Rhonda Maluia, NAVCIRT
GAIC Practical

NETWORK DETECTS

ANALYSIS #1 FTP and TELNET Probes

```
03:06:32.872813 24.218.49.75.4334 > XYZ.XYZ.X.X.21: S
1173394192:1173394192(0) win 16384  (DF)
03:06:35.838067 24.218.49.75.4334 > XYZ.XY.X.X.21: S
1173394192:1173394192(0) win 16384  (DF)
03:06:41.846599 24.218.49.75.4334 > XYZ.XYZ.X.X.21: S
1173394192:1173394192(0) win 16384  (DF)
03:07:23.047467 24.218.49.75.6446 > XYZ.XYZ.X.X.23: S
3758660690:3758660690(0) win 16384  (DF)
03:07:23.047997 XYZ.XYZ.X.X.23 > 24.218.49.75.6446: R 0:0(0) ack
3758660691 win 0 (DF)
03:07:23.506035 24.218.49.75.5386 > XYZ.XYZ.X.X.23: S
2149841368:2149841368(0) win 16384  (DF)
03:07:23.506564 XYZ.XYZ.X.X.23 > 24.218.49.75.5386: R 0:0(0) ack
2149841369 win 0 (DF)
03:07:24.007036 24.218.49.75.4796 > XYZ.XYZ.X.X.23: S
277906213:277906213(0) win 16384  (DF)
03:07:24.007562 XYZ.XYZ.X.X.23 > 24.218.49.75.4796: R 0:0(0) ack
277906214 win 0 (DF)
```

1. Source of trace: This is a shadow detection from a U.S. Navy command.
   Source IP address: 24.218.49.75 ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-6)

2. Detect was generated by: Shadow in TCP dump format.

```
      1               2         3           4          5  6    7                             8         9
0 3:06:32.872813 24.218.49.75.4334 > XYZ.XYZ.X.X.21: S 1173394192:1173394192(0) win 16384  (DF)
```

1. Timestamp
2. Source IP
3. Source port
4. Destination IP
5. Destination port
6. Flag
7. Sequence Number:Attack number
8. TCP Window size
9. Do not fragment

3. Probability this address was spoofed: Due to the nature of the probes, it would be of no benefit for the source to conduct the activity and spoof the address if the results were not able to be utilized. This activity is probably probing for services and is not spoofed.

4. Description of attack: The attack is against ports 21 (FTP) and Telnet (23). These are both login services . These probes are attempts to establish active sessions with the destination IP, search for remote logins to systems (telnet), or to possibly see if anonymous FTP services are available, that are denied. No activity is observed to port 20, therefore no data is passed. The destination sent a RESET ACK disallowing a connection. Therefore, attempts to connect were denied. The sequence numbers do not change during the FTP portion of the attack, under normal conditions, the TCP sequence number changes whenever a host sends a packet to a new system. The source IP retries to establish the connection without success.

5. Attack Mechanism: The source IP utilizes an ephemeral port, greater than 1023, in an attempt to establish an FTP session. FTP is the standard protocol for file transfer between systems. It supports simple password authentication which can be bypassed or scripted out using a standard FTP configuration file. A SYN is sent to the target IP three times, but no response is observed from the destination IP address. The source IP then attempts to establish a telnet connection to the same destination IP address utilizing another ephemeral port. Telnet is the standard remote login protocol and application which provides a character based connection between two systems. Throughout the attempt to connect to telnet, the source IP address changes ephemeral port (not unusual). During this session the destination IP address sends RESET ACK's (this is an anomaly)to the source IP address denying the request for a telnet connection. No three-way handshake is established therefore no connection is established.

6. Correlations: This detect is not correlated to any other activity. A query of the JCD database indicates that the source IP was not previously involved in any unauthorized activity against navy networks. However, previous activity is noted from other IP addresses belonging to ServiceCo LLC-Road Runner.
Numerous known vulnerabilities can be associated with both TELNET and FTP.
CVE-1999-0017 FTP servers can allow a hacker to connect to arbitrary ports on machines other than the FTP client, aka FTP bounce.
CVE-199-0230 Buffer overflow in Cisco 7xx router through TELNET
CVE-1999-0073 TELNET allows a remote client to specify environment variables including LD_Library_Path allowing a hacker to bypass the normal systems libraries and gain root access.

7. Evidence of active targeting: The attempt to establish both an FTP and Telnet session with the destination IP targeted only 1 IP address. This provides evidence of active targeting. Because the source IP address was persistent and attempted to utilize two different services, it <u>is not likely that is the case of a wrong number</u>, moreover it is a deliberate attempt to establish a connection or gather information about the network services and operating system.

8. Severity: *Severity* = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) *(5+2)-(5+5)=7-10=-3*

9. Defensive recommendations: Attack was blocked by router or firewall policy. The current defenses provided adequate protection against the attack. Login services should be restricted to machines on the internal network. If this is not a practical consideration for the network, care should be given to the strict authentication of passwords (no clear text that can be easily intercepted).

10. Multiple Choice test question:

Which of the following can be utilized for remote login
A. NetBIOS
B. Telnet
C. DNS
D. ICMP

Answer: B

Analysis #2 Probing for proxies, Ring 0

```
05:17:19.076529 203.96.159.167.2046 > XYZ.XYZ.XYZ.XYZ.8080: S
983232:983232(0) win 8192  (DF)
05:17:22.277045 203.96.159.167.2046 > XYZ.XYZ.XYZ.XYZ.8080: S
983232:983232(0) win 8192  (DF)
05:17:28.687616 203.96.159.167.2046 > XYZ.XYZ.XYZ.XYZ.8080: S
983232:983232(0) win 8192  (DF)
05:17:41.766061 203.96.159.167.2046 > XYZ.XYZ.XYZ.XYZ.8080: S
983232:983232(0) win 8192  (DF)
05:18:07.761743 203.96.159.167.2097 > XYZ.XYZ.XYZ.XYZ.3128: S
1031964:1031964(0) win 8192  (DF)
05:18:11.003334 203.96.159.167.2097 > XYZ.XYZ.XYZ.XYZ.3128: S
1031964:1031964(0) win 8192  (DF)
05:18:17.431682 203.96.159.167.2097 > XYZ.XYZ.XYZ.XYZ.3128: S
1031964:1031964(0) win 8192  (DF)
05:18:30.451435 203.96.159.167.2097 > XYZ.XYZ.XYZ.XYZ.3128: S
1031964:1031964(0) win 8192  (DF)
```

1. Source of trace: This is a shadow detection from a U.S. Navy command
   Source IP address: Paradise Net Ltd, Wellington, NZ.

2. Detect was generated by: Shadow

```
      1               2      3           4        5 6            7                8          9
03:06:32.872813 24.218.49.75.4334 > XYZ.XYZ.X.X.21: S 1173394192:1173394192(0) win 16384  (DF)
```

1. Timestamp
2. Source IP
3. Source port
4. Destination IP
5. Destination port

6. Flag
7. Sequence Number:Attack number
8. TCP Window size
9. Do not fragment

3. Probability this address was spoofed: Since this is a probe for proxy servers the source IP address will want the information and the likelihood of the source being spoofed is low. Tracerouting back to the source IP address, checking the hop count and checking the TTL values would provide information on the legitimacy of the source IP address.

4. Description of attack: The attack is against ports 8080(alt HTTP) and 3128 (squid proxy), which is indicative of the Ring 0 Trojan or a scan for squid proxies. This type of Trojan hides and runs hidden processes on the victim. There are 3 versions of this Trojan. From this attack, the version of the attempted Trojan can not be determined, if this is in fact a Trojan scan.

The SYN was not acknowledged by the destination IP address indicating that the command does not allow activity to this port or the host is unreachable. The source IP address is perhaps searching for proxy servers rather than attempting to install a Trojan. Due to the non-changing sequence numbers, the detect shows evidence a retry on the part of the source address however, this is also indicative of a scan as the ports do not increment.

