp 2844 dp 53
11 02 2001 14:27:21Z 208.156.1.100 10.250.180.194 p 1 pk 1 size 83 3/3 port unreachable
11 02 2001 14:48:50Z 208.156.1.100  10.201.4.2 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 14:48:55Z 208.156.1.100  10.201.5.2 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 14:48:59Z 208.156.1.100  10.201.6.2 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:10:30Z 208.156.1.100  10.201.4.3 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:10:36Z 208.156.1.100  10.201.5.3 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:10:39Z 208.156.1.100  10.201.6.3 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:32:10Z 208.156.1.100  10.201.4.4 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:32:16Z 208.156.1.100  10.201.5.4 p  6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 15:32:19Z 208.156.1.100  10.201.6.4 p  6 pk 2 size 80 sp 53 dp 53 flg  0x7
11 02 2001 15:32:19Z 208.156.1.100  10.201.6.4 p  6 pk 4 size 216 sp 3647 dp 53 flg 0x13
11 02 2001 15:32:35Z 208.156.1.100  10.201.6.4 p 17 pk 1 size 55 sp 4504 dp 53
11 02 2001 15:32:35Z 208.156.1.100 10.250.180.194 p 1 pk 1 size 83 3/3 port unreachable
11 02 2001 15:53:52Z 208.156.1.100  10.201.4.5 p  6 pk 2 size  80 sp 53 dp 53 flg  0x7
11 02 2001 15:53:56Z 208.156.1.100  10.201.5.5 p  6 pk 2 size  80 sp 53 dp 53 flg  0x7
11 02 2001 15:53:58Z 208.156.1.100  10.201.4.5 p 6 pk 4 size 216 sp 4182 dp 53 flg  0x13
11 02 2001 15:53:58Z 208.156.1.100  10.201.5.5 p 6 pk 4 size 216 sp 4183 dp 53 flg  0x13
11 02 2001 15:53:59Z 208.156.1.100  10.201.6.5 p  6 pk 1 size  40 sp 53 dp 53 flg  0x3
11 02 2001 15:54:10Z 208.156.1.100  10.201.4.5 p 17 pk 1 size 55 sp 2149 dp 53
11 02 2001 15:54:10Z 208.156.1.100  10.201.5.5 p 17 pk 1 size 55 sp 2150 dp 53
11 02 2001 15:54:10Z 208.156.1.100 10.250.180.194 p 1 pk 2 size 166 3/3 port unreachable
11 02 2001 16:15:32Z 208.156.1.100  10.201.4.6 p 6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 16:15:37Z 208.156.1.100  10.201.5.6 p 6 pk 1 size 40 sp 53 dp 53 flg  0x3
11 02 2001 16:15:43Z 208.156.1.100  10.201.6.6 p 6 pk 2 size 80 sp 53 dp 53 flg  0x7
11 02 2001 16:15:43Z 208.156.1.100  10.201.6.6 p 6 pk 4 size 216 sp 4774 dp 53 flg  0x13
11 02 2001 16:15:56Z 208.156.1.100 10.201.6.6 p 17 pk  1 size 55 sp  3885 dp 53
11 02 2001 16:15:56Z 208.156.1.100 10.250.180.194 p 1 pk 1 size 83 3/3 port unreachable
```

This trace is similar to detect 2 however, the activity is directed at a single port (53 – DNS) and adds packets with additional flags set. I believe this makes this detect uniquely different from detect 2 and addressable in a separate detect.

1. Source of Trace: Own network.

2. Detect was generated by:

   A. Real Secure: These logs were generated with Real Secure version 5.0. They were extracted directly from Real Secures Access database. The table comprises of select fields from the Real Secure database.

      a. Time – Date and time of event in Zulu.
      b. Eventname – The name of the signature that triggered. In this case "IPHalfscan."
      c. Protocol – The protocol type (1 – ICMP, 6 – TCP, 17 – UDP). In this case TCP.
      d. Source port – Self-explanatory.
      e. Source address – Source IP Address.
      f. Dest port – Self-explanatory.
      g. Dest address – Destination IP Address

   B. Netflow.

   Although Netflow can provide all packet header information, this extract only contains the following: Day Month Year Time(Zulu) : Source IP : Destination IP : Protocol type : Number of packets : Total size of packets in bytes : Source port : Destination port : TCP flags.

3. Probability the source address was spoofed:

It is unlikely the source address was spoofed. This activity appeared to be a DNS scan. If the source were spoofed, the results would not have been gathered unless the scanning host was on a segment along the return route.

4. Description of attack:

This was very similar to a SYN/FIN scan but with SYN/FIN/ACK and SYN/FIN/RST packets added to the mix. This may be another fingerprinting method to identify OS and version of DNS.

5. Attack mechanism:

Unfortunately, during this time, Netflow was not capturing all packets. This was due to an error in configuration. It appears that Netflow was only recording traffic inbound. Going off of the incomplete data, more than likely, the scenario is that the 10.201.X.X addresses are being scanned for DNS services and other OS/daemon fingerprinting. This is using SYN/FIN and SYN/FIN/RST packets from port 53 to port 53, SYN/FIN/ACK packets from ephemeral ports to port 53 and UDP packets from ephemeral ports to port 53. There was a firewall in place downstream of Real Secure and Netflow with the IP address 10.250.180.194. This is the host that received ICMP port unreachable messages. This would either be a spoofed packet or a response from a packet from the firewall. As a response, there is a possibility that I came up with that might explain this. The firewall blocks the activity and automatically executes a traceroute-like function or possibly a probe to validate to the source. This activity using TCP or UDP protocol destined for a closed port would generate the ICMP message.

Host Info:

Host name: Picard.centralva.net
IP address: 208.156.1.100
Alias(es): None

6. Correlations:

Although there are many reports on similar activity involving SYN-FIN scans, I could not find any correlating reports using the combinations of flags used here. More than likely, this is a variant of the SYN-FIN scan used for OS detection and firewall penetration.

7. Evidence of active targeting:

There is no indication of active targeting. This appears to be scan of a whole range of IP addresses.

8. Severity:

Severity = (criticality + lethality) – countermeasures (system + net)
-3 = (3 + 1) - (5 + 2)
3 – criticality: an average of all systems.
1 – lethality: no effect on systems.

5 – system countermeasures; modern operating systems w/ patches.
2 – network countermeasures; restrictive firewall.

9. Defensive recommendation:
None. All indications show the firewall was effective in blocking the scan.

10. Multiple choice test question:

```
11 02 2001 14:09:31Z 208.156.1.100 10.201.4.1 p 6  pk 2 size  80 sp  53 dp 53 flg  0x7
11 02 2001 14:09:34Z 208.156.1.100 10.201.5.1 p 6  pk 1 size  40 sp  53 dp 53 flg  0x3
11 02 2001 14:09:41Z 208.156.1.100 10.201.6.1 p 6  pk 1 size  40 sp  53 dp 53 flg  0x3
11 02 2001 14:09:41Z 208.156.1.100 10.201.4.1 p 6  pk 4 size 216 sp 1455 dp 53 flg  0x13
```

The packets shown above are likely crafted because…
a) SYN/FIN/RST, SYN/FIN and SYN/FIN/ACK packets cannot be legitimate traffic.
b) TCP packets from port 53 to port 53 cannot be legitimate traffic.
c) 40 Bytes are too small to be legitimate TCP traffic.
d) 208.156.1.100 is an invalid IP address.

a)

Detect 4

```
13 10 2000 12:39:4Z :195.22.25.98: 10.213.252.72: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.101.98: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.194.117: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.94.46: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.8.10: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.237.77: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.125.68: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.192.38: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.170.35: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.212.115.30: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.200.12: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.3.64: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:7Z :195.22.25.98: 10.213.64.8: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:13Z :195.22.25.98: 10.213.210.65: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:13Z :195.22.25.98: 10.212.78.67: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:13Z :195.22.25.98: 10.213.145.59: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:13Z :195.22.25.98: 10.213.207.78: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.215.38: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.213.100.68: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.109.18: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.196.96: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.244.127: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.213.224.83: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.219.2: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:16Z :195.22.25.98: 10.212.179.116: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.127.83: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.212.15.36: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.45.23: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.176.13: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.212.171.60: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.143.105: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.217.86: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.241.49: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.35.24: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.154.36: p 1: pk 1 : size 56 :3/1 host unreachable
```

```
13 10 2000 12:39:28Z :195.22.25.98: 10.213.59.124: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.58.118: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.37.16: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:35Z :195.22.25.98: 10.212.242.12: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:35Z :195.22.25.98: 10.213.47.127: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:40Z :195.22.25.98: 10.212.86.58: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:40Z :195.22.25.98: 10.213.6.77: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:40Z :195.22.25.98: 10.212.59.35: p 1: pk 1 : size 56 :3/1 host unreachable
```

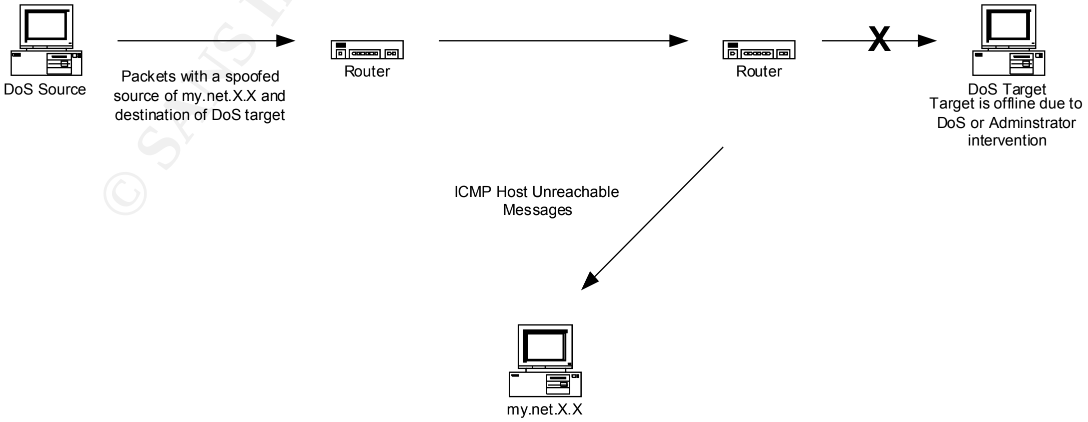
1. Source of Trace: Own network.

2. Detect was generated by:
Netflow.
Although Netflow can provide all packet header information, this extract only contains the following: Day Month Year Time(Zulu) : Source IP : Destination IP : Protocol type : Number of packets : Total size of packets in bytes : ICMP type/code message.

3. Probability the source address was spoofed:
It is unlikely the source address was spoofed. This activity appeared to be results of DOS attack on a different source address. A router upstream to the victim generated these packets.

4. Description of attack:
This was the result of a DOS on an outside source. We received the ICMP messages because our address space was used as a spoofed source.

5. Attack mechanism:
The attacker used some sort of DOS attack on the victim using our IP addresses as spoofed sources. This could have been any type of packets. For whatever reason, the victim was down. This could be that the victim had crashed as a result of DOS or the system administrator may have shut the system down. Subsequently, the router on that local subnet reports, “host unreachable” back to the spoofed source.


DoS Source
Packets with a spoofed source of my.net.X.X and destination of DoS target
Router
Router
X
DoS Target
Target is offline due to DoS or Adminstrator intervention
ICMP Host Unreachable Messages
my.net.X.X

Host Info:
European Regional Internet Registry/RIPE NCC (NETBLK-RIPE-C)

These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-CBLK3
Netblock: 195.0.0.0 - 195.255.255.255
Maintainer: RIPE

6. Correlations:

This is common type of detect, however, most are not ICMP host unreachable from the same source host. These are the correlations I've found on the GIAC website.

- GIAC (Detects Analyzed 9/26/00)
- Donald McLachlan: GIAC (Detects Analyzed 8/13/00)
- Dustin Decker: GIAC (12/12/2000)

7. Evidence of active targeting:

This does not appear to be active targeting. This appears to use random IP addresses from our subnet.

8. Severity:

Severity = (criticality + lethality) – countermeasures (system + net)
-3 = (3 + 1) - (5 + 2)
3 – criticality: an average of all systems.
1 – lethality: no effect on systems.
5 – system countermeasures; modern operating systems w/ patches.
2 – network countermeasures; restrictive firewall.

9. Defensive recommendation:

None, the only defensive measure would be to block ICMP host unreachable messages from entering internal networks. Although this would be feasible, the restriction could cause additional barriers in troubleshooting network problems.

10. Multiple choice test question:

```
13 10 2000 12:39:24Z :195.22.25.98: 10.213.176.13: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.212.171.60: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.143.105: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.217.86: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:24Z :195.22.25.98: 10.213.241.49: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.35.24: p 1: pk 1 : size 56 :3/1 host unreachable
13 10 2000 12:39:28Z :195.22.25.98: 10.213.154.36: p 1: pk 1 : size 56 :3/1 host unreachable
```

Which statement is likely true?
a) 195.22.25.98 is a router.

b) 195.22.25.98 not a router.
c) 195.22.25.98 is the destination host that was unreachable
d) 195.22.25.98 is offline.

a)

Detect 5

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:18.059291 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57681 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:18.820777 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57721 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:19.644791 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57757 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] SCAN wingate attempt [**]
03/15-21:10:18.059291 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57681 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:18.820777 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57721 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] SCAN wingate attempt [**]
03/15-21:10:19.644791 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3140 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57757 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB765DA6  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[root@forbidden1 66.6.36.140]# more TCP:3170*
[**] SCAN wingate attempt [**]
03/15-21:10:20.060660 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3170 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57777 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB94F669  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:20.913773 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3170 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57815 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB94F669  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/15-21:10:21.753563 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3170 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57848 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB94F669  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] SCAN wingate attempt [**]
03/19-21:38:33.454975 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.142:4920 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:37100 IpLen:20 DgmLen:48 DF
******S* Seq: 0x52B2C6D9  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/19-21:38:36.439922 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.142:4920 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:37186 IpLen:20 DgmLen:48 DF
******S* Seq: 0x52B2C6D9  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK
```

1. Source of Trace: Own network.

2. Detect was generated by:

This detect was from my personal system running SNORT. The output is as follows: Date : Time : Source MAC address -> Destination MAC address : Frame Type : Frame length : Source IP address . Source port -> Destination IP address . Destination port : Protocol Type : Time to live : Type of Service : IP ID : IP length : Datagram Length : Don't Fragment bit : TCP flags : Sequence Number : Acknowledgement Number : Window size : TCP length : TCP Options.
This connection is via cable modem and only logs activity to a single host.

3. Probability the source address was spoofed:

It is unlikely the source address was spoofed. This activity appeared to be a DNS scan, possibly to identify OS and version of DNS. If the source were spoofed, the resulting data would not be accessible unless the scanning host was on a segment along the return route.

4. Description of attack:

This appears to be a scan to identify proxy servers. SNORT identifies this activity as a "SCAN wingate attempt." Once identified, wingate servers can be used as relay points to launch attacks anonymously.

5. Attack mechanism:

This activity appears to be a straightforward SYN scan for port 1080. The SNORT signature that triggers this alert is: "alert tcp $EXTERNAL_NET any -> $HOME_NET 1080,8080 (msg:"SCAN wingate attempt";flags:S;)." This translates to any TCP SYN packet from an external source to a destination port of 1080 or 8080. Although, the source port remained the same, the IP ID variations rule out TCP retransmits. The fact that the IP addresses are part of the same subnet may indicate a dynamic pool (Lookups on the IP address do not indicate whether these are part of a dynamic pool or not.) or a compromised host on the same subnet. In the compromised host situation, an attacker could spoof the source IP as another IP in the same subnet. This would allow the true source to be masked and still allow return packets to be sniffed. In either case, the identical TTLs lead to the assumption these packets originated in the same location.

Host Info:

Host name: dial-140.waterloo.mwci.net
IP address: 66.6.36.140
Alias(es): None

Host name: dial-142.waterloo.mwci.net
IP address: 66.6.36.142
Alias(es): None

6. Correlations:

This appears to be very common recent detect. These are the correlations I've found on the GIAC website.

- Tim Lyons: SANS GIAC (January 18, 2001)
- JOHN S BEST JR. - GIAC Intrusion Detection Curriculum Practical Assignment for SANS Security DC 2000
- Bryce Alexander: GIAC (Detects Analyzed 4/26/00)

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

Reference: BUGTRAQ:19980221 WinGate DoS
Reference: BUGTRAQ:19980326 WinGate Intermediary Fix/Update
Reference: XF:wingate-dos

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

Reference: XF:wingate-unpassworded

7. Evidence of active targeting:

These logs are compiled from an IDS monitoring a single host so the larger picture cannot be determined; however it appears that this activity is indiscriminant. There is no evidence of active targeting.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)
-5 = (1 + 1) - (5 + 2)
1 – criticality: personal system, not critical.
1 – lethality: no effect on systems.
5 – system countermeasures; modern operating systems w/ patches.
2 – network countermeasures; restrictive firewall.

9. Defensive recommendation:

There are no defensive recommendations. No proxy services are run from this host.

10. Multiple choice test question:

```
[**] SCAN wingate attempt [**]
03/15-21:10:21.753563 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.140:3170 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:57848 IpLen:20 DgmLe
n:48 DF
******S* Seq: 0xAB94F669  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] SCAN wingate attempt [**]
03/19-21:38:33.454975 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.142:4920 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:37100 IpLen:20 DgmLen:48 DF
******S* Seq: 0x52B2C6D9  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] SCAN wingate attempt [**]
03/19-21:38:36.439922 8:0:3E:0:53:13 -> 0:50:BA:44:85:63 type:0x800 len:0x42
66.6.36.142:4920 -> 10.31.65.123:1080 TCP TTL:112 TOS:0x0 ID:37186 IpLen:20 DgmLen:48 DF
******S* Seq: 0x52B2C6D9  Ack: 0x0  Win: 0x2238  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK
```

Which statement is a false assumption from the log entry above?

a) There is data in the TCP options field.
b) These are results of TCP retries.
c) These are TCP SYN packets.
d) The packets traversed the same number of hops.

b.

Assignment 2 - Describe the State of Intrusion Detection

A complete solution for Intrusion Detection.

With today's growing Internet base, Intrusion Detection Systems (IDS) need to diversify in order to keep up with developments. The term "diversify" is used loosely, but what is intended is that the idea of intrusion detection should be all encompassing. In this paper I also refer to IDS in this manner as not a single system, but many integrated systems. All too often, we envision IDS as a prepackaged, single box emplaced "somewhere" in the network. "Unrealistic expectations about intrusion-detection and vulnerability assessment products must be corrected: these products are not silver bullets…".[1] In reality the concept of IDS should be integrated tightly into network structures down to the design of the hardware. It should "feel" the entire network from the gateway to the individual host. Maybe even to the application level. IDS should also utilize multiple techniques and algorithms for detection. It is common to consider security as an afterthought, and even more so to have Intrusion detection not considered at all. These design flaws need to be addressed before any great steps in Intrusion Detection technology is to take place. New designs in hardware, software, network topologies and polices should be considered. Intrusion detection needs to be integrated into every facet of our networks.

To start off, let's pose the question, "What is your network?" Obviously, it is necessary to understand what is your network in order to determine what you're monitoring and protecting. The answer may seem trivial, but it may be more complicated as we progress into the future. More and more Internet technology is finding its way into everyday devices. Internet appliances, phones, PDAs, TVs are just a few that are. Shouldn't these devices incorporate IDS? Is it absurd to think someone in the cubical next to you may try to hack your PDA through your infrared port? As an example of the challenges, it would not be unreasonable to consider every car will have an IP address in the near future. After all, the technology to unlock your doors via satellite is already reality. This presents a significant challenge to security and intrusion detection. With an infinite number of potential devices with an Internet connection, who will secure them? Ultimately the responsibility relies on you, the owner, but would you setup a PC running snort in the trunk of your car? IDS need to find its way into the hardware designs of these circuit boards. Like the engine diagnostic checks the airflow in the intake manifold and oxygen in the exhaust pipe, shouldn't it also check if its memory is being accessed or its configuration is being changed?   If the common tasks of monitoring the day-to-day maintenance of an automobile can be integrated into a circuit board, so could intrusion detection. This is not to say intrusion analysis can be designed into "dumb" systems, but at least a primitive intrusion alarm system can warn users of a potential problem. Maybe there will be a job in the future for an automotive intrusion analyst.

IDS in automobiles may seem pretty novel, but how else can we expect to secure all of our personal devices on the Internet. Automobiles were an example, but the same could be said about appliances like refrigerators, stoves, or maybe something a little closer to reality like a home security system. Our networks presently incorporate the normal hosts, but what about the not so distant future. Are we prepared to handle your kitchen stove as host on your network? Let's switch gears to a more conventional view. How about IDS integrated into current network hardware? Devices like routers, switches and even NICs would be perfect candidates for IDS. Routers and switches are without a doubt, big, juicy targets. Routers would be prime candidate to run not only host-base IDS, but network-based IDS as well. How about one-step further and integrating IDS into all network hardware. If even lowly printers are vulnerable to DOS why not have IDS integrated into its NIC. This would enable the network security professional a total view of the network from every host. In this sense, the questions your network and you IDS would be one and the same. Sensor feeds could be collected from many sources down to every node.

Even with current hardware technology limitations, network designs can be altered to give the analyst a better view. Most network topology designs incorporate one or two network-based IDS and a firewall. There is no good reason to limit the number of IDS. The cost for setting up additional sensors is negligible compared to the load balancing and redundancy provided. Whoever said you cannot setup a pair of IDS sensors, each handling half or your IDS policy. How about four sensors with each having a fourth of the policy? This may be a good solution to a foreseeable future problem of an unmanageable amount of signature definitions. We can also use this design to incorporate redundancy. How about eight sensors, four with a fourth of a strong signature policy and four with a fourth of a weak signature policy. The possibilities are endless. This may also be a viable defense against attackers using DOS tools specifically constructed to attack IDS sensors. If we are willing to invest thousands of dollars on redundant drives, redundant servers, redundant routes, why not have redundant IDS sensors. "Given the implications of the failure of an ID component, it is reasonable to assume that ID systems are themselves logical targets for attack. A smart intruder who realizes that an IDS has been deployed on a network she is attacking will likely attack the IDS first, disabling it or forcing it to provide false information (distracting security personnel from the actual attack in progress, or framing someone else for the attack)."[2]

Hardware is only part of the picture. IDS software, like hardware, can also be diversified. Current mainstream IDS software relies on signatures to detect intrusions. Although this concept has considerable merit, signature based IDS will always be one step behind the intrusion techniques. Even a stateful inspection IDS would be a good improvement. (Among these signature-based solutions, it's worth mentioning SNORT with its open standard and ease of configuration as a good design methodology to be very useful into the future. Any exploit, once published, can be analyzed and turned into a rule set quickly. The community and not a single vendor guide the design.) There are other designs in development that use traffic patterns and norm comparisons to detect anomalies, however I would think these lack a granular view and are highly susceptible to false positives. The idea however, does have merit. The real answer should lie in a blend of all techniques. "The current generation of IDS is just the beginning. In the future, we'll see IDS that combine Anomaly Detection with Misuse Detection, and hopefully they will integrate smoothly with firewalls and other security systems."[3] Even integrated IDS in a NIC as mentioned above would still have deficiencies. The same methods of subversion that elude network-based intrusion detection systems could also avoid detection in the link-layer device. This is one of the benefits of host based intrusion detection software. Application level IDS would detect activity in the format that it is passed to the application. Methods of subversion on Network-based IDS would be caught by this technique. Part of difficulty of Host-based IDS is management. Maybe a good idea would be to integrate host-based intrusion detection with anti-virus software. Off all other applications, anti-virus software closely resembles the functions of IDS. Functional areas even overlap to a certain extent with Trojans. Ideally, a single console as in current "corporate editions" can control signatures and management. This, of course, would still be a part of a larger system of network-based IDS. In this way, Host-based and Network-based, Application-based and Network-layer-based, Signature-based and Traffic based could all be collaborated into one analytical process. "Both network and host based IDS solutions have unique strengths and benefits that complement each other. A next-generation IDS, therefore, must include tightly integrated host and network components. Combining these two technologies will greatly improve network resistance to attacks and misuse, enhance the enforcement of security policy and introduce greater flexibility in deployment options." [4] Not unlike the developments with LDAP and Active directory, IDS should integrate all sensors into one management console. Maybe the ultimate solution is to integrate LDAP and IDS management and logging, one single, integrated database for IDS, firewalls, servers, routers…etc. Of course other feeds into the database could also be logs from self-scans, honey pots and sniffer data. This integration of pertinent data would greatly aid the analysis process.