5. Attack Mechanism: The source attempts to search for proxy servers. Port 3128 is the default port for squid proxy. It is likely that one scanning this port is searching for proxies to conseal themselves while traveling the Internet. If a trojan scan and the Trojan was successfully installed, the Trojan would utilize ITS.EXE to retrieve files from web servers and use PST.EXE as an active scanner . The combination of the two, who work independently of one another, discovers proxies and sends IP addresses to a selected server. However, if this is not an attempt to utilize a Trojan, this type of activity is an unsuccessful probe for proxy servers as no acknowledgement from the destination address is noted.

6. Correlations: Much activity has been seen to ports 80, 8080, and 3128. Though this Trojan was discovered approximately 1 year ago, activity of this nature and probes to these ports continue as is evident by the date/time of the above detect.
http://www.symantec.com/avcenter/venc/data/ringzero.trojan.html
http://www.techweb.com/wire/story/TWB19991013S0018.

7. Evidence of active targeting: The source is targeting the same system throughout the scan. There is only one source IP address and this is not evidence of active targeting, mearly probing.

. Severity: *Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)* *(2+4) –(5+5)=-4*

9. Defensive recommendations: Attack was blocked by router or firewall policy. There were no acknowledgements to the probes by the destination IP address. Blocking services on ports 8080 and 3128 (if the site does not use proxy servers) and restricting services to the sites use only(if the site does use proxy servers) is a strong recommendation. Watch outgoing traffic from ports 8080 and 3128. If this activity is

observed, on a network that does not use proxy servers, it is an indication that the system perhaps has been infected by the RingZero.

10. Multiple Choice test question:

Probes to port 80, 8080, and 3128 are indicative of what type of activity?

A. Network Mapping Attempt
B. Sub 7 Trojan
C. Portmapper probe
D. Ring 0 Trojan

Answer: D

Detect #3 Probe to unassigned ports (please excuse profanity)

This log is from Sep 30, 2000

```
Sat Sep 30 03:18:39 2000  Alert indicated in rule. Source 216.149.211.49:9532, Destination
XXX.XX.XX.72:21962, protocol:6(tcp).
Sat Sep 30 03:19:53 2000  Alert indicated in rule. Source 216.149.211.49:54874, Destination
XXX.XX.XX.85:48654, protocol:6(tcp).
```

216.149.211.49 Net 9Avenue, Inc.

```
03:11:37.377391 will.fuck.for.an.o-line.st.62696 > XXX.XXX.X2.78.54795: R 0:0(0) win 0 [tos 0x8]
03:12:34.007460 will.fuck.for.an.o-line.st.18928 > NET1.navy.mil.24078: R 0:0(0) win 0 [tos 0x8]
03:12:42.065258 will.fuck.for.an.o-line.st.10493 > XXX.XXX.X2.67.42600: R 0:0(0) win 0 [tos 0x8]
03:16:02.309865 will.fuck.for.an.o-line.st.11743 > XXX.XXX.5Y.49.20051: R 0:0(0) win 0 [tos 0x8]
03:16:42.466257 will.fuck.for.an.o-line.st.43256 > XXX.XXX.6Y.77.49687: R 0:0(0) win 0 [tos 0x8]
```

This log is from 29 Sep 2000

```
22:50:05.957408 will.fuck.for.an.o-line.st.15197 > NET2.NAVY.MIL.23152: R 0:0(0) win 0 [tos 0x8]
22:50:44.869236 will.fuck.for.an.o-line.st.50177 > XXX.XXX.Z2.1.2725: R 0:0(0) win 0 [tos 0x8]
22:51:41.581387 will.fuck.for.an.o-line.st.43388 > YYY.YY.YYY.76.39514: R 0:0(0) win 0 [tos 0x8]
22:53:50.377317 will.fuck.for.an.o-line.st.27736 > NET3.NAVY.MIL.18276: R 0:0(0) win 0 [tos 0x8]
22:55:45.983848 will.fuck.for.an.o-line.st.54437 > NET4.NAVY.MIL.10995: R 0:0(0) win 0 [tos 0x8]
22:57:05.043472 will.fuck.for.an.o-line.st.52830 > XXX.XXX.X7.1.45609: R 0:0(0) win 0 [tos 0x8]
```

The above resolves to 216.149.211.49 Net 9Avenue, Inc.

This log is from 25 Sep 2000

```
15:57:03.263401 talk.shit.and.your.box.will.get.rooted.co.za.132 > XXX.XXX.X7.52.60539: R 0:0(0) ack
1 win 0
16:04:59.338355 talk.shit.and.your.box.will.get.rooted.co.za.nameserver > XXX.XXX.4X.82.57858: R
0:0(0) ack 1 win 0
16:08:18.777404 talk.shit.and.your.box.will.get.rooted.co.za.54 > XXX.XXX.5X.12.38420: R 0:0(0) ack 1
win 0
16:11:35.317055 talk.shit.and.your.box.will.get.rooted.co.za.8 > NET5.NAVY.MIL.33461: R 0:0(0) ack 1
win 0
16:13:19.456531 talk.shit.and.your.box.will.get.rooted.co.za.84 > XXX.XXX.4X.71.33839: R 0:0(0) ack 1
win 0
```

```
16:27:16.780245 talk.shit.and.your.box.will.get.rooted.co.za.5 > XXX.XXX.X7.4.6953: R 0:0(0) ack 1 win
0
16:30:08.867497 talk.shit.and.your.box.will.get.rooted.co.za.rtelnet > NET6.NAVY.MIL.23332: R 0:0(0)
ack 1 win 0
16:31:53.121011 talk.shit.and.your.box.will.get.rooted.co.za.whois > XXX.XXX.4X.104.23710: R 0:0(0)
ack 1 win 0
```

The above resolves to **216.111.123.195** 3DFX INTERACTIVE FAIRFIELD, CA (Leased from Qwest)

This log is from 27 Aug 2000

```
01:08:20.094607 talked.too.much.shit.and.got.rooted.co.za.27612 > NET7.NAVY.MIL.58256: R 0:0(0)
ack 1508430659 win 0 [tos 0x8]
01:08:25.396175 talked.too.much.shit.and.got.rooted.co.za.49248 > XXX.XXX.3X.84.51180: R 0:0(0) ack
1027921731 win 0 [tos 0x8]
01:08:51.308277 talked.too.much.shit.and.got.rooted.co.za.7712 > XXX.XXX.5X.68.17769: R 0:0(0) ack
3149981763 win 0 [tos 0x8]
01:09:18.406665 talked.too.much.shit.and.got.rooted.co.za.19255 > ZZZ.ZZZ.Z67.4.49288: R 0:0(0) ack
920713795 win 0 [tos 0x8]
01:15:22.167656 talked.too.much.shit.and.got.rooted.co.za.49871 > XXX.XXX.5X.3.30646: R 0:0(0) ack
3977111620 win 0 [tos 0x8]
01:15:29.051824 talked.too.much.shit.and.got.rooted.co.za.47159 > NET8.NAVY.MIL.64278: R 0:0(0)
ack 1903094852 win 0 [tos 0x8]
```

The above resolves to **216.149.211.50** Net 9Avenue, Inc.