This analysis process is another shortfall of current IDS. Most designs of intrusion detection often end too abruptly in the whole analytical process. They are not geared for correlating, associating, organizing, sorting and dissecting data. You're given an alarm to tell you something is suspicious, but then you're left to fend for yourself and analyze it. Collection and analysis tools are often left out of the scope of the IDS. IDS designs should include sniffers and other analysis tools. If casinos and banks place video cameras all over the place in order to get a good view of the entire operation, shouldn't sniffers be used the same way? Like video cameras, Sniffers are accurate records of all events. They allow the analyst to collect detailed packet information, which in many cases are essential to arrive at conclusive answers. Sniffers also provide an opportunity to validate alarms in IDS. This analysis on the IDS signatures itself is essential to good intrusion detection. "Because of its importance within a security system, it is critical that intrusion detection systems function as expected by the organizations deploying them. In order to be useful, site administration needs to be able to rely on the information provided by the system; flawed systems not only provide less information, but also a dangerously false sense of security. Moreover, the forensic value of information from faulty systems is not only negated, but potentially misleading."[5]

Although they are not technology issues, human psychology is so important in intrusion detection and must be addressed. The two subjects that are pertinent are proactive analysis and policies that support intrusion detection.

Arguably, the most important part of an intrusion detection system is the analyst. This component will separate effective IDS from an ineffective one. All of the alarms in the world will not have any value if the information cannot be processed into usable, and defendable solutions. Beyond relying on prepackaged software, Intrusion Detection Analysts need to be proactive. An important part of intrusion detection is proactive analysis. Analysts need to know what to look for just as importantly as where to look for it. It is obvious that not all vulnerabilities are published and not all published vulnerabilities are exploited, but being prepared is probably be the best advantage an analyst can have. Of course, system administrators applying the latest vendor patches negate the vulnerability, but identifying the exploit or even knowing you are being exploited is another story. It's all a part of knowing your enemy and its capabilities.

Policies also play a key role in the capabilities or limitations for intrusion detection. The most powerful of course would be an education policy. Individual users should be a part of the sensor pool. Like your network and application layer sensors, users can be another “layer” of intrusion detection. Users need to be educated “enough” to be able to determine when a good time to call and notify the Intrusion Detection analyst that something is going on. There are too many vulnerabilities to catch everything. Not only with intrusions, but attempted intrusion as it relates to Social Engineering. Information that an outside source is attempting to gather information about your systems by social engineering would be very valuable information to add to analysis. Another bonus for education is to stress the importance of intrusion detection or security in general. A good attitude, especially in management, on intrusion detection would go a long way into effectiveness. It provides a support structure both financial and social resources.

Hardware, software, topologies, proactive analysis and policies are all a part of good intrusion detection system. Each is an integral part of a complete picture. All too easily we fall into the mindset of intrusion detection as a single system. Resting all dependency on single system to detect and catch all the potential security vulnerabilities in an entire network. Often times this includes dial-in modems, other back-door connections, wireless devices, mobile laptops and more. A solution of one or two sensors out in the DMZ or around the firewall is a grossly incomplete solution. Intrusion detection must be built-in by design. It should monitor the entire network with multiple technologies, integrated into a central database, and include analysis tools. It needs to be “diversified.”

References

1. An Introduction to Intrusion Detection and Assessment Prepared
Rebecca Bace from Infidel, Inc. for ICSA, Inc
http://secinf.net/info/ids/intrusion/

2. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
Thomas H. Ptacek
tqbf@securenetworks.com
Timothy N. Newsham
newsham@securenetworks.com
Secure Networks, Inc.
January 1998
http://secinf.net/info/ids/idspaper/idspaper.html

3. Intrusion Detection: Challenges and Myths
Marcus J. Ranum (mjr@nfr.net <mailto:mjr@nfr.net>)
CEO, Network Flight Recorder, Inc.
http://secinf.net/info/ids/ids_mythe.html

4. Network- vs. Host-based Intrusion Detection A Guide to Intrusion Detection Technology
by Internet Security Systems
http://secinf.net/info/ids/nvh_ids/

5. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
Thomas H. Ptacek
tqbf@securenetworks.com
Timothy N. Newsham
newsham@securenetworks.com
Secure Networks, Inc.
January, 1998
http://secinf.net/info/ids/idspaper/idspaper.html

Assignment 3 – "Analyze This" Scenario

Analysis Methods/Tools

I tried browsing through the SNORT logs however this was clearly not the way to go. If anything, 155 MB of text forces one to find a better way. The analysis tools that were used to parse this information into something manageable were the grep utility and MS Excel.

First, I uploaded all the logs to a RedHat Linux host. I reviewed the SNORT signatures and listed all the keywords I felt would be present in important events. I used a few grep commands to generate some "filtered" log files;

I.e. grep –ri backdoor * > backdoor_hits.txt

The "-r" option specifies recursive searches through lower directories. The "- i" option allows the search to be non-case sensitive. (This option proved to be valuable with signatures like "DoS.") The redirect generates a text file with all the log entries with the keyword. These are the strings I searched for:

"backdoor"
"dos"
"dns"
"exploit"
"finger"
"ftp"
"netbios"
"rpc"
"telnet"
"virus"
"web"
"snmp"
"pcanywhere"
"access"
"administrator"
"root"

Next, I imported these text files into Excel. This was tedious with some files due to fields not lining up. However, once in Excel, I could sort on time, source IP, destination IP...etc.

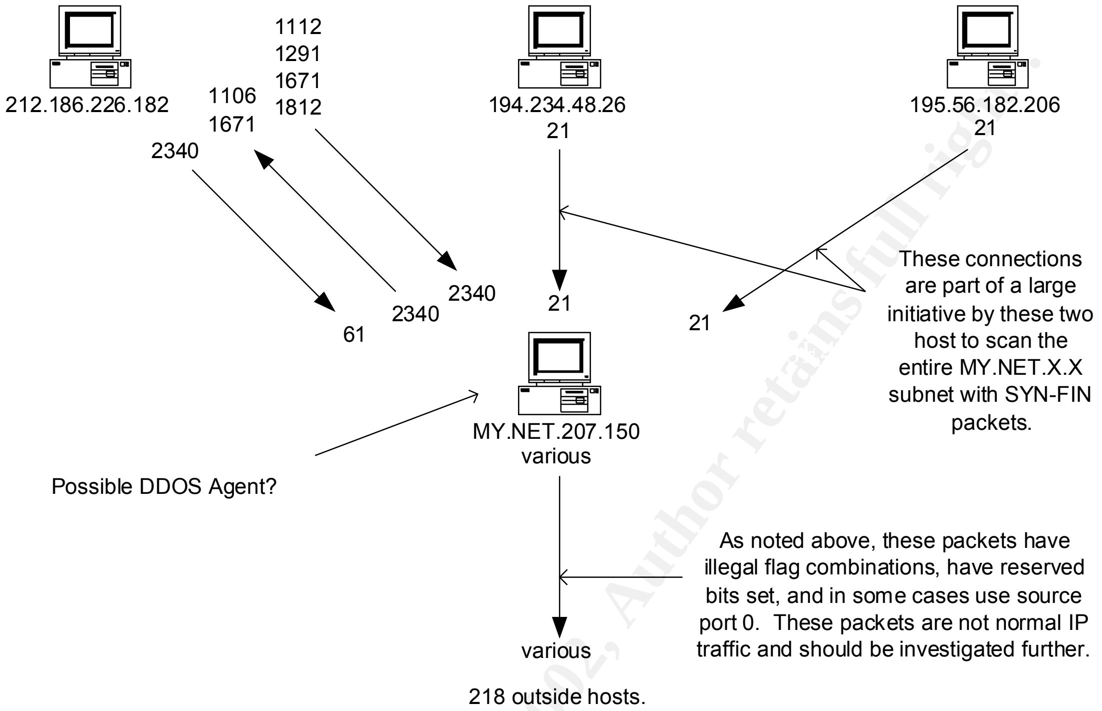
General Analysis

Most of these logs were typical Internet traffic. There were many scans for Sun RPC, Wingate and subseven Trojans as well as other port scans. However, in general scans occur often on the Internet and do not represent a great risk as long as systems are secured. There were also a lot activities associated with gaming. Ie. Diablo, Halflife, unreal masters…etc. This is a management issue. If this type of activity is not acceptable and management desires to pursue this, logs can be extracted and a list of IP addresses can be generated. From a security standpoint, these events are regular activities on the Internet and should not be overemphasized. Network administrators should be aware, however that gaming activity may present potential vulnerabilities and may adversely affect network throughput. Suggestions to overlook these activities should not to downplay good security practices however. Policies like keeping up to date with all vendor patches, periodic vulnerability testing and user education are essential to ensuring network security. Of the many events Snort logged, the signatures below are potentially critical traffic and need to be addressed.

Snort OOS

Snort OOS data revealed MY.NET.217.150, MY.NET.217.158, MY.NET.217.126 and MY.NET.219.126 sending unusual packets to hundreds of outside hosts. This activity does not represent the typical incoming traffic monitored by IDS and subsequently address separately here. Packets being sent from this host have illegal flag combinations, have reserved bits set, and in some cases use source port 0. These packets are not normal IP traffic and should be investigated further. This host may be a compromised system being used as a Distributed Denial of Service (DDOS) Agent, jump point or an employee(s) using a GIAC Enterprises computer to conduct potentially malicious activities. The following diagrams represent these activities as link graphs based on Snort OOS data.

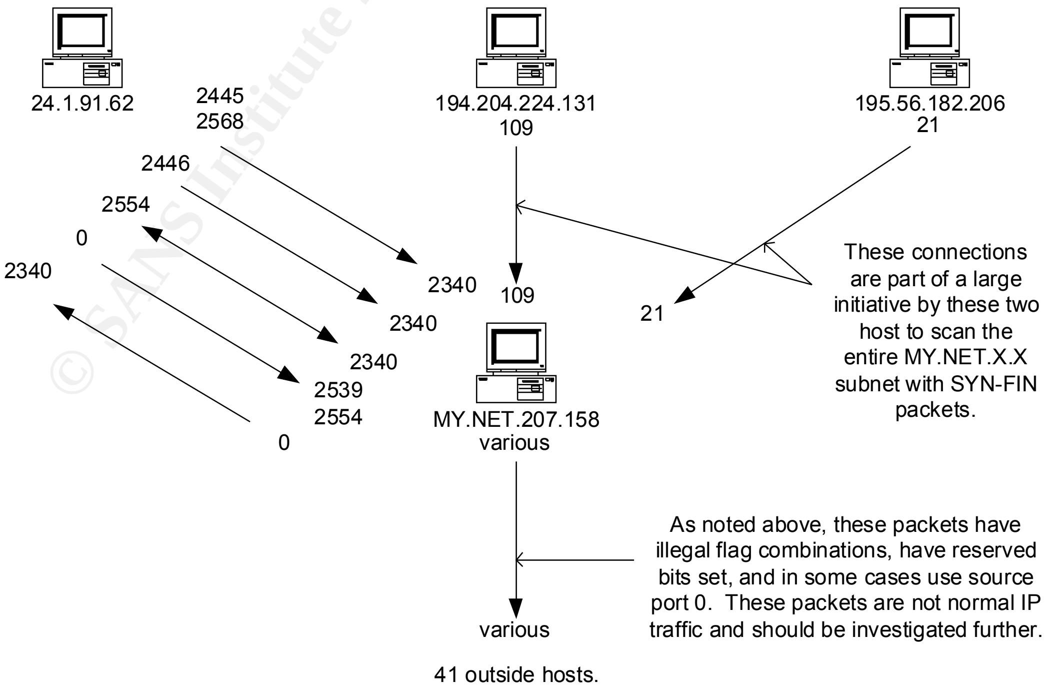
MY.NET.217.150:
Note: port 2340



These connections are part of a large initiative by these two host to scan the entire MY.NET.X.X subnet with SYN-FIN packets.

As noted above, these packets have illegal flag combinations, have reserved bits set, and in some cases use source port 0. These packets are not normal IP traffic and should be investigated further.

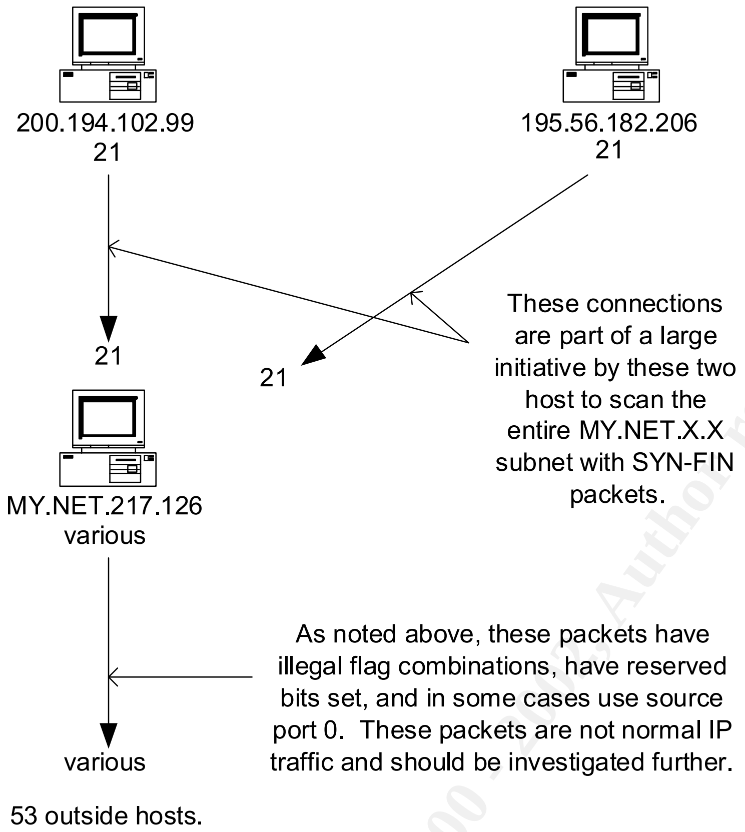
MY.NET.217.158:
Note port 2340



These connections are part of a large initiative by these two host to scan the entire MY.NET.X.X subnet with SYN-FIN packets.

As noted above, these packets have illegal flag combinations, have reserved bits set, and in some cases use source port 0. These packets are not normal IP traffic and should be investigated further.

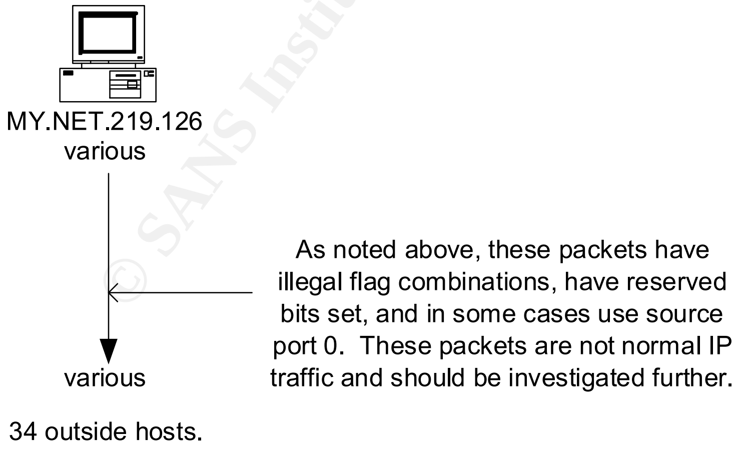
MY.NET.217.126:



These connections are part of a large initiative by these two host to scan the entire MY.NET.X.X subnet with SYN-FIN packets.

As noted above, these packets have illegal flag combinations, have reserved bits set, and in some cases use source port 0. These packets are not normal IP traffic and should be investigated further.

MY.NET.219.126:



As noted above, these packets have illegal flag combinations, have reserved bits set, and in some cases use source port 0. These packets are not normal IP traffic and should be investigated further.

The following analysis is the result of the keyword greps as mentioned in the analysis/tools section above. They represent high priority events that need initial attention. They are in the format defined in Assignment 1.

Watchlist

There was a considerable amount of traffic associated with a “watchlist…” These appeared to be specific connection events to track traffic with IL-ISDNNET and NET-NCFC. These events appeared to be SMTP, HTTPS, Authentication Service, FTP, napster and various other high port connections. The administrator who set up these signatures in Snort should be consulted in order to determine the purpose for tracking this activity and the legitimacy of the traffic.

IL-ISDNNET

Date / Time	Snort Signature	Source IP : Port	Destination IP : Port
01/03-16:51:02.975381	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3952	MY.NET.253.112:443
01/03-16:51:03.344287	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3952	MY.NET.253.112:443
01/03-16:51:06.967307	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3953	MY.NET.253.112:443
01/03-16:51:07.585893	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3953	MY.NET.253.112:443
01/03-16:51:08.546976	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3953	MY.NET.253.112:443
01/03-16:51:09.631413	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3953	MY.NET.253.112:443
01/03-16:51:10.041368	Watchlist 000220 IL-ISDNNET-990517	212.179.42.102:3953	MY.NET.253.112:443
…			
12/31-00:04:24.686708	Watchlist 000220 IL-ISDNNET-990517	212.179.127.3:1594	MY.NET.60.17:113
12/31-00:04:24.688611	Watchlist 000220 IL-ISDNNET-990517	212.179.127.3:1594	MY.NET.60.17:113
…			
11/28-02:59:24.733026	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
11/28-02:59:26.153729	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
11/28-02:59:26.536487	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
11/28-02:59:27.100252	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
11/28-02:59:27.450177	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
11/28-02:59:27.696981	Watchlist 000220 IL-ISDNNET-990517	212.179.15.122:2317	MY.NET.218.14:6699
…			
11/29-05:31:19.092301	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
11/29-05:31:19.405106	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
11/29-05:31:19.405904	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
11/29-05:31:19.860845	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
11/29-05:31:20.175688	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
11/29-05:31:20.175742	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:46807	MY.NET.201.230:4561
…			
11/29-05:56:50.256226	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:58131	MY.NET.209.22:4670
11/29-05:56:50.709111	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:58131	MY.NET.209.22:4670
11/29-06:15:58.323562	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:15991	MY.NET.209.22:4670
11/29-06:15:58.625149	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2:15991	MY.NET.209.22:4670

Of the many connections, it is likely only the various high port connections are questionable. Napster, HTTPS and Authentication probably have legitimate purposes.

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however some of these appear to be long sessions with potentially a lot of data transfer. In this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

The connections appear to be "regular" TCP connections. This appears to be due to normal communication between applications. This could be some sort of backdoor software or a legitimate application.

5. Attack mechanism:

It appears that most of the connections are from bezeqint.net. It is possible this person/group is using an account from this Internet Service Provider (ISP). These IP addresses probably belong to an address pool. When a user dials in (assuming its ISDN or some kind of modem), DHCP will assign the host from this pool. This would account for different addresses from the same subnet.

The attack, if any, may be using a backdoor listening at various high ports. This conclusion, however, is not perfect. Many facts make this difficult to assess. First of all, logs record one-way traffic. (The watchlist ruleset only generate logs on incoming traffic.) This makes it a guess that a connection is established and two-way communication is occurring. In many instances, it appears to be two-way because of IP address to port pairs. The same consistent source and destination ports are used for each session. The second fact is that makes this conclusion difficult is that although most of the connection traffic appears to be a connection with a single port to IP pair, there are instances with different ports for the same IP. This would disagree with a backdoor listener on a single port. Finally, there are many different listening ports, most in the range of 4000-5000. The theory of many compromised host with backdoor listeners would be much easier to swallow if a single port were used on all hosts.

Another possible solution is some sort of application communicating between both networks. This matter needs to be addressed by the Network Administrator.

Host Info:

212.179.79.2
No DNS Record

```
Host name: clnt-8164.bezeqint.net
IP address: 212.179.8.164
Alias(es): None

Host name: clnt-15122.bezeqint.net
IP address: 212.179.15.122
Alias(es): None
212.179.17.4
No DNS Record

Host name: clnt-27006.bezeqint.net
IP address: 212.179.27.6
Alias(es): None

Host name: clnt-27111.bezeqint.net
IP address: 212.179.27.111
Alias(es): None

Host name: PT10-33254.bezeqint.net
IP address: 212.179.33.254
Alias(es): None

Host name: clnt-38135.bezeqint.net
IP address: 212.179.38.135
Alias(es): None

Host name: clnt-38180.bezeqint.net
IP address: 212.179.38.180
Alias(es): None

Host name: fr-c42102.bezeqint.net
IP address: 212.179.42.102
Alias(es): None

Host name: bzq-44-106.bezeqint.net
IP address: 212.179.44.106
Alias(es): None

212.179.56.5
No DNS Record

Host name: cable-95005.bezeqint.net
IP address: 212.179.95.5
Alias(es): None

Host name: bzq-125-114.bezeqint.net
```

IP address: 212.179.125.114
Alias(es): None

European Regional Internet Registry/RIPE NCC (NET-RIPE-NCC-)
These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-NCC-212
Netblock: 212.0.0.0 - 212.255.255.255
Maintainer: RIPE

6. Correlations:

None. Only after consulting with the network administrator can correlations be made. Without knowing the reason for tracking these connections, any correlation would strictly be a guess.

7. Evidence of active targeting:

Much of this activity appeared to be established connections between two hosts. This is a good indication of active targeting, legitimate or otherwise.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

If this traffic is unwelcome, there are many steps that this organization can take to negate some of these vulnerabilities. The first should be to implement proxy services or Network Address Translation (NAT) for hosts that do not require public access. This will prevent most of the outside connections to internal hosts by using private addresses. The second recommendation would be to implement a stateful inspection firewall. This will also prevent unwanted outside connections to internal hosts. Publicly accessible hosts should use security features such as TCP wrappers to protect themselves at the host level. If there is absolutely no legitimate interface with this network, blocks can be implemented through Access Control Lists (ACLs) and firewalls. If GIAC Enterprises desires to continue allowing these connections with the intent to monitor the activity, sniffers should be used. At minimum, the Snort watchlist signatures should be modified to record activity both ways.

NET-NCFC

Date / Time	Snort Signature	Source IP : Port	Destination IP : Port
12/05-09:58:27.471131	Watchlist 000222 NET-NCFC	159.226.91.20:3203	MY.NET.100.230:25
12/05-09:59:44.837113	Watchlist 000222 NET-NCFC	159.226.91.20:3203	MY.NET.100.230:25
…			
11/29-06:58:59.812627	Watchlist 000222 NET-NCFC	159.226.47.217:36347	MY.NET.6.34:25
11/29-06:59:39.836466	Watchlist 000222 NET-NCFC	159.226.47.217:36347	MY.NET.6.34:25
11/29-07:07:00.403717	Watchlist 000222 NET-NCFC	159.226.47.217:36350	MY.NET.6.35:25
11/29-07:07:44.421232	Watchlist 000222 NET-NCFC	159.226.47.217:36350	MY.NET.6.35:25
11/29-07:07:45.936791	Watchlist 000222 NET-NCFC	159.226.47.217:36350	MY.NET.6.35:25
11/29-07:07:53.008498	Watchlist 000222 NET-NCFC	159.226.47.217:36350	MY.NET.6.35:25
11/29-07:07:53.735158	Watchlist 000222 NET-NCFC	159.226.47.217:36350	MY.NET.6.35:25
…			
12/04-00:11:41.984334	Watchlist 000222 NET-NCFC	159.226.47.14:34129	MY.NET.145.18:21
12/04-00:11:41.984377	Watchlist 000222 NET-NCFC	159.226.47.14:34129	MY.NET.145.18:21
…			
12/04-00:23:15.319427	Watchlist 000222 NET-NCFC	159.226.47.14:34148	MY.NET.145.18:21
…			
12/21-02:46:53.715854	Watchlist 000222 NET-NCFC	159.226.47.14:33181	MY.NET.145.18:21
12/21-02:49:41.743283	Watchlist 000222 NET-NCFC	159.226.47.14:33182	MY.NET.145.18:21
12/21-02:52:34.803727	Watchlist 000222 NET-NCFC	159.226.47.14:33184	MY.NET.145.18:21
12/21-02:56:35.783738	Watchlist 000222 NET-NCFC	159.226.47.14:33186	MY.NET.145.18:21
12/21-02:56:36.323340	Watchlist 000222 NET-NCFC	159.226.47.14:33186	MY.NET.145.18:21
12/21-02:57:00.758518	Watchlist 000222 NET-NCFC	159.226.47.14:33186	MY.NET.145.18:21
12/21-03:05:27.684670	Watchlist 000222 NET-NCFC	159.226.47.14:33188	MY.NET.145.18:21
…			
12/03-10:51:07.174310	Watchlist 000222 NET-NCFC	159.226.228.1:113	MY.NET.253.41:60044
…			
12/04-00:11:34.952469	Watchlist 000222 NET-NCFC	159.226.47.14:113	MY.NET.145.18:46206
…			
12/04-12:23:43.065285	Watchlist 000222 NET-NCFC	159.226.66.130:4255	MY.NET.253.52:113

Of the many connections, it is likely only the FTP connections are questionable. HTTPS and Authentication probably have legitimate purposes.

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however any attempt to transfer data would have been very difficult. In this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

Ten connections to FTP on MY.NET.145.18 were attempted.