1. Source of trace: This is a shadow detection from a U.S. Navy command..
   Source IP addresses 216.149.211.50 and 216.149.211.50 resolve to 9 Net Avenue, Inc. Secaucus, NJ US, however co.za resolves to: The Internet Solution (Pty) Ltd , Parklands, South Africa. 216.111.123.195 resolves to 3DFX INTERACTIVE FAIRFIELD, CA (Leased from Qwest)

```
       1                                   2                   3                4           5     6     7
01:08:20.094607 talked.too.much.shit.and.got.rooted.co.za.27612 > NET7.NAVY.MIL.58256: R 0:0(0)
8         9          10      11
ack 1508430659 win 0 [tos 0x8]
```

1. Time
2. Source address
3. Source Port
4. Destination address
5. Destination port
6. RESET Flag
7. Data
8. ACK Flag
9. Sequence number
10. Window size
11. Type of service: maximize throughput

2. Detect was generated by: Shadow

3. Probability this address was spoofed: This address is probably not spoofed. Tracerts to each IP address revealed that the IP addresses are from the same source or a person associated with both domain names. A correlation is also made by the nature of the domain names though this may not be reliable..
4. Description of attack: This is a reset probe sent to various IP addresses utilizing unassigned ports. This probe is "loud" and may be utilized to distract the analyst and bring attention to itself as a decoy for other activity. The person has attempted this type of activity numerous times (14 separate incidents of this nature in our database), always utilizing high number ports and RESET ACK packets that are crafted. There is no pattern to the probing and the IP addresses and ports do not repeat. The person may be probing to see what boxes are alive which will return a host unreachable. This is perhaps a scripted attack utilizing crafted packets.
5. Attack Mechanism: The attack mechanism seems to be inverse mapping and a random scanning of ports. The type of service is maximize throughput . The RESET ACK (crafted) may be utilized to see if a router will answer up and tell if the selected boxes are alive. From this information an attacker can may an attack on networks (s) more effectively.
6. Correlations: I was able to query our database and found previous activity (14 incidents) from what is most likely the same person/s. Interestingly enough rooted.co.za correlated to The Internet Solution (Pty)Ltd, South Africa and the country code for ST resolved to an island off the coast of Africa. However when DNS lookups are performed the IP address resolves to Net9Avenue, Inc USA. Net9 Avenue allows one to register a domain name. The third IP address resolves to 3DFX INTERACTIVE which is leases a block from Qwest. While the ISP is different for the "rooted" addresses because of the nature of the phrase, the two addresses should be further investigated for correlation to the same person or persons. Please see traceroutes for further correlation.
CAN-1999-0586 (under review) Description: A network service is running on a nonstandard port.
7. Evidence of active targeting: There is evidence of active reconnaissance. The different source IP addresses target the same navy.mil domains utilizing 2 and possibly 3 separate IP addresses.

```
Tracing route to talk.shit.and.your.box.will.get.rooted.co.za [216.111.123.195]
over a maximum of 216 hops:

  1   110 ms   100 ms   100 ms  154-042.sybercom.net [209.96.154.42]
  2   100 ms   120 ms     *     nn-t1-gw.vabch.com [209.96.154.1]
  3   100 ms   111 ms   110 ms  eth32.core1.Norfolk.visi.net [206.246.204.5]
  4   100 ms   121 ms   110 ms  hssi31.core1.Richmond.visi.net [206.246.247.137]
  5   110 ms   121 ms   110 ms  hssi31.core1.WashDC.visi.net [209.96.135.53]
  6   100 ms   111 ms   120 ms  fe7-4.core2.wdc.cais.net [63.216.1.37]
  7   120 ms   111 ms   120 ms  pos2-1.core.ralgh.cais.net [63.216.141.57]
  8   120 ms   121 ms     *     pos1-0.core2.ralgh.cais.net [63.216.141.14]
  9   131 ms   140 ms   130 ms  pos2-2.core.atl.cais.net [63.216.31.57]
 10    141 ms   140 ms   130 ms  qwest.pos2-3.core1.atl.cais.net [63.216.31.69]
 11    140 ms   140 ms   140 ms  atl-core-03.inet.qwest.net [205.171.21.105]
 12   150 ms   130 ms   130 ms  wdc-core-03.inet.qwest.net [205.171.5.241]
 13   130 ms   130 ms   140 ms  wdc-core-01.inet.qwest.net [205.171.24.10]
 14   170 ms   170 ms   161 ms  chi-core-03.inet.qwest.net [205.171.5.227]
 15   160 ms   170 ms   171 ms  chi-edge-10.inet.qwest.net [205.171.20.134]
 16   170 ms   191 ms   180 ms  s0-0.col.brdr1.foonet.net [63.144.66.26]
 17   191 ms   190 ms   200 ms  f0-0.col.core1.foonet.net [216.207.29.66]
 18   180 ms   190 ms   180 ms  talk.shit.and.your.box.will.get.rooted.co.za
[216.111.123.195]

Trace complete.

Tracing route to talked.too.much.shit.and.got.rooted.co.za [216.149.211.50]
over a maximum of 30 hops:

  1   111 ms   110 ms   120 ms  154-042.sybercom.net [209.96.154.42]
  2   101 ms   110 ms   120 ms  nn-t1-gw.vabch.com [209.96.154.1]
  3   100 ms   111 ms   110 ms  eth32.core1.Norfolk.visi.net [206.246.204.5]
  4   111 ms   110 ms   120 ms  hssi31.core1.Richmond.visi.net [206.246.247.137]
  5   131 ms   120 ms   120 ms  hssi31.core1.WashDC.visi.net [209.96.135.53]
  6   121 ms   130 ms   120 ms  mae-east2.digex.net [192.41.177.192]
  7   121 ms   120 ms   120 ms  iad1-core4-pos3-0.atlas.icix.net [165.117.52.194]
  8   121 ms   120 ms   110 ms  dca6-core2-pos1-3.atlas.icix.net [165.117.63.5]
  9   120 ms   120 ms   120 ms  dca6-core1-pos6-0.atlas.icix.net [165.117.48.101]
 10   120 ms   120 ms   130 ms  dca6-core5-pos6-0.atlas.icix.net [165.117.48.106]
 11   120 ms   120 ms   120 ms  jfk3-core4-pos5-0.atlas.icix.net [165.117.48.34]
 12   120 ms   120 ms   130 ms  jfk3-core2-pos7-0.atlas.icix.net [165.117.48.165]
 13   120 ms   140 ms   140 ms  ewr1-core1-s4-1-0.atlas.icix.net [165.117.50.189]
 14   120 ms   130 ms   120 ms  209.118.52.198
 15   140 ms   121 ms   130 ms  Vlan9.rsm2.sc.nj.9netave.net [216.156.0.30]
 16   120 ms   141 ms   120 ms  talked.too.much.shit.and.got.rooted.co.za
[216.149.211.50]

Trace complete.

Tracing route to will.fuck.for.an.o-line.st [216.149.211.49]
over a maximum of 30 hops:

  1   110 ms   110 ms   100 ms  154-042.sybercom.net [209.96.154.42]
  2   100 ms   120 ms   120 ms  nn-t1-gw.vabch.com [209.96.154.1]
  3   100 ms   100 ms   110 ms  eth32.core1.Norfolk.visi.net [206.246.204.5]
  4   100 ms   130 ms   120 ms  hssi31.core1.Richmond.visi.net [206.246.247.137]
  5   110 ms   130 ms   110 ms  hssi31.core1.WashDC.visi.net [209.96.135.53]
  6   140 ms   120 ms   120 ms  mae-east2.digex.net [192.41.177.192]
  7   110 ms   140 ms   110 ms  iad1-core4-pos3-0.atlas.icix.net [165.117.52.194]
  8   120 ms   120 ms   130 ms  dca6-core2-pos1-3.atlas.icix.net [165.117.63.5]
  9   120 ms   120 ms   130 ms  dca6-core1-pos6-0.atlas.icix.net [165.117.48.101]
```

```
10   120 ms   130 ms   120 ms  dca6-core5-pos6-0.atlas.icix.net [165.117.48.106]
11   120 ms   140 ms   131 ms  jfk3-core4-pos5-0.atlas.icix.net [165.117.48.34]
12   120 ms   130 ms   121 ms  jfk3-core2-pos7-0.atlas.icix.net [165.117.48.165]
13   130 ms     *      130 ms  ewr1-core1-s4-1-0.atlas.icix.net [165.117.50.189]
14   120 ms   120 ms   120 ms  209.118.52.198
15   120 ms   131 ms   120 ms  Vlan9.rsm2.sc.nj.9netave.net [216.156.0.30]
16   131 ms   130 ms   130 ms  will.fuck.for.an.o-line.st [216.149.211.49]

Trace complete.
```

8. Severity: *Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)   (2+3) – (5+5)= -5*

9. Defensive recommendations: Attack was blocked by router or firewall policy. The current defenses provided adequate protection against the attack.