5. Attack mechanism:

It appears this activity did not involve data transfer. The lack of logs involving port 22 confirms this (assuming port 22 is a signature in this rule set). Of the ten attempts, four may be TCP retransmits.

Host Info:

Host name: amath3.amt.ac.cn
IP address: 159.226.47.14
Alias(es): None

Host name: lsc02.iss.ac.cn
IP address: 159.226.47.217
Alias(es): None

No DNS Record
The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
CN
Netname: NCFC
Netblock: 159.226.0.0 - 159.226.255.255

6. Correlations:

None. Only after consulting with the network administrator can correlations be made. Without knowing the reason for tracking these connections, any correlation would strictly be a guess.

7. Evidence of active targeting:

In the case of FTP connections, there is reason to believe this is active targeting. The NCFC watchlist logged attempts to only a single host. This would obviously point toward active targeting.

8. Severity:

Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

If this traffic is unwelcome, there are many steps that this organization can take to negate some of these vulnerabilities. The first should be to implement proxy services or Network Address Translation (NAT) for hosts that do not require public access. This will prevent most of the outside connections to internal hosts by using private addresses. The second recommendation would be to implement a stateful inspection firewall. This will also prevent unwanted outside connections to internal hosts. Publicly accessible hosts should use security features such as TCP wrappers to protect themselves at the host level. If there is absolutely no legitimate interface with this network, blocks can be implemented through Access Control Lists (ACLs) and firewalls. If GIAC Enterprises desires to continue allowing these connections with the intent to monitor the activity, sniffers should be used. At minimum, the Snort watchlist signatures should be modified to record activity both ways.

WU-FTP Exploit

Date/Time	Snort Signature	Source IP : Port	Destination IP : Port
11/26-17:30:50.939661	site exec - Possible wu-ftpd exploit - GIAC000623	24.23.255.246:4507	MY.NET.130.98:21
12/16-12:21:46.219962	SITE EXEC - Possible wu-ftpd exploit - GIAC000623	209.162.94.11:4584	MY.NET.156.127:21
12/21-15:26:29.595664	site exec - Possible wu-ftpd exploit - GIAC000623	64.217.116.106:1684	MY.NET.97.162:21

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however any attempt to transfer data would have been very difficult. In this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

This is probably an attempt by an attacker exploiting the Wu-Ftpd Remote Format String Stack Overwrite Vulnerability.

5. Attack mechanism:

The attacker logs in remotely to the FTP server as user Anonymous. Then, he or she runs the exploit which uses a format string or a buffer overflow to drop into a shell code and execute commands as root.

Host Info:

Host name: cm47580-a.ftwrth1.tx.home.com
IP address: 24.23.255.246
Alias(es): None

No DNS records
Verio, Inc. (NET-VRIO-R-2)
8005 South Chester Street
Englewood, CO 80112
US
Netname: VRIO-R-2
Netblock: 209.162.64.0 - 209.162.127.255
Maintainer: VRIO

Host name: adsl-64-217-116-106.dsl.hstntx.swbell.net
IP address: 64.217.116.106
Alias(es): None

6. Correlations:
Network Ice
http://advice.networkice.com/Advice/Intrusions/2001322/default.htm

Bugtraq
http://www.securityfocus.com/bid/1387.html

CVE-1999-0997
wu-ftp with FTP conversion enabled allows an attacker to execute commands via a malformed file name that is interpreted as an argument to the program that does the conversion, e.g. tar or uncompress.

Reference: BUGTRAQ:19991220 Security vulnerability in certain wu-ftpd (and derivitives) configurations (fwd)
Reference: XF:wuftp-ftp-conversion

CVE-1999-0880
Denial of service in WU-FTPD via the SITE NEWER command, which does not free memory properly.

Reference: CERT:CA-99-13
Reference: XF:wuftp-site-newer-dos

CVE-1999-0879
Buffer overflow in WU-FTPD and related FTP servers allows remote attackers to gain root privileges via macro variables in a message file.

Reference: CERT:CA-99-13

Reference: XF:wuftp-message-file-root

7. Evidence of active targeting:

Evidence of active targeting is not clear with limited information. If all three hosts are running WU FTP then there is strong evidence. We can, however, assume this is weak evidence that active targeting is implied by the fact that only three hosts were targeted.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

These hosts should be reviewed very carefully. If they are running an older version of WU FTP, we should assume these hosts are compromised and steps should be taken to collect forensic evidence. This would include disconnecting the hosts from the network, imaging the drive using “dd” or some other utility that will execute a binary copy and contacting law enforcement (if GIAC Enterprises wishes to pursue an investigation). The sensitivity of the information on these hosts should also be assessed. Any trust relationships with this host should also be reviewed and appropriate action should be taken on other hosts.

Once rebuilt, system administrators should ensure the latest vendor patches and version of WU FTP is installed.

Virus

Date/Time	Snort Signature	Source IP : Port	Destination IP : Port
12/22-20:25:10.840208	Happy 99 Virus	63.216.198.158:2239	MY.NET.6.47:25

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

It is not likely the source address was spoofed. The activity appears to a normal mail exchange between two mail servers.

4. Description of attack:

Happy 99 is a worm that displays fireworks and a “happy new year 1999!” message while infecting the host.

5. Attack mechanism:

This worm propagates through newsgroup postings and as an email attachment. When infected, the host displays fireworks and a “happy new year 1999!” message. The worm then copies itself as ska.exe and moves ska.dll to the windows\system directory. It then moves changes wsock32.dll to wsock32.ska and copies a new wsock32.dll file to the windows\system directory. When the new wsock32.dll file detects a connection to the Internet, the wsock.dll file loads ska.dll into memory. Ska.dll then creates a new self-infected posting or email and sends it to a newsgroup or email address.

Host Info:
Host name: ffml.fanfic.com
IP address: 63.216.198.158
Alias(es): None

6. Correlations:
Network Associates
http://vil.nai.com/vil/dispVirus.asp?virus_k=10144

Symantec
http://www.symantec.com/avcenter/venc/data/happy99.worm.html

7. Evidence of active targeting:

In this case, there is no reason to believe this is active targeting. Although a specific email account can be targeted, it is likely the source account is infected with this worm.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

If there are any clients infected with this worm, they can be cleaned using a utility called fixhappy.exe by Symantec. This utility can be downloaded from http://www.sarc.com/avcenter/venc/data/fix.happy99.worm.html.

Defensive recommendations are to use an antivirus product on every host. A specific product for email servers should also be used. Beyond this, System Administrators need to take steps to ensure updates are applied on a regular basis. Use of enterprise level antivirus software to manage upgrades and signature updates would be highly recommended.

DNS DoS

Date/Time	Snort Signature	Source IP : Port	Destination IP : Port
01/06-18:30:02.600073	DNS udp DoS attack described on unisog	209.67.50.203:9247	MY.NET.1.3:53
01/06-18:30:03.176672	DNS udp DoS attack described on unisog	209.67.50.203:6616	MY.NET.1.5:53
01/06-18:30:03.735366	DNS udp DoS attack described on unisog	209.67.50.203:7115	MY.NET.1.5:53
01/06-18:30:03.870078	DNS udp DoS attack described on unisog	209.67.50.203:16707	MY.NET.1.4:53
01/06-18:30:05.030330	DNS udp DoS attack described on unisog	209.67.50.203:10165	MY.NET.1.3:53
01/06-18:30:05.051934	DNS udp DoS attack described on unisog	209.67.50.203:14525	MY.NET.1.4:53
01/06-18:30:05.243735	DNS udp DoS attack described on unisog	209.67.50.203:2266	MY.NET.1.5:53
01/06-18:30:06.101392	DNS udp DoS attack described on unisog	209.67.50.203:3452	MY.NET.1.4:53
01/06-18:30:06.379466	DNS udp DoS attack described on unisog	209.67.50.203:2937	MY.NET.1.4:53
01/06-18:30:06.800306	DNS udp DoS attack described on unisog	209.67.50.203:17208	MY.NET.1.4:53
01/06-18:30:08.201785	DNS udp DoS attack described on unisog	209.67.50.203:5827	MY.NET.1.4:53
01/06-18:30:08.226652	DNS udp DoS attack described on unisog	209.67.50.203:27265	MY.NET.1.3:53
…			
01/06-19:59:59.820729	DNS udp DoS attack described on unisog	209.67.50.203:17112	MY.NET.1.3:53
01/06-20:00:00.395683	DNS udp DoS attack described on unisog	209.67.50.203:22465	MY.NET.1.3:53
01/06-20:00:00.401199	DNS udp DoS attack described on unisog	209.67.50.203:16692	MY.NET.1.5:53
01/06-20:00:00.497696	DNS udp DoS attack described on unisog	209.67.50.203:28333	MY.NET.1.4:53
01/06-20:00:00.685505	DNS udp DoS attack described on unisog	209.67.50.203:6158	MY.NET.1.4:53
01/06-20:00:00.698393	DNS udp DoS attack described on unisog	209.67.50.203:29931	MY.NET.1.5:53
01/06-20:00:00.725528	DNS udp DoS attack described on unisog	209.67.50.203:13299	MY.NET.1.4:53
01/06-20:00:00.826654	DNS udp DoS attack described on unisog	209.67.50.203:12032	MY.NET.1.4:53
01/06-20:00:00.939018	DNS udp DoS attack described on unisog	209.67.50.203:20065	MY.NET.1.5:53
01/06-20:00:00.968516	DNS udp DoS attack described on unisog	209.67.50.203:28054	MY.NET.1.4:53
01/06-20:00:01.567114	DNS udp DoS attack described on unisog	209.67.50.203:23516	MY.NET.1.3:53

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

There is a high probability the source IP address is spoofed. The attacker needs to do this in order for this attack to work.

4. Description of attack:

This is a Denial of Service attack against the DNS server at 209.67.50.203 (register.com.) MY.NET.1.3 is being use as an amplifier.

5. Attack mechanism:

This is a DoS sends many UDP packets from a spoofed source. These UDP packets are requests for hosts that are not in the DNS server's domain.

The responses are then sent to the spoofed source. The GIAC Enterprises DNS server is an amplifier for this attack on 209.67.50.203. It is likely other sites are also included as amplifiers.

Host Info:
Host name: futuresite.register.com
IP address: 209.67.50.203
Alias(es): None

6. Correlations:
Unisog Archive
http://www.theorygroup.com/Archive/Unisog/2001/msg00166.html
http://www.theorygroup.com/Archive/Unisog/2001/msg00028.html

7. Evidence of active targeting:

There is evidence of active targeting in the fact that the DNS server (assuming it is a DNS server) is correctly being sent request packets, although the true target is register.com.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

Because this attack is not targeting GIAC Enterprises, there is no defensive posture to assume. However, as a good Samaritan, GIAC enterprises should participate in blocking DNS requests from 209.67.50.X addresses. This will prevent GIAC Enterprises from being an amplifier for this attack on register.com.