10. Multiple Choice test question:
If a router receives a probe to a non-existent host, it will issue the following message:
A. It will not issue a message at all
B. Host unreachable
C. Go away
D. Non-existent host domain

Answer: D

Detect #4 Network Mapping Attempt

```
> 06:54:39.922903 213-167-205-25.flat.galactica.it > XXX.YYY.X1.255: icmp: echo
request
> 06:54:39.925721 213-167-205-25.flat.galactica.it > XXX.YYY.X1.0: icmp: echo
request
> 06:54:39.935969 213-167-205-25.flat.galactica.it > XXX.YYY.X2.255: icmp: echo
request
> 06:54:39.938390 213-167-205-25.flat.galactica.it > XXX.YYY.X2.0: icmp: echo
request
> 06:54:39.949074 213-167-205-25.flat.galactica.it > XXX.YYY.X3.255: icmp: echo
request
> 06:54:39.950209 213-167-205-25.flat.galactica.it > XXX.YYY.X3.0: icmp: echo
request
> 06:54:39.958465 213-167-205-25.flat.galactica.it > XXX.YYY.X4.0: icmp: echo
request
> 06:54:39.969926 213-167-205-25.flat.galactica.it > XXX.YYY.X4.255: icmp: echo
request
> 06:54:39.977405 213-167-205-25.flat.galactica.it > XXX.YYY.X5.0: icmp: echo
request
> 06:54:39.978072 213-167-205-25.flat.galactica.it > XXX.YYY.X5.255: icmp: echo
request
> 06:54:39.988819 213-167-205-25.flat.galactica.it > XXX.YYY.X6.0: icmp: echo
request
```

```
> 06:54:39.989583 213-167-205-25.flat.galactica.it > XXX.YYY.X6.255: icmp: echo
request
```

1. Source of trace: This is a shadow detection from a Naval command.
   Source IP 213.167.205.25: Galactica Internet Service Provider Milano, IT.
2. Detect was generated by: Shadow

3. Probability this address was spoofed: The source IP address is probably not spoofed as this is a network mapping attempt. This in an intelligence gathering phase. The information gained from the echo request could provide information necessary to form a more efficient attack at a later date that may not necessarily come from the source IP observed above.

4. Description of attack: Broadcast ICMP is the most common type of mapping technique. The source IP address actually mapped the entire XXX.YYY.XX network. This is an excerpt from the entire attack. This is an example of an "Efficient Mapper" (SANs Intrusion Analysis Book I pg 6-14). This attack follows an increasing numeric sequence and is the result of a type of automated scan. The scan focuses on the final octet utilizing the network and broadcast addresses. The 0 in the final octet may illicit a response from the UNIX BSD operating system and Windows operating systems may respond to the .255 address.. It is hoped that any live hosts on the subnet will respond to the broadcast address. This can be used to narrow an attack to only live hosts on a network.

5. Attack Mechanism: ICMP echo requests (ping) packets addresses to an IP broadcast address can generate a large number of responses when each host on the subnet replies. The large number of responses can consume network bandwidth and prevent legitimate traffic from being transmitted. This type of activity is commonly used by a third party , where the attacker forges the targets address in a smurf attack against a different target. ICMP is the control messages for TCP/IP. There are no ports associated with ICMP. ICMP may be used for network mapping, Denial of Service, or to redirect traffic. ICMP is not capable of being utilized to crack a system, however, the information gathered from this activity can be used to make attacks more efficient. While network mapping attempts do not require analytical expertice and are easily identified, they should not be overlooked. If one were to trace back a serious attempt or successful crack a network mapping attempt (as well as traceroutes) are normally seen early on.
6. Correlations: A query of our database indicates that previous network mapping has been observed from the Italian ISP.

CVE-1999-0513-ICMP broadcast addresses are allowed, allowing for smurf attacks that could cause a denial of service.

http://www.infowar.com/hacker/hack_072397a.html-ssi "ICMP ECHO_REQUESTS to BROADCAST addresses."

7. Evidence of active targeting: There is no evidence of active targeting, this is mearly an intelligence gathering phase on a class B network.
8. Severity: *Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) (1+1) – (5+5)=2-10=-8*

9. Defensive recommendations: Reconfigure your perimeter router or firewall to disallow ICMP echo requests onto the broadcast address and internal network. This will prevent someone from using the network to mount a SMURF attack against another target. Also, disallow ICMP echo replies entering your network, this will prevent SMURF attacks from targeting the network. http://www.securityfocus.com/frames/?content=/templates/archive.pike%3Flist%3D1%26msg%3Dg6yb6w8f2u.fsf%40daedalus.crosslink.net "Re: ICMP ECHO_REQUEST on BROADCAST--HOWTO Filter!"

10. Multiple Choice test question:

ICMP echo requests to the .255 and .0 addresses are indicative of which of the following?
A. Remote login attempt
B. A hack in progress
C. Network mapping
D. Traceroute
Answer: C

EVALUATE AN ATTACK

1. Give the URL, location, or command that you acquired the attack from: U.S. Navy command (sanitized).
2. Description of attack The scan is the result of a scripted attack. Note the times of the attacks, there is a fraction of a second between the events. The first part of the scan started with a traceroute from the aggressor to the victim. The second phase of the attack was to perform an NMAP on the system to determine open ports and services. The last phase of the attack, and the focus of this evaluation, concentrated on one of the ports found to be open (FINGER). During this attack there is no user logged on and no information is given from the victim.

Description of the FINGER protocol: The finger protocol (port 79), based on TCP, returns information on one or more users on a specified host. It is used to determine who is currently logged on, logon names, when the person logged on, the last time mail was checked and who it was from, and even has the ability to track conversations. It provides detailed information about the user that may be considered personal. .

How the FINGER protocol operates: A TCP connection is opened by the local host to a remote host on port 79. A Remote User Information Program (RUIP) is made available on the remote side of the connection to process. The local host sends the RUIP a one line query based upon the Finger query specification, and waits for the RUIP to respond. The RUIP receives and processes the query, returns an answer, then initiates the close of the connection. The local host receives the answer and the close signal, then proceeds closing its end of the connection. Finger is similar to FTP, Telnet and SMTP, Finger is

one of the protocols at the security perimeter of a host."
Correlations:
RFC 1288
CVE-1999-0612 A version of finger is running that exposes valid user information to any entity on the network.

SCRIPT

```
Script done on Thu Oct 12 16:51:19 2000
Script started on Thu Oct 12 16:53:12 2000
> /usr/w     [Kshow     [K     [K     [Kbin/showmount -e 204.37.1.     [K1.4

mount clntudp_create: RPC: Program not registered
> namp     [K     [K     [Kmap -v 204.37.11.11□ □[K     [K4

Starting nmap V. 2.3BETA6 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
No tcp,udp, or ICMP scantype specified, assuming vanilla tcp connect() scan. Use -sP if you really don't
want to portscan (and just want to see what hosts are up).
Host  (XXX.XX.XX.X) appears to be up ... good.
Initiating TCP connect() scan against  (XXX.XX.XX.X)
Adding TCP port 79 (state Open).
Adding TCP port 1024 (state Open).
Adding TCP port 513 (state Open).
Adding TCP port 111 (state Open).
Adding TCP port 98 (state Open).
Adding TCP port 514 (state Open).
Adding TCP port 25 (state Open).
Adding TCP port 23 (state Open).
Adding TCP port 21 (state Open).
Adding TCP port 80 (state Open).
Adding TCP port 113 (state Open).
Adding TCP port 985 (state Open).
Adding TCP port 515 (state Open).
The TCP connect scan took 1 seconds to scan 1489 ports.
Interesting ports on  (XXX.XX.XX.X):
Port    State       Protocol  Service
21      open        tcp       ftp
23      open        tcp       telnet
25      open        tcp       smtp
79      open        tcp       finger
80      open        tcp       http
98      open        tcp       linuxconf
111     open        tcp       sunrpc
113     open        tcp       auth
513     open        tcp       login
514     open        tcp       shell
515     open        tcp       printer
985     open        tcp       unknown
1024    open        tcp       unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
> finger @XXX.XX.XX.X

[XXX.XX.XX.X]
```

```
> finger@     [K     [K     [Ker
redteam     [K     [K     [K     [K     [K     [K     [KXXXXXX@30□ □[K     [K204.37.11.4

[XXX.XX.XX.X]

> ls

00-119-reports.tar  Desktop  alex.txt                           mail  small_scans
00-121-reports.tar  Mail     kvncviewer-0.0.3.tar.gz  mbox
> rm *.tar

> tol     [Koltalk

tooltalk: Command not found.
> q     [Kquit     [K     [K     [K     [K     ls

Desktop  Mail  alex.txt  kvncviewer-0.0.3.tar.gz  mail mbox  small_scans
> exit


Script done on Thu Oct 12 16:59:16 2000
```