SNMP Public Access from an outside IP

Date / Time	Snort Signature	Source IP : Port	Destination IP : Port
01/10-16:34:49.681860	SNMP public access	128.46.156.231:3613	MY.NET.100.143:161
01/12-09:32:02.380437	SNMP public access	128.46.156.231:1092	MY.NET.100.143:161
01/12-09:32:04.048761	SNMP public access	128.46.156.231:1093	MY.NET.100.143:161
01/12-09:32:04.082561	SNMP public access	128.46.156.231:1093	MY.NET.100.143:161
01/12-09:32:04.134998	SNMP public access	128.46.156.231:1094	MY.NET.100.143:161
01/12-09:32:32.861225	SNMP public access	128.46.156.231:1118	MY.NET.100.143:161
01/12-09:32:54.185026	SNMP public access	128.46.156.231:1139	MY.NET.100.143:161
…			
01/12-09:48:31.267780	SNMP public access	128.46.156.231:1836	MY.NET.100.143:161
01/12-09:50:07.163350	SNMP public access	128.46.156.231:1904	MY.NET.100.143:161
01/12-09:51:28.690592	SNMP public access	128.46.156.231:1936	MY.NET.100.143:161

```
01/12-09:52:36.669423    SNMP public access    128.46.156.231:1993    MY.NET.100.143:161
01/12-09:52:50.768559    SNMP public access    128.46.156.231:2007    MY.NET.100.143:161
01/12-09:55:20.701278    SNMP public access    128.46.156.231:2063    MY.NET.100.143:161
01/12-09:56:43.001464    SNMP public access    128.46.156.231:2163    MY.NET.100.143:161
01/12-09:58:18.352143    SNMP public access    128.46.156.231:2199    MY.NET.100.143:161


01/12-09:31:41.697088    SNMP public access    128.46.156.231:1030    MY.NET.100.206:161
01/12-09:32:32.317978    SNMP public access    128.46.156.231:1114    MY.NET.100.206:161
01/12-09:32:32.569345    SNMP public access    128.46.156.231:1116    MY.NET.100.206:161
01/12-09:32:53.662295    SNMP public access    128.46.156.231:1135    MY.NET.100.206:161
01/12-09:32:53.709137    SNMP public access    128.46.156.231:1136    MY.NET.100.206:161
01/12-09:32:53.947386    SNMP public access    128.46.156.231:1138    MY.NET.100.206:161
01/12-09:33:17.654381    SNMP public access    128.46.156.231:1158    MY.NET.100.206:161
01/12-09:33:17.968169    SNMP public access    128.46.156.231:1160    MY.NET.100.206:161
01/12-09:34:42.314712    SNMP public access    128.46.156.231:1284    MY.NET.100.206:161
01/12-09:42:57.341289    SNMP public access    128.46.156.231:1514    MY.NET.100.206:161
01/12-09:44:19.520108    SNMP public access    128.46.156.231:1591    MY.NET.100.206:161
01/12-09:45:44.116775    SNMP public access    128.46.156.231:1689    MY.NET.100.206:161
01/12-09:47:07.313113    SNMP public access    128.46.156.231:1771    MY.NET.100.206:161
01/12-09:48:30.740509    SNMP public access    128.46.156.231:1832    MY.NET.100.206:161
01/12-09:48:31.026710    SNMP public access    128.46.156.231:1835    MY.NET.100.206:161
01/12-09:51:14.084949    SNMP public access    128.46.156.231:1918    MY.NET.100.206:161
01/12-09:51:14.130191    SNMP public access    128.46.156.231:1919    MY.NET.100.206:161
01/12-09:52:36.428963    SNMP public access    128.46.156.231:1992    MY.NET.100.206:161
01/12-09:53:57.883877    SNMP public access    128.46.156.231:2014    MY.NET.100.206:161
01/12-09:56:42.477347    SNMP public access    128.46.156.231:2159    MY.NET.100.206:161
01/12-09:58:03.820059    SNMP public access    128.46.156.231:2181    MY.NET.100.206:161


01/12-09:32:10.408144    SNMP public access    128.46.156.231:1096    MY.NET.100.99:161
01/12-09:32:10.649334    SNMP public access    128.46.156.231:1097    MY.NET.100.99:161
01/12-09:32:16.978157    SNMP public access    128.46.156.231:1100    MY.NET.100.99:161
01/12-09:32:17.639995    SNMP public access    128.46.156.231:1102    MY.NET.100.99:161
01/12-09:32:19.840132    SNMP public access    128.46.156.231:1104    MY.NET.100.99:161
01/12-09:32:21.340805    SNMP public access    128.46.156.231:1105    MY.NET.100.99:161
01/12-09:32:36.751741    SNMP public access    128.46.156.231:1122    MY.NET.100.99:161
01/12-09:32:38.252377    SNMP public access    128.46.156.231:1122    MY.NET.100.99:161
01/12-09:32:39.755890    SNMP public access    128.46.156.231:1123    MY.NET.100.99:161
01/12-09:32:40.383916    SNMP public access    128.46.156.231:1126    MY.NET.100.99:161
01/12-09:32:56.605378    SNMP public access    128.46.156.231:1143    MY.NET.100.99:161
…
01/12-09:54:12.361099    SNMP public access    128.46.156.231:2027    MY.NET.100.99:161
01/12-09:55:21.726622    SNMP public access    128.46.156.231:2065    MY.NET.100.99:161
01/12-09:55:21.990634    SNMP public access    128.46.156.231:2066    MY.NET.100.99:161
01/12-09:55:28.716139    SNMP public access    128.46.156.231:2073    MY.NET.100.99:161
01/12-09:55:29.144785    SNMP public access    128.46.156.231:2075    MY.NET.100.99:161
01/12-09:56:48.423324    SNMP public access    128.46.156.231:2168    MY.NET.100.99:161
```

```
01/12-09:56:50.337560   SNMP public access   128.46.156.231:2171   MY.NET.100.99:161
01/12-09:56:53.542213   SNMP public access   128.46.156.231:2173   MY.NET.100.99:161
01/12-09:58:11.687024   SNMP public access   128.46.156.231:2193   MY.NET.100.99:161
01/12-09:58:11.887152   SNMP public access   128.46.156.231:2194   MY.NET.100.99:161
01/12-09:58:18.098849   SNMP public access   128.46.156.231:2197   MY.NET.100.99:161
```

```
01/11-16:41:49.070093   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-16:51:49.082046   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-16:51:55.503209   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-16:52:01.506795   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-16:52:07.538894   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-17:42:07.773525   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-17:52:07.771329   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-18:02:07.816540   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/11-18:12:07.868642   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/12-09:17:50.224557   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/12-09:27:50.250923   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
01/12-09:37:50.305146   SNMP public access   128.183.38.30:1032    MY.NET.154.26:161
```

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however any attempt to transfer data would have been very difficult. In this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

Access to SNMP agents can be used as a method of performing reconnaissance or attack.

5. Attack mechanism:

SNMP is used to manage network devices. Consoles are able to pass configuration information to agents on network devices. Potential attackers can also use this for their advantage. SNMP can present attackers with vital network infrastructure information. There is also a possibility an attacker can use SNMP to change the configuration of network device. This may be a Denial of Service if a router or switch is reconfigured or by changing routing tables an attacker may be able to bypass firewalls, IDS or other security measures.

Host Info:

Host name: ece156-dhcp-2.ecn.purdue.edu
IP address: 128.46.156.231
Alias(es): None

Host name: cesdis6.gsfc.nasa.gov
IP address: 128.183.38.30
Alias(es): None

6. Correlations:
CVE-1999-0294
All records in a WINS database can be deleted through SNMP for a denial of service.

Reference: XF:nt-wins-snmp2

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.

Reference: XF:netcache-snmp
Reference: BUGTRAQ:Apr7,1999

CVE-2000-0221
The Nautica Marlin bridge allows remote attackers to cause a denial of service via a zero length UDP packet to the SNMP port.

Reference: BUGTRAQ:20000225 Scorpion Marlin
Reference: BID:1009

CVE-2000-0379
The Netopia R9100 router does not prevent authenticated users from modifying SNMP tables, even if the administrator has configured it to do so.

Reference: BUGTRAQ:20000507 Advisory: Netopia R9100 router vulnerability
Reference:
http://www.securityfocus.com/templates/archive.pike?list=1&msg=200005082054.NAA32590@linux.mtndew.com
Reference:
CONFIRM:http://www.netopia.com/equipment/purchase/fmw_update.html
Reference: BID:1177
Reference: XF:netopia-snmp-comm-strings

CVE-2000-0515

The snmpd.conf configuration file for the SNMP daemon (snmpd) in HP-UX 11.0 is world writable, which allows local users to modify SNMP configuration or gain privileges.

Reference: BUGTRAQ:20000607 [Hackerslab bug_paper] HP-UX SNMP daemon vulnerability
Reference: BUGTRAQ:20000608 Re: HP-UX SNMP daemon vulnerability
Reference: BID:1327
Reference: XF:hpux-snmp-daemon

CVE-2000-1058
Buffer overflow in OverView5 CGI program in HP OpenView Network Node Manager (NNM) 6.1 and earlier allows remote attackers to cause a denial of service, and possibly execute arbitrary commands, in the SNMP service (snmp.exe), aka the "Java SNMP MIB Browser Object ID parsing problem."

Reference: BUGTRAQ:20000926 DST2K0014: BufferOverrun in HP Openview Network Node Manager v6.1 (Round2)
Reference: HP:HPSBUX0009-121
Reference: XF:openview-nmm-snmp-bo

7. Evidence of active targeting:

The logs appear to be specific connections to a few GIAC hosts. This leads to the conclusion of active targeting.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

Network managers should take steps to disable any SNMP agents not in use. They should also ensure default passwords are not used. Routers or firewalls should block any SNMP request from outside networks.