NMAP scan retrieved from WWW.insecure.org/NMAP

NMAP EXCERPT

```
16:42:32.410827 <aggressor.navy.mil.4082 > victim.navy.mil.finger: S
906050238:906050238(0) win 32120 <mss 1460,sackOK,timestamp 19162875
0,nop,wscale 0> (DF)
```

First packet of the three way handshake

```
16:42:32.410939 > victim.navy.mil.finger > aggressor.navy.mil.4082: S
143972985:143972985(0) ack 906050239 win 32120 <mss 1460,sackOK,timestamp
1227938 19162875,nop,wscale 0> (DF)
```

Second part of three way handshake

```
16:42:32.411406 < aggressor.navy.mil.4082 > victim.navy.mil.finger: . 1:1(0) ack 1 win
32120 <nop,nop,timestamp 19162875 1227938> (DF)
```

Three way handshake completed

```
16:42:32.411567 < aggressor.navy.mil.4082 > victim.navy.mil.finger: P 1:3(2) ack 1 win
32120 <nop,nop,timestamp 19162875 1227938> (DF)
```

Aggressor pushes data for finger relative ISN 1-3

```
16:42:32.411618 > victim.navy.mil.finger > aggressor.navy.mil.4082: . 1:1(0) ack 3 win
32120 <nop,nop,timestamp 1227938 19162875> (DF)
```

Victim acks receipt of data (ack 3)

```
16:42:37.431149 > victim.navy.mil.finger > aggressor.navy.mil.4082: R 1:1(0) ack 3 win
32120 <nop,nop,timestamp 1228440 19162875> (DF)
```

Victim resets connection

```
16:43:04.808818 < aggressor.navy.mil.4083 > victim.navy.mil.finger: S
948572409:948572409(0) win 32120 <mss 1460,sackOK,timestamp 19166115
0,nop,wscale 0> (DF)
```

Aggressor attempt to syn victim to establish another connection

```
16:43:04.808964 > victim.navy.mil.finger > aggressor.navy.mil.4083: S
167801952:167801952(0) ack 948572410 win 32120 <mss 1460,sackOK,timestamp
1231177 19166115,nop,wscale 0> (DF)
```

Victim acks syn, second part of handshake

```
16:43:04.809427 < aggressor.navy.mil.4083 > victim.navy.mil.finger: . 1:1(0) ack 1 win
32120 <nop,nop,timestamp 19166115 1231177> (DF)
```

Aggressor completes handshake

```
16:43:04.908849 < aggressor.navy.mil.4083 > victim.navy.mil.finger: P 1:8(7) ack 1 win
32120 <nop,nop,timestamp 19166125 1231177> (DF)
```

Aggressor pushes data to victim

```
16:43:04.908957 > victim.navy.mil.finger > aggressor.navy.mil.4083: . 1:1(0) ack 8 win
32120 <nop,nop,timestamp 1231187 19166125> (DF)
```

Victim acks data

```
16:43:04.909364 < aggressor.navy.mil.4083 > victim.navy.mil.finger: P 8:10(2) ack 1
win 32120 <nop,nop,timestamp 19166125 1231187> (DF)
```

Aggressor pushes more data

```
16:43:04.910813 > victim.navy.mil.finger > aggressor.navy.mil.4083: . 1:1(0) ack 10 win
32120 <nop,nop,timestamp 1231188 19166125> (DF)
```

Victim acks data

```
16:43:09.831224 > victim.navy.mil.finger > aggressor.navy.mil.4083: R 1:1(0) ack 10
win 32120 <nop,nop,timestamp 1231680 19166125> (DF)
```

Victim sends reset

TCPDUMP –FINGER (what the victim logs)

```
16:42:32.410827 < aggressor.navy.mil.4082 > victim.navy.mil.finger: S
906050238:906050238(0) win 32120 <mss 1460,sackOK,timestamp 19162875
0,nop,wscale 0> (DF)
16:42:32.410939 > aggressor.navy.mil.finger > victim.navy.mil.4082: S
143972985:143972985(0) ack 906050239 win 32120 <mss 1460,sackOK,timestamp
1227938 19162875,nop,wscale 0> (DF)
16:42:32.411406 < aggressor.navy.mil.4082 > victim.navy.mil.finger: . 1:1(0) ack 1 win
32120 <nop,nop,timestamp 19162875 1227938> (DF)
16:42:32.411567 < aggressor.navy.mil.4082 > victim.navy.mil.finger: P 1:3(2) ack 1 win
32120 <nop,nop,timestamp 19162875 1227938> (DF)
16:42:32.411618 > victim.navy.mil.finger > aggressor.navy.mil.4082: . 1:1(0) ack 3 win
32120 <nop,nop,timestamp 1227938 19162875> (DF)
16:42:37.431149 > aggressor.fiwc.navy.mil.finger > victim.navy.mil.4082: R 1:1(0) ack
3 win 32120 <nop,nop,timestamp 1228440 19162875> (DF)
16:43:04.808818 < aggressor.navy.mil.4083 > victim.navy.mil.finger: S
948572409:948572409(0) win 32120 <mss 1460,sackOK,timestamp 19166115
0,nop,wscale 0> (DF)
16:43:04.808964 > victim.navy.mil.finger > aggressor.navy.mil.4083: S
167801952:167801952(0) ack 948572410 win 32120 <mss 1460,sackOK,timestamp
1231177 19166115,nop,wscale 0> (DF)
```

```
16:43:04.809427 < aggressor.navy.mil.4083 > victim.navy.mil.finger: . 1:1(0) ack 1 win
32120 <nop,nop,timestamp 19166115 1231177> (DF)
16:43:04.908849 < aggressor.navy.mil.4083 > victim.navy.mil.finger: P 1:8(7) ack 1 win
32120 <nop,nop,timestamp 19166125 1231177> (DF)
16:43:04.908957 > aggressor.navy.mil.finger > victim.navy.mil.4083: . 1:1(0) ack 8 win
32120 <nop,nop,timestamp 1231187 19166125> (DF)
16:43:04.909364 < victim.navy.mil.4083 > aggressor.navy.mil.finger: P 8:10(2) ack 1
win 32120 <nop,nop,timestamp 19166125 1231187> (DF)
16:43:04.910813 > victim.navy.mil.finger > aggressor.navy.mil.4083: . 1:1(0) ack 10 win
32120 <nop,nop,timestamp 1231188 19166125> (DF)
16:43:09.831224 > victim.navy.mil.finger > aggressor.navy.mil.4083: R 1:1(0) ack 10
win 32120 <nop,nop,timestamp 1231680 19166125> (DF)
```

ANALYZE THIS

For this exercise a months worth of incomplete logs were provided. Analysts were asked to provide a bid to provide security services for MY.NET. Several problems have been encountered such as power outages and insufficient disk space. The following is an analysis of the incomplete logs in terms of compromised systems, network problems, and malicious activity against the network.

Synopsis: Major reconnaissance was conducted against the MY.NET network. NMAP scans, Finger probes, Scans for proxies, Null scans, Queso fingerprinting are to name a few. With logs missing and gaps in time is difficult to determine the exact extent of the probing. A distributed denial of service attack was also attempted against the network. Trojans and viruses were also observed. Access attempts utilizing key ports with vulnerabilities were observed throughout the scanning. After examining the logs, utilizing grep command to parse for relevant data, I came up with a list of addresses which warrant investigation. The following is a summary, by IP address of what activities were conducted against them.

MY.NET.1.3

```
07/19-09:49:16.702569  [**] Queso fingerprint [**] 212.171.169.46:24122 ->
MY.NET.1.3:21
Jul 29 13:06:49 208.50.27.150:21 -> MY.NET.1.3:21 SYNFIN **SF****
```

SYN-FIN is an unreasonable combination, this is of malicious intent.

```
07/14-13:48:58.394814  [**] spp_portscan: portscan status from MY.NET.1.3: 10
connections across 2 hosts: TCP(0), UDP(10) [**]
```

```
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41909 UDP
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41910 UDP
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41911 UDP
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41912 UDP
```

```
 Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41913 UDP
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41914 UDP
Aug  5 10:32:29 MY.NET.1.3:53 -> MY.NET.101.89:41916 UDP
```

MY.NET.1.3 scanned its own network

MY.NET 60.8

The above IP address sustained the following alarms:
1 instance of SYN-FIN
1 instance of Queso Fingerprint
25 instances of Wingate 8080 attempt
240 instance of 1080 attempt

The above IP was the source of the following:
8/5/00 1847:13-1856:11 TELNET login incorrect from 255.254.60.8 to 207.172.151.22 ports 1674, 1026, and 1197.

MY.NET.253.114

```
07/28-23:32:11.772069  [**] WinGate 1080 Attempt [**] 216.127.150.136:1856 ->
MY.NET.253.114:1080
07/28-23:32:23.368753  [**] Null scan! [**] 216.127.150.136:57878 -> MY.NET.253.114:22
07/28-23:32:23.408944  [**] NMAP TCP ping! [**] 216.127.150.136:57882 ->
MY.NET.253.114:1
08/05-13:37:20.335822  [**] SUNRPC highport access! [**] 209.138.185.157:4067 ->
MY.NET.253.114:32771
08/05-13:37:20.337188  [**] SUNRPC highport access! [**] 209.138.185.157:4067 ->
MY.NET.253.114:32771
```

MY.NET.1.8

This IP address sustained the following:

2 instances of attempted Sun RPC high port access
6 instances of Tiny fragments-possible hostile activity
34 incidents of NMAP TCP Pings

Chronology of events:
6/27/00 0739:28-0736:33 two sets of NMAP TCP ping scans from 209.218.228.46 to 255.254.1.8 ports 80 and 53 utilizing source ports of 80 and 53.

```
06/27-07:39:33.390475  [**] NMAP TCP ping! [**] 209.218.228.46:80 -> MY.NET.1.8:53
06/27-07:39:33.390629  [**] NMAP TCP ping! [**] 209.218.228.46:53 -> MY.NET.1.8:53
```

6/28/00 0635:13 4 tiny fragment alarms from 63.236.34.174

6/30/00 0534:58 NMAP TCP ping alarms from 209.218.46 to 255.254.1.8 utilizing ports 80 and 53 as both source and destination ports.
6/30/00 0641:26 NMAP TCP ping alarms from 209.218.228.201 to 255.254.1.8 utilizing source/dest ports 80 and 53.

07/08-07:21:32.145547 [**] Attempted Sun RPC high port access [**] 64.27.29.2:2385 -> MY.NET.1.8:32771 ***
07/08-07:33:06.203162 [**] Attempted Sun RPC high port access [**] 207.230.26.34:1295 -> MY.NET.1.8:32771 ***
07/08-20:02:37.444826 [**] NMAP TCP ping! [**] 209.218.228.46:80 -> MY.NET.1.8:53 *** note the high port!

7/11/00 1012:48 NMAP from 195.54.105.6 to and from port 53

7/27/00 0254:39 NMAP from 209.218.228.46

8/4/00 0548:01 attempted Sun RPC high port access from 203.197.88.130

```
8/4/00  1049:00  NMAP Ping from 205.128.11.157 ports 80 and 53
        1118:28   from 205.128.11.157
        1243:24   from 205.128.11.157
8/5/00   0619  NMAP ping from 209.218.228.46
         0814  NMAP ping from  205.128.11.157
         1321  NMAP ping from  205.128.11.157
         2147  NMAP ping from  205.128.11.157
         2148  NMAP ping from  205.128.11.157
         2325  NMAP ping from  205.128.11.157
```

MY.NET.99.51

06/27-13:20:12.138930 Wingate Attempt from 255.254.51.20 to 255.254.101.155
06/29-04:40:46.546586 [**] WinGate 1080 Attempt [**] 207.114.4.46:3816 -> MY.NET.99.51:1080
06/30-05:54:34.091505 [**] WinGate 1080 Attempt [**] 207.114.4.46:4360 -> MY.NET.99.51:1080
07/26-02:46:25.820700 [**] WinGate 1080 Attempt [**] 207.114.4.46:3875 -> MY.NET.99.51:1080
07/28-05:44:51.442479 [**] WinGate 1080 Attempt [**] 207.114.4.46:1272 -> MY.NET.99.51:1080
08/05-19:03:45.522918 [**] IDS08 - TELNET - daemon-active [**] MY.NET.99.51:23-> 24.25.111.117:1029
53 total Wingate hits
*****Telnet daemon indicates successful telnet connection has been established from outside local network**
ABSnet Internet Services (NETBLK-ABSNET-BLK1)
200 East Lexington Street
Baltimore, MD 21202

USA

MY.NET.99.145

7/29/00 1624:35-:53   14 instances of SUNRPC high port access
Source: 205.188.3.205

```
07/29-16:24:35.903923  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:36.856924  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:37.660049  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:37.681154  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:37.886257  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:42.003947  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:43.950767  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:48.732229  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:50.394313  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:50.395577  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:51.127465  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:51.872439  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:51.879197  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
07/29-16:24:53.247324  [**] SUNRPC highport access! [**] 205.188.3.205:5190 ->
MY.NET.98.145:32771
```

Whois : 205.188.3.205
America Online, Inc (NETBLK-AOL-DTC)
22080 Pacific Blvd
Sterling, VA 20166

MY.NET.60.14

6/30/00 0826:02 NMAP ping from 195.25.86.2 to 255.254.60.14 on port 80
08/03/00 1959:23 Null scans from 149.225.111.69 port 7904 to 225.254.60.14 on ports 7, 22, 37, 137, 513.

Comprehensive list of signatures

Total number of alerts: 362,199 alerts processed

362199 alerts processed.			
Earliest alert at on /			
Latest alert at 23:54:28.705424 on 08/05			
Signature	# Alerts	# Sources	# Destinations
FTP-bad-login	1	1	1
IDS08 TELNET daemon-active	1	1	1
PING-ICMP Source Quench	1	1	1
Back Orifice	1	1	1
Poss wu-ftpd GIAC000623	2	1	2
Queso fingerprint	3	3	3
Happy 99 Virus	4	4	4
site exec Poss wu-ftpd expl.	5	3	4
IDS246 MISC Large ICMP Pkt	5	5	1
IDS127 TELNET Login Incorr	7	3	6
External RPC call	8	2	1
Tiny Frags Poss Hostile Act	9	3	3
Napster Client Data	12	8	7
SUNRPC highport access!	18	3	3
Null scan!	30	20	19
NMAP TCP ping!	45	6	5
Napster 7777 Data	170	14	13
GIAC 000218 VA-CIRT 35555	182	28	9
GIAC 000218 VA-CIRT 34555	196	25	9
SMB Name Wildcard	229	5	4
Napster 8888 Data	323	8	8
SNMP public access	1147	28	1
IDS247 MISC Large UDP Pack	1170	1	1
WinGate 1080 Attempt	2042	353	305
Attmpt Sun RPC hghprt acs	2241	10	8
WinGate 8080 Attempt	3222	89	16
Watchlist 000222 NET-NCFC	4711	40	12
PING-ICMP Time Exceeded	6689	299	117
PING-ICMP Dest Unreach	12313	133	144
Watchlist 000220 IL	13962	19	17
SYN-FIN scan!	19844	11	19801
	293606	1	1

Generated by Snortsnarf v100400.1 (Jim Hoagland and Stuart Staniford)

362,199 event records were discovered after running a PERL script on all of the SANS files (Procedure to be discussed in section 4).. I first started by asking who, what, when, where, and how.