SUNRPC highport access

Date / Time	Snort Signature	Source IP : Port	Destination IP : Port
01/05-11:19:08.063764	SUNRPC highport access!	128.169.50.34:21	MY.NET.5.11:32771
01/05-11:19:08.068073	SUNRPC highport access!	128.169.50.34:21	MY.NET.5.11:32771
01/05-11:19:08.158010	SUNRPC highport access!	128.169.50.34:21	MY.NET.5.11:32771
01/05-11:19:08.323482	SUNRPC highport access!	128.169.50.34:21	MY.NET.5.11:32771
01/05-11:19:16.210572	SUNRPC highport access!	128.169.50.34:21	MY.NET.5.11:32771
12/21-22:43:46.133922	SUNRPC highport access!	130.207.7.22:51606	MY.NET.7.22:32771

```
12/21-22:43:46.133985   SUNRPC highport access!   130.207.7.22:51606      MY.NET.7.22:32771

12/03-13:54:20.365600   SUNRPC highport access!   152.163.241.59:5190     MY.NET.54.217:32771

12/31-06:40:42.244777   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771
12/31-06:40:42.253250   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771
12/31-06:40:42.263516   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771
12/31-06:40:42.270972   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771
12/31-06:40:42.462597   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771
12/31-06:40:42.471049   SUNRPC highport access!   152.163.241.88:5190     MY.NET.17.44:32771

12/05-20:17:38.253815   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:20:07.794599   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:20:15.224827   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:21:40.992571   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:23:36.396887   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:29:37.192939   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:44:40.540182   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:46:21.208842   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/05-20:47:29.276028   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/06-21:56:06.048893   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/06-22:36:44.771799   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/06-23:44:00.407711   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-01:15:41.604838   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-01:53:07.656459   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-03:14:59.350922   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-03:26:34.012538   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-03:43:24.715842   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-05:15:06.849350   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-05:37:38.369554   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-06:47:10.597296   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-06:57:10.607799   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-06:59:10.462834   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-07:03:37.759272   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-07:18:11.287656   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-07:28:21.587730   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-07:41:07.540439   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-07:52:21.771867   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/07-08:52:10.546675   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-13:33:41.037653   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-13:33:42.006481   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-13:34:49.012699   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-13:50:55.635303   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-13:59:49.873022   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-14:28:45.357388   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:11:48.189807   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:45:15.934457   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:48:54.024562   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:51:23.327064   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:52:23.676359   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:54:37.798610   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:55:22.278493   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
12/20-15:55:27.276329   SUNRPC highport access!   205.188.153.139:9898   MY.NET.213.158:32771
```

```
12/20-15:55:34.584624    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-16:09:16.740087    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-16:42:29.508005    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-16:42:47.294021    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-16:44:07.729812    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-18:45:16.132094    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-18:45:55.649855    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-19:16:26.973037    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-21:10:41.229108    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-21:45:54.082534    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-21:47:20.172507    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-21:54:26.252952    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-21:59:26.258679    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-22:37:25.940422    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/20-23:26:15.014694    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-00:58:02.549503    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-01:03:02.553989    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-01:38:26.484112    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-01:48:26.496497    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-01:59:28.450355    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-02:13:43.572091    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-02:38:25.269309    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:00:58.015693    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:38:19.684849    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:43:19.690080    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:45:39.642812    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:50:23.550569    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-03:51:02.039171    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-04:50:32.993419    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-05:15:45.737805    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-05:20:45.944337    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-05:29:02.708723    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-05:50:38.614684    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-05:59:17.992393    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-06:04:18.000998    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-06:44:07.863992    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-07:15:18.103222    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-07:21:29.504931    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-07:26:05.401892    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-07:31:05.406500    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-07:31:06.691139    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-08:17:54.863343    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-08:28:57.072293    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-08:45:28.879304    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-08:50:28.884277    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-09:51:34.780357    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-10:19:30.370628    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-11:51:13.481152    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771
12/21-12:42:13.617301    SUNRPC highport access!    205.188.153.139:9898    MY.NET.213.158:32771

01/16-01:59:15.223453    SUNRPC highport access!    205.188.4.6:5190        MY.NET.218.238:32771
01/16-01:59:15.231934    SUNRPC highport access!    205.188.4.6:5190        MY.NET.218.238:32771
01/16-01:59:15.448343    SUNRPC highport access!    205.188.4.6:5190        MY.NET.218.238:32771
```

```
01/16-01:59:15.457213    SUNRPC highport access!    205.188.4.6:5190         MY.NET.218.238:32771

12/15-22:24:53.415576    SUNRPC highport access!    205.188.5.160:5190       MY.NET.222.2:32771
01/08-18:22:53.058420    SUNRPC highport access!    205.188.7.102:5190       MY.NET.98.191:32771

12/31-00:21:20.039275    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:20.156283    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:20.157864    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:20.746944    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:21.335161    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:21.617221    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771
12/31-00:21:21.743409    SUNRPC highport access!    206.196.168.157:2609     MY.NET.99.51:32771

11/28-20:09:53.108823    SUNRPC highport access!    209.10.41.242:1042       MY.NET.99.104:32771

12/13-03:41:03.439255    SUNRPC highport access!    209.39.89.55:25          MY.NET.6.47:32771

12/23-20:59:11.702742    SUNRPC highport access!    213.188.15.246:21        MY.NET.97.100:32771

12/05-15:55:07.601880    SUNRPC highport access!    216.10.12.2:23           MY.NET.213.158:32771

12/03-20:36:24.582489    SUNRPC highport access!    216.10.12.30:2078        MY.NET.206.222:32771
12/03-20:36:29.704960    SUNRPC highport access!    216.10.12.30:2078        MY.NET.206.222:32771
12/03-20:36:29.720767    SUNRPC highport access!    216.10.12.30:2078        MY.NET.206.222:32771
12/03-20:36:29.722192    SUNRPC highport access!    216.10.12.30:2078        MY.NET.206.222:32771
12/05-16:37:55.326324    SUNRPC highport access!    216.10.12.30:2078        MY.NET.213.158:32771

12/12-14:49:32.433800    SUNRPC highport access!    216.10.14.143:10344      MY.NET.213.158:32771
12/12-14:49:32.899424    SUNRPC highport access!    216.10.14.143:10344      MY.NET.213.158:32771
12/12-15:06:16.221657    SUNRPC highport access!    216.10.14.143:10344      MY.NET.213.158:32771

12/20-12:31:53.282646    SUNRPC highport access!    216.10.14.143:1300       MY.NET.213.158:32771

11/28-06:33:10.939778    SUNRPC highport access!    216.148.218.160:443      MY.NET.206.222:32771
12/15-04:44:44.944459    SUNRPC highport access!    216.148.218.160:443      MY.NET.213.158:32771

01/12-15:07:27.354404    SUNRPC highport access!    216.35.221.79:7070       MY.NET.218.158:32771

12/30-21:37:38.581244    SUNRPC highport access!    216.99.200.242:24618     MY.NET.202.94:32771
12/30-21:37:41.575658    SUNRPC highport access!    216.99.200.242:24618     MY.NET.202.94:32771
12/30-21:12:18.803354    SUNRPC highport access!    216.99.200.242:24713     MY.NET.202.94:32771
12/30-21:12:21.788295    SUNRPC highport access!    216.99.200.242:24713     MY.NET.202.94:32771
12/30-21:37:51.603517    SUNRPC highport access!    216.99.200.242:26684     MY.NET.202.94:32771
12/30-21:37:57.610694    SUNRPC highport access!    216.99.200.242:26684     MY.NET.202.94:32771

12/23-14:44:43.627109    SUNRPC highport access!    24.180.174.167:2731      MY.NET.60.11:32771
12/23-17:31:14.213666    SUNRPC highport access!    24.180.174.167:3439      MY.NET.60.11:32771

12/03-12:21:46.696560    SUNRPC highport access!    24.180.202.45:1991       MY.NET.99.51:32771
12/03-12:21:46.801019    SUNRPC highport access!    24.180.202.45:1991       MY.NET.99.51:32771
12/03-12:21:46.819925    SUNRPC highport access!    24.180.202.45:1991       MY.NET.99.51:32771
```

```
12/03-12:21:46.827424   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:46.855923   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:46.897947   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:47.119851   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:47.162132   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
…
12/03-12:21:48.251599   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.302220   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.311342   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.331620   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.363330   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.372490   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.384401   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771
12/03-12:21:48.464327   SUNRPC highport access!   24.180.202.45:1991     MY.NET.99.51:32771

01/10-21:37:53.953115   SUNRPC highport access!   24.189.31.228:4986     MY.NET.217.150:32771
12/08-09:33:45.135402   SUNRPC highport access!   24.7.177.100:12409     MY.NET.213.158:32771
12/08-09:34:49.853518   SUNRPC highport access!   24.7.177.100:12409     MY.NET.213.158:32771
12/08-09:36:20.036298   SUNRPC highport access!   24.7.177.100:12409     MY.NET.213.158:32771
12/08-09:56:33.848086   SUNRPC highport access!   24.7.177.100:12409     MY.NET.213.158:32771
12/08-16:12:56.533814   SUNRPC highport access!   24.7.177.100:12409     MY.NET.213.158:32771

12/23-15:46:15.473588   SUNRPC highport access!   61.139.110.69:3499     MY.NET.98.174:32771

12/13-19:17:32.258784   SUNRPC highport access!   63.17.39.163:2406      MY.NET.213.158:32771

01/15-16:12:31.758899   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:12:32.126660   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:12:32.286508   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:13:07.686859   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:13:27.826047   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:13:31.159723   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:13:46.117024   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:14:01.040646   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:14:02.922115   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:14:22.843477   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:14:57.840949   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:15:02.856726   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:15:27.282224   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:15:57.952991   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:16:12.999754   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:16:52.113058   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:16:52.123816   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:17:03.073912   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
01/15-16:17:38.034816   SUNRPC highport access!   64.4.13.74:1863        MY.NET.98.199:32771
```

Many of these logs are likely false positives. The signature looks for a connection with port 32771. In some cases, 32771 is an ephemeral port used as the source port for connections to the Internet. Some of this traffic included AOL, FTP, MSNP, telnet, HTTPS…etc. However, there is a possibility an attacker could use common source ports to fool IDS and Intrusion Analysts alike. For this reason, all connections should be further analyzed.

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however in this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

Sun RPC services can be exploited with known vulnerabilities. These services run at dynamic ports from 32771 and up. Statd, Calendar Manager and Tooltalk are a few of the more commonly exploited buffer overlows associated with Sun RPC.

5. Attack mechanism:

Once the service identified, an attacker can run scripts against that port to cause a buffer overflow. In many cases, this would drop the attacker down to a command prompt running at root level. Often, once these exploits are used, attackers will then create backdoors.

Host Info:

Host name: HELIOS.TNS.UTK.EDU
IP address: 128.169.50.34
Alias(es): None

Host name: smitheus.cc.gatech.edu
IP address: 130.207.7.22
Alias(es): None

No DNS Record
America Online (NET-ANS-BNET8)
12100 Sunrise Valley Drive
Reston, VA 20191
US
Netname: AOL-BNET
Netblock: 152.163.0.0 - 152.163.255.255

Host name: toc-d01.blue.aol.com
IP address: 205.188.153.139

```
Alias(es): None

No DNS Record
America Online, Inc (NETBLK-AOL-DTC)
22080 Pacific Blvd
Sterling, VA 20166
US
Netname: AOL-DTC
Netblock: 205.188.0.0 - 205.188.255.255

Host name: baltbay1-29.dial.umd.edu
IP address: 206.196.168.157
Alias(es): None

Host name: zeus.kernel.org
IP address: 209.10.41.242
Alias(es): 242.41.10.209.in-addr.arpa

Host name: mailcluster.processrequest.com
IP address: 209.39.89.55
Alias(es): None

No DNS Record
European Regional Internet Registry/RIPE NCC (NETBLK-213-
RIPE)
These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-213
Netblock: 213.0.0.0 - 213.255.255.255
Maintainer: RIPE

Host name: kinetic.cpanel.net
IP address: 216.10.12.2
Alias(es): 2.12.10.216.in-addr.arpa

Host name: gravity.cpanel.net
IP address: 216.10.12.30
Alias(es): 30.12.10.216.in-addr.arpa

No DNS Record
Virtual Development Inc (NETBLK-VDI)
1373 Broad Street, Suite 306
Clifton, NJ 07013
```

```
US
Netname: VDI
Netblock: 216.10.0.0 - 216.10.31.255
Maintainer: VDI

Host name: head.rwc.rhns.redhat.com
IP address: 216.148.218.160
Alias(es): None

No DNS Records
Exodus Commnications Inc. (NETBLK-ECI-7)
1605 Wyatt Dr. Santa Clara, CA
95054US
US
Netname: ECI-7
Netblock: 216.32.0.0 - 216.35.255.255
Maintainer: ECI

Host name: securedesign.net
IP address: 216.99.200.242
Alias(es): None

Host name: cc768805-a.hwrd1.md.home.com
IP address: 24.180.174.167
Alias(es): None

Host name: cc889103-a.hwrd1.md.home.com
IP address: 24.180.202.45
Alias(es): None

Host name: ool-18bd1fe4.dyn.optonline.net
IP address: 24.189.31.228
Alias(es): None

Host name: cc263637-a.chstfld1.va.home.com
IP address: 24.7.177.100
Alias(es): None

No DNS Records
Asia Pacific Network Information Center (NETBLK-APNIC2)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC3
```

Netblock: 61.0.0.0 - 61.255.255.255
Maintainer: AP

Host name: 1Cust163.tnt18.det3.da.uu.net
IP address: 63.17.39.163
Alias(es): None

Host name: msgr-sb5.msgr.hotmail.com
IP address: 64.4.13.74
Alias(es): None

6. Correlations:
SANS: How To Eliminate The Ten Most Critical
Internet Security Threats
http://www.sans.org/topten.htm

CVE-1999-0493
rpc.statd allows remote attackers to forward RPC calls to the local operating system via the SM_MON and SM_NOTIFY commands, which in turn could be used to remotely exploit other bugs such as in automountd.

Reference: CERT:CA-99-05
Reference: SUN:00186
Reference: CIAC:J-045
Reference: BUGTRAQ:19990103 SUN almost has a clue! (automountd)
Reference: BID:450

CVE-1999-0019
Delete or create a file via rpc.statd, due to invalid information.

Reference: CERT:CA-96.09.rpc.statd
Reference: XF:rpc-stat
Reference: SUN:00135

CVE-1999-0018
Buffer overflow in statd allows root privileges.

Reference: CERT:CA-97.26.statd
Reference: AUSCERT:AA-97.29
Reference: XF:statd
Reference: BID:127

CVE-1999-0003
Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd)

Reference: NAI:NAI-29
Reference: CERT:CA-98.11.tooltalk
Reference: SGI:19981101-01-A
Reference: SGI:19981101-01-PX
Reference: XF:aix-ttdbserver
Reference: XF:tooltalk
Reference: BID:122

CVE-1999-0696
Buffer overflow in CDE Calendar Manager Service Daemon (rpc.cmsd)

Reference: BUGTRAQ:19990709 Exploit of rpc.cmsd
Reference: SCO:SB-99.12
Reference: SUN:00188
Reference: SUNBUG:4230754
Reference: HP:HPSBUX9908-102
Reference: COMPAQ:SSRT0614U_RPC_CMSD
Reference: CERT:CA-99-08
Reference: CIAC:J-051
Reference: XF:sun-cmsd-bo

CVE-1999-0189
Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.

Reference: NAI:NAI-15
Reference: SUN:00142
Reference: XF:rpc-32771

CVE-1999-0190
Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access.

Reference: SUN:00167
Reference: XF:sun-rpcbind

CVE-1999-0208
rpc.ypupdated (NIS) allows remote users to execute arbitrary commands.

Reference: XF:rpc-update
Reference: CERT:CA-95.17.rpc.ypupdated.vul

CVE-1999-0211
Extra long export lists over 256 characters in some mount daemons allows NFS directories to be mounted by anyone.

Reference: CERT:CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability

7. Evidence of active targeting:

As stated above, many of these are probably false positives; however any hosts running Sun RPC services would be a strong indication of targeting.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

Incident response should first be taken care of, beginning with review of IDS logs identifying the *NIX hosts. This would be a good first cut. System administrators should review these hosts for vulnerable versions of RPC services and the presence of backdoor listeners. Any indication of compromise should be dealt with by taking the host offline, creating a binary image of the hard drive and contacting law enforcement (if desired).

Defensive recommendations are to make a determination if RPC services are needed. Any host without this requirement should have these services disabled. Hosts that do require Sun RPC should have the latest vendor patches installed. Host based IDS would also be very recommendable.