The Who

: Analysts were provided with two watch lists which consisted of IP addresses from both China and Israel. A separate list was compiled displaying the most active source and destination addresses correlated to the type of alarm that were not on the watch list. These were generated to aide analysts in determining the source of the attacks. While watch lists were present, they only concentrated on foreign activity. Closer examination of logs and a more comprehensive watch list should be developed to include U.S. commercial companies.

Watchlist 000220 IL-ISDNNET-990517
Israel

Total number of alerts from Israel: 13962 (watch list 000220 IL-ISDNET-990517)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
212.179.38.141	4320	4320	1	1
212.179.19.134	3231	3231	1	1
212.179.41.218	1970	1970	1	1
212.179.54.69	1805	1805	1	1
212.179.23.4	1702	1702	1	1
212.179.4.238	730	730	1	1
212.179.101.218	85	85	1	1
212.179.123.13	64	64	1	1
212.179.69.68	10	10	1	1
212.179.27.6	9	9	1	1
212.179.126.2	7	7	1	1
212.179.125.114	6	6	1	1
212.179.126.8	4	4	1	1
212.179.29.132	4	4	1	1
212.179.103.179	4	4	1	1
212.179.5.131	4	4	2	2
212.179.103.232	4	4	1	1
212.179.30.29	2	2	1	1
212.179.58.2	1	1	1	1

Watchlist 000222 NET-NCFC
China

Total number of alerts from China: 4711 (watch list 000222 NET-NCFC)

Whois: 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

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))

159.226.64.164	1681	1681	3	3
159.226.115.1	1345	1345	1	1
159.226.5.77	296	296	3	3
159.226.91.37	256	256	1	1
159.226.45.3	244	244	4	4
159.226.66.130	96	96	3	3
159.226.21.3	87	87	4	4
159.226.45.108	84	84	1	1
159.226.5.152	75	75	1	1
159.226.5.65	72	72	3	3
159.226.63.200	45	45	1	1
159.226.5.222	44	44	1	1
159.226.228.1	37	37	2	2
159.226.39.134	34	34	2	2
159.226.159.1	31	31	1	1
159.226.39.1	30	30	3	3
159.226.21.134	28	28	1	1
159.226.64.137	24	24	2	2
159.226.240.66	21	21	3	3
159.226.5.188	21	21	2	2
159.226.42.3	20	20	1	1
159.226.61.6	19	19	3	3
159.226.91.38	17	17	1	1
159.226.5.94	13	13	1	1
159.226.67.61	12	12	1	1
159.226.165.25	11	11	1	1
159.226.23.155	11	11	1	1
159.226.219.1	10	10	1	1
159.226.116.129	9	9	1	1
159.226.114.1	8	8	1	1
159.226.158.188	6	6	1	1
159.226.63.190	5	5	2	2
159.226.45.109	5	5	1	1
159.226.49.23	4	4	1	1
159.226.52.248	3	3	1	1
159.226.250.54	2	2	1	1
159.226.21.171	2	2	1	1
159.226.224.1	1	1	1	1
159.226.47.217	1	1	1	1
159.226.8.50	1	1	1	1

Most active sources/alarms (not on watch)

Number of alerts	IP address	type of alarm/exploit	whois
1	255.254.99.51	ACTIVE TELNET DAEMON	
1	209.245.5.158	ICMP SOURCE QUENCH	LEVEL 3
1	202.159.46.234	BACKORRIFICE	INDONET, INDONESIA
2	151.164.223.206	WU-FTPD	SOUTHWESTERN BELL,TX
1	24.3.29.155	QUESO FINGERPRINT	@HOME , MD
1	210.84179.196	QUESO FINGERPRINT	OZEMAIL2-AU
1	192.203.80.142	QUESO FINGERPRINT	RUSSIAN ACADEMY OF SCI
1	203.251.136.2	HAPPY 99 VIRUS	KOREA TELECOM
1	200.223.11.7	HAPPY 99 VIRUS	RNP BRAZIL
1	206.67.51.242	HAPPY 99 VIRUS	MEDIA 3 TECH
1	208.130.42.17	HAPPY 99 VIRUS	LOGON AMERICA
6	63.236.34.174	TINY FRAGMENTS	QUOKA SPORTS
14	205.188.3.205	SUNRPC HIGH PORT ACCESS	AOL
3	210.121.242.164	NULL SCAN	KOREA TELECOM
5	149.225.111.69	NULL SCAN	AUNET, DE
23	205.128.11.157	NMAP TCP PING	HEADHUNTER NET
90	208.184.216.183	NAPSTER 7777 DATA	ABOVENET
14	207.217.120.29	GAIC PORT 35555	EARTHLINK
63	152.163.224.100	GIAC 000218 VA-CIRT PORT 34555	AOL
219	255.254.101.160	SMB NAME WILDCARD	
205	208.184.216.189	NAPSTER 888 DATA	ABOVENET
131	255.254.97.237	SNMP PUBLIC ACCESS	
159	255.254.97.80	SNMP PUBLIC ACCESS	
208	255.254.97.186	SNMP PUBLIC ACCESS	
1170	211.40.176.214	large UDP packet	BORANET KOREA
155	168.120.16.250	WINGATE 1080	ASSUMPTION UNIVERSITY, TH
104	208.240.218.220	WINGATE 1080	PROF. COMPUTER SERVICES
2166	205.188.153.111	SUNRPC	AOL, VIRGINIA
1145	128.231.171.123	WINGATE 8080	National Inst of Health (1 DEST)
275	24.3.26.53	WINGATE	@ HOME MD, CATV (1 Dest)
222	216.0.124.26	WINGATE	DIGEX INC, MD
208	24.3.42.201	WINGATE	@HOME, MD
19818	202.0.178.98	SYN/FIN	China Motion Telcom Holdings Ltd.
4923	24.23.96.119 (PA)	dest unreachable	@Home Network
2346	24.4.52.197 (TX)	dest unreachable	@Home Network
801	255.254.14.2	ICMP time exceeded	MY.NET (112 destinations)

The above table was derived to provide a quick snapshot of activity against the network to provide evidence of the type of activity and from whom.

Most active Destination IP

Number of alerts	IP address	type of alarm/exploit	whois
1	24.25.111.117	TIME WARNER ROADRUNNER MN	
1	255.254.70.121	ICMP SOURCE QUENCH	

1	255.254.100.100	BACKORRIFICE
1	255.254.99.16	WU-FTPD
1	255.254.144.59	WU-FTPD
1	255.254.60.8	QUESO
1	255.254.6.44	QUESO
1	255.254.99.23	QUESO
1	255.254.110.150	HAPPY 99
1	255.254.253.42	HAPPY 99
1	255.254.6.47	HAPPY 99
1	255.254.6.34	HAPPY 99
6	255.254.1.8	TINY FRAGMENTS
14	255.254.98.145	SUNRPC HIGH PORT ACCESS
5	255.254.60.14	NULL SCAN
4	255.254.100.236	NULL SCAN
34	255.254.1.8	NMAP
90	255.254.97.204	NAPSTER 7777
74	255.254.253.24	GIAC 000218 35555
115	255.254.253.24	GIAC 000218 34555
219	255.254.101.192	SMB NAME WILDCARD
249	255.254.201.2	NAPSTER 888
1147	255.254.101.192	SNMP PUBLIC ACCESS
1170	255.254.98.179	LARGE UDP PACKET
150	255.254.60.16	WINGATE 1080
241	255.254.60.8	WINGATE 1080
285	255.254.60.11	WINGATE 1080
ALL MY.NET RECEIVED 1 SYN/FIN.		
2166	255.254.217.126	SUNRPC
2854	255.254.253.105	WINGATE (51 SOURCES)
11305	255.254.70.121	dest unreachable
271	255.254.140.9	dest unreachable
5830	255.254.140.9	ICMP Time exceeded

Evidence of Suspicious Activity
The What/When

: The first alarm that is of interest is the **SYN–FIN scan**. The majority of the alarms were generated by IP address 202.0.178.98 (19818). SYN-FIN is an unreasonable flag combination and is indicative of a crafted packet. Please note that many of the ports are to and from ports that are well known perhaps hoping that it would conseal the attack. The SYN-FIN attack was found throughout the entire period.