External RPC Call

Date / Time	Snort Signature	Source IP : Port	Destination IP : Port
11/29-08:01:31.926544	External RPC call	208.37.228.142:4818	MY.NET.100.130:111
12/03-15:41:59.837838	External RPC call	65.33.58.115:894	MY.NET.6.15:111
12/03-15:52:33.025189	External RPC call	65.33.58.115:2789	MY.NET.100.130:111
12/12-20:36:52.984296	External RPC call	211.50.30.241:914	MY.NET.6.15:111
12/12-20:43:18.574178	External RPC call	61.9.26.50:1196	MY.NET.6.15:111
12/16-18:02:36.892562	External RPC call	195.116.66.14:958	MY.NET.6.15:111
12/16-18:16:58.151187	External RPC call	195.116.66.14:4348	MY.NET.133.65:111
12/16-18:17:02.161221	External RPC call	195.116.66.14:4508	MY.NET.133.225:111
12/16-18:17:02.163382	External RPC call	195.116.66.14:4521	MY.NET.133.238:111
12/16-18:17:04.128419	External RPC call	195.116.66.14:4468	MY.NET.133.185:111
12/16-18:17:04.130640	External RPC call	195.116.66.14:4472	MY.NET.133.189:111
12/16-18:17:05.163587	External RPC call	195.116.66.14:4532	MY.NET.133.249:111
12/16-18:17:05.163641	External RPC call	195.116.66.14:4533	MY.NET.133.250:111
12/17-15:21:11.182993	External RPC call	209.178.23.187:1966	MY.NET.133.100:111
12/20-15:05:30.479083	External RPC call	148.228.125.215:1754	MY.NET.133.16:111
12/20-15:05:30.492407	External RPC call	148.228.125.215:1826	MY.NET.133.87:111
12/20-15:05:33.432083	External RPC call	148.228.125.215:1995	MY.NET.133.252:111
12/20-15:05:33.433899	External RPC call	148.228.125.215:1997	MY.NET.133.254:111
12/20-15:05:33.434043	External RPC call	148.228.125.215:1740	MY.NET.133.2:111
12/20-15:05:33.434096	External RPC call	148.228.125.215:1742	MY.NET.133.4:111
12/20-15:05:33.478589	External RPC call	148.228.125.215:1942	MY.NET.133.199:111
12/20-15:05:33.478686	External RPC call	148.228.125.215:1813	MY.NET.133.74:111
12/20-15:05:33.478738	External RPC call	148.228.125.215:1814	MY.NET.133.75:111

```
12/20-15:05:33.485015    External RPC call    148.228.125.215:1842    MY.NET.133.103:111
12/20-15:05:33.485064    External RPC call    148.228.125.215:1843    MY.NET.133.104:111
12/20-15:05:33.485983    External RPC call    148.228.125.215:1850    MY.NET.133.111:111
12/20-15:05:33.495392    External RPC call    148.228.125.215:1884    MY.NET.133.141:111
12/22-09:33:22.421500    External RPC call    195.57.62.153:2567      MY.NET.15.127:111
12/24-23:09:31.264010    External RPC call    208.185.235.100:1605    MY.NET.6.15:111
12/24-23:09:31.264509    External RPC call    208.185.235.100:1605    MY.NET.6.15:111
12/24-23:09:31.439030    External RPC call    208.185.235.100:1605    MY.NET.6.15:111
12/24-23:29:40.993129    External RPC call    208.185.235.100:4065    MY.NET.94.75:111
12/24-23:30:55.515786    External RPC call    208.185.235.100:4213    MY.NET.100.130:111
12/29-19:44:58.915910    External RPC call    63.11.25.117:1661       MY.NET.6.15:111
12/29-19:44:59.267296    External RPC call    63.11.25.117:1661       MY.NET.6.15:111
12/29-19:44:59.283486    External RPC call    63.11.25.117:1661       MY.NET.6.15:111
12/29-19:44:59.574997    External RPC call    63.11.25.117:2          MY.NET.6.15:111
12/29-19:44:59.672590    External RPC call    63.11.25.117:5          MY.NET.6.15:111
12/29-19:44:59.914419    External RPC call    63.11.25.117:4          MY.NET.6.15:111
12/29-19:45:05.937334    External RPC call    63.11.25.117:1009       MY.NET.6.15:111
12/30-14:26:56.780877    External RPC call    130.212.20.72:3810      MY.NET.6.15:111
12/30-14:26:56.917902    External RPC call    130.212.20.72:969       MY.NET.6.15:111
12/30-14:26:57.014288    External RPC call    130.212.20.72:969       MY.NET.6.15:111
12/30-14:26:57.014350    External RPC call    130.212.20.72:969       MY.NET.6.15:111
12/30-14:28:00.689070    External RPC call    130.212.20.72:2254      MY.NET.15.127:111
01/01-11:00:03.077635    External RPC call    211.48.210.193:1251     MY.NET.15.127:111
01/02-15:00:55.007003    External RPC call    192.71.148.152:4847     MY.NET.15.127:111
01/06-05:04:21.793408    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:21.829933    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:21.830004    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:21.888825    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:21.888876    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:21.919235    External RPC call    206.210.80.6:1414       MY.NET.6.15:111
01/06-05:04:45.761356    External RPC call    206.210.80.6:3832       MY.NET.15.127:111
01/06-05:08:19.304357    External RPC call    206.210.80.6:1751       MY.NET.100.130:111
01/18-20:12:23.068148    External RPC call    202.84.134.141:748      MY.NET.6.15:111
01/18-20:12:23.672941    External RPC call    202.84.134.141:748      MY.NET.6.15:111
01/18-20:12:46.806033    External RPC call    202.84.134.141:615      MY.NET.15.127:111
01/18-20:16:20.752084    External RPC call    202.84.134.141:718      MY.NET.100.130:111
```

Although all of these connections should be investigated at the destination hosts, of particular interest are the following sourced connections:

65.33.58.115
211.50.30.241
195.116.66.14
63.11.25.117
130.212.20.72
202.84.134.141

These activities involve abnormal source ports and probably represent crafted packets. These primarily indicate malicious intent.

1. Source of Trace: GIAC Enterprises.

2. Detect was generated by: SNORT

These tables were copied from Excel spreadsheets. They contain data that was imported from Snort logs. The columns (as labeled) represent: Date/Time, Snort signature, Source IP and Port, and Destination IP and Port.

3. Probability the source address was spoofed:

The connections are probably not spoofed. The difficulty of spoofing these connections in order to mask the true source would outweigh its practicality. Sniffing packets could do this and/or hijacking a session on a segment between both hosts, however in this situation, it would be much easier to use a normal connection with a compromised host.

4. Description of attack:

RPC calls may indicate a portmapper request for assigned ports for RPC services.

5. Attack mechanism:

This activity can be a reconnaissance effort and a precursor to attack. These requests are significant because they are a method of identifying services and associating listening ports with them. This information can be used to identify common Sun RPC vulnerabilities and followed with exploits on services such as Statd, Calendar Manger and Tooltalk.

Host Info:

Host name: w142.z208037228.nyc-ny.dsl.cnc.net
IP address: 208.37.228.142
Alias(es): None

Host name: ubr-33.58.115.unionpark.cfl.rr.com
IP address: 65.33.58.115
Alias(es): None

No DNS Record
Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-BLK)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC-CIDR-BLK2
Netblock: 210.0.0.0 - 211.255.255.255

No DNS Record
Asia Pacific Network Information Center (NETBLK-APNIC2)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,

```
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC3
Netblock: 61.0.0.0 - 61.255.255.255
Maintainer: AP

No DNS Record
European Regional Internet Registry/RIPE NCC (NETBLK-RIPE-C)
These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-CBLK3
Netblock: 195.0.0.0 - 195.255.255.255
Maintainer: RIPE

Host name: CBL187.pool010.CH001-riverside.dhcp.hs.earthlink.net
IP address: 209.178.23.187
Alias(es): None

No DNS Record
NIC-Mexico (NETBLK-REDMEX-BNETS)REDMEX-BNETS
                  148.203.0.0 - 148.250.255.255
Benemerita Universidad Autonoma de Puebla (NET-NET-UAP)
         NET-UAP 148.228.0.0 - 148.228.255.255

No DNS Record
European Regional Internet Registry/RIPE NCC (NETBLK-RIPE-C)
These addresses have been further assigned to European users.
Contact info can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html
NL
Netname: RIPE-CBLK3
Netblock: 195.0.0.0 - 195.255.255.255
Maintainer: RIPE

Host name: sdsl-208-185-235-100.dsl.sjc.megapath.net
IP address: 208.185.235.100
Alias(es): None

Host name: 1Cust117.tnt1.yakima.wa.da.uu.net
IP address: 63.11.25.117
Alias(es): None
```

```
Host name: rsensing2.sfsu.edu
IP address: 130.212.20.72
Alias(es): None

No DNS Record
Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-
BLK)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC-CIDR-BLK2
Netblock: 210.0.0.0 - 211.255.255.255

Host name: birx22ms1.teliamobile.net
IP address: 192.71.148.152
Alias(es): None

No DNS Records
Stargate Industries, LLC (NET-SII-CIDR-206-210-64)
40 24th St, Suite 300
Pittsburgh, PA 15222
US
Netname: SII-CIDR-206-210-64
Netblock: 206.210.64.0 - 206.210.95.255
Maintainer: SII

No DNS Record
Asia Pacific Network Information Center (APNIC2)
These addresses have been further assigned to Asia-Pacific users.
Contact info can be found in the APNIC database,
at WHOIS.APNIC.NET or http://www.apnic.net/
Please do not send spam complaints to APNIC.
AU
Netname: APNIC-CIDR-BLK
Netblock: 202.0.0.0 - 203.255.255.255
Maintainer: AP
```

6. Correlations:
The trouble with RPCs - Stephen Northcutt
http://www.sans.org/y2k/trouble_RPCs.htm

CVE-1999-0493

rpc.statd allows remote attackers to forward RPC calls to the local operating system via the SM_MON and SM_NOTIFY commands, which in turn could be used to remotely exploit other bugs such as in automountd.

Reference: CERT:CA-99-05
Reference: SUN:00186
Reference: CIAC:J-045
Reference: BUGTRAQ:19990103 SUN almost has a clue! (automountd)
Reference: BID:450

CVE-1999-0019
Delete or create a file via rpc.statd, due to invalid information.

Reference: CERT:CA-96.09.rpc.statd
Reference: XF:rpc-stat
Reference: SUN:00135

CVE-1999-0018
Buffer overflow in statd allows root privileges.

Reference: CERT:CA-97.26.statd
Reference: AUSCERT:AA-97.29
Reference: XF:statd
Reference: BID:127

CVE-1999-0003
Execute commands as root via buffer overflow in Tooltalk database server (rpc.ttdbserverd)

Reference: NAI:NAI-29
Reference: CERT:CA-98.11.tooltalk
Reference: SGI:19981101-01-A
Reference: SGI:19981101-01-PX
Reference: XF:aix-ttdbserver
Reference: XF:tooltalk
Reference: BID:122

CVE-1999-0696
Buffer overflow in CDE Calendar Manager Service Daemon (rpc.cmsd)

Reference: BUGTRAQ:19990709 Exploit of rpc.cmsd
Reference: SCO:SB-99.12
Reference: SUN:00188
Reference: SUNBUG:4230754
Reference: HP:HPSBUX9908-102
Reference: COMPAQ:SSRT0614U_RPC_CMSD

Reference: CERT:CA-99-08
Reference: CIAC:J-051
Reference: XF:sun-cmsd-bo

CVE-1999-0189
Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111.

Reference: NAI:NAI-15
Reference: SUN:00142
Reference: XF:rpc-32771

CVE-1999-0190
Solaris rpcbind can be exploited to overwrite arbitrary files and gain root access.

Reference: SUN:00167
Reference: XF:sun-rpcbind

CVE-1999-0208
rpc.ypupdated (NIS) allows remote users to execute arbitrary commands.

Reference: XF:rpc-update
Reference: CERT:CA-95.17.rpc.ypupdated.vul

CVE-1999-0211
Extra long export lists over 256 characters in some mount daemons allows NFS directories to be mounted by anyone.

Reference: CERT:CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability

7. Evidence of active targeting:

At least part of these logs appears to be a scanning attempt and do not indicate active targeting; however, there are other parts that do seem to be consistent calls to MY.NET.6.15. This may be an indication that this host has been identified and targeted.

8. Severity:
Severity = (criticality + lethality) – countermeasures (system + net)

N/A. Calculation of severity is impossible without a complete assessment of the GIAC Enterprise network structure and a complete list of its hosts and functions.

9. Defensive recommendation:

Defensive recommendations are to make a determination if RPC services are needed. Any host without this requirement should have these services disabled. This includes port 111. Hosts that do require Sun RPC should have the latest vendor patches installed. An addition recommendation would be to block incoming requests to port 111 at the gateway router or firewall.