SYN-FIN

6/28/00 IP address **202.0.178.98** performed a scripted automated SYN-FINscan of nearly all subnets from 225.254.1.3-255.254.254.255 against port 53 (DNS). The duration of the attack was from 0652:28-0714:23. The duration of the attack on each subnet lasted for exactly 5 seconds per subnet scanned (very fast!). Source IP resolves to:

```
inetnum:   202.0.160.0 - 202.0.179.255
netname:   CMNET-HK
descr:      China Motion Telcom Holdings Ltd.
descr:      Roaming Paging Services Provider
descr:      Roaming Trunking Services Provider
descr:      Hong Kong
06/28-06:57:51.979238  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.60.141:
53
06/28-06:57:51.982215  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.60.140:
53
06/28-06:57:52.012786  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.60.142:
53
06/28-06:57:52.041484  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.60.145:
53
```

****note incrementing target IP addresses**

6/29/00 IP address **210.222.31.100** conducted probes to ports 1524 (ingreslock) and 2222 (Allen-Bradley unregistered port) on IP addresses 255.254.1.4 and 255.254.1.5 respectively. Source IP resolves to:

```
IP Address      : 210.222.31.96-210.222.31.127
Connect ISP Name   : KORNET
Connect Date : 1999.09.17
Registration Date: 19991027
Network Name    : KRJD-GAME
```

IP address **207.236.111.226** conducted activity against 255.254.1.4 source/dest port 21 (FTP).

```
Bell Global Network Operations (NETBLK-BELLGLOBAL-2)
160 Elgin Street, Floor 12
Ottawa, Ontario K2P 2C4
Ca
```

7/11/00 1910:54 IP address **210.222.31.100** (Network Name   : KRJD-GAME) conducts SYN-FIN against 255.254.1.4-1.5 on ports 1524 (ingreslock).

```
IP Address      : 210.222.31.96-210.222.31.127
Connect ISP Name   : KORNET
Connect Date : 1999.09.17
Registration Date: 19991027
Network Name    : KRJD-GAME
```

7/17/00 0304:29 IP address **200.255.45.3**7 conducted   0304:29 IP address 200.255.45.37 conducted a SYN-FIN against 255.254.1.4-1.5 with a source and destination port of 25 (smtp).

```
RNP (Brazilian Research Network) (NETBLK-BRAZIL-BLK2)
Rua Pio XI, 1500
Sao Paulo, 05468-901
BR
```

7/29/00 IP address **208.50.27.150** conducted probes to ports 53 on addresses 255.254.1.3-1.5. The times were 1306:49 and 1751:09 (2 sets).
Source IP resolves to:
UB Networks (NETBLK-FGC-REQ000000004806-1)
624 S Grand 1 Wilshire BLDG
Los Angeles, CA 90007
US
IP address **212.177.241.139** at 1752:43 conducted SYN-FIN activity against port 109 (pop-2)
8/1/00 IP address 207.0.62.254 conducted probes to port 1524 and 9704 to addressed 255.254.1.4-1.5 at 0442:24 and 1432:06 respectively.
inetnum: 212.177.0.0 - 212.177.255.255
netname: IT-UUNET-990512
descr: PROVIDER
country: IT

8/3/00 IP address **206.78.1.18** conducted SYN-FIN scan to 255.254.1.4-1.5, source/destination port of 21(FTP).
Tulare County Office of Education (NETBLK-TCOENET-0-31)
2637 West Burrel
Visalia, CA 93278-5091
US

IP address **63.69.63.2** conducted activity against 255.254.1.4 source/dest port 21 (FTP).
Guthrie & Assoc. & Realty (NETBLK-UU-63-69-63)
1357 Washington Street
Clarkesville, GA 30523
US
8/5/00 IP address **63.16.52.48** conducted SYN-FIN activity against 255.254.1.4-1.5 port 53 (DNS).
UUNET Technologies, Inc. (NETBLK-NETBLK-UUNET97DU)
3060 Williams Drive, Suite 601
Fairfax, va 22031
US
The SYN-FIN scan is a reconassance /Intel gathering effort on the part of the attackers. It is unreasonable to have this flag combination, which is crafted, for other than malicious intent. The FIN is sent in hopes of penetrating the firewall without detection.

The Null scans

```
08/03-19:59:23.475592  [**] SYN-FIN scan! [**] 149.225.111.69:7904 -> MY.NET.60.
14:1302
08/03-19:59:23.729894  [**] Null scan! [**] 149.225.111.69:7904 -> MY.NET.60.14:
7
```

```
08/03-19:59:23.774250  [**] Null scan! [**] 149.225.111.69:7904 -> MY.NET.60.14:
22
08/03-19:59:23.823304  [**] Null scan! [**] 149.225.111.69:7904 -> MY.NET.60.14:
37
08/03-19:59:23.877719  [**] Null scan! [**] 149.225.111.69:7904 -> MY.NET.60.14:
137
08/03-19:59:23.971660  [**] Null scan! [**] 149.225.111.69:7904 -> MY.NET.60.14:
513
```

EUnet Deutschland GmbH (NET-CUMULUS-)
Emil-Figge-Str. 80
D-44227 Dortmund
DE

```
06/30-08:26:02.939759  [**] NMAP TCP ping! [**] 195.25.86.2:80 -> MY.NET.60.14:8
0
```

```
inetnum:     202.0.160.0 - 202.0.179.255
netname:     CMNET-HK
descr:       China Motion Telcom Holdings Ltd.
descr:       Roaming Paging Services Provider
descr:       Roaming Trunking Services Provider
descr:       Hong Kong
```

Ports with known vulnerabilities are scanned in the above session:
1302- unassigned
7-echo
22-SSH Remote Login Protocol
37-Time
137-NETBIOS Name Service
513-remote login a la telnet
80-World Wide Web HTTP
53-Domain Name Server

```
06/28-07:01:47.613225  [**] SYN-FIN scan! [**] 202.0.178.98:53 -> MY.NET.106.190
:53
07/12-18:58:16.425144  [**] Null scan! [**] 24.6.244.27:1778 -> MY.NET.106.190:6
699
07/12-18:58:24.335726  [**] Null scan! [**] 24.6.244.27:128 -> MY.NET.106.190:17
78
07/12-18:58:38.347294  [**] Null scan! [**] 24.6.244.27:1778 -> MY.NET.106.190:6
699
07/12-18:58:38.535136  [**] Null scan! [**] 24.6.244.27:1778 -> MY.NET.106.190:6
699
```

ports:
53- Domain Name Server
6699-NAPSTER
1778- prodigy-internet

SYN-FIN and Null scans are stealth attempts to pass through firewalls and packet filters

Null scans are utilized to gather important information about a network. To include the names of administrators/users, home directories, password information, account information, log on/off times, last server logged on to. !: According to the current snort ruleset, this alert triggers when no TCP flags are set, and the sequence and acknowledgement numbers are
both zero.

FINGER

```
07/26-11:22:52.958328  [**] spp_portscan: End of portscan from 193.251.15.20 (TO
TAL HOSTS:76 TCP:79 UDP:0) [**]
07/26-13:39:58.959906  [**] spp_portscan: End of portscan from 193.251.15.20 (TO
TAL HOSTS:76 TCP:79 UDP:0) [**]
07/26-13:50:29.936857  [**] spp_portscan: End of portscan from 193.251.15.20 (TO
TAL HOSTS:76 TCP:79 UDP:0) [**]
07/27-05:16:22.683021  [**] spp_portscan: End of portscan from 193.251.15.20 (TO
TAL HOSTS:76 TCP:79 UDP:0) [**]
07/27-05:32:57.576868  [**] spp_portscan: End of portscan from 193.251.15.20 (TO
TAL HOSTS:76 TCP:79 UDP:0) [**]
```

This is yet another powerful information gathering technique to gain information about a network, similar to null scan. A review of finger was provided in section 2.

Wingate

Number of alerts	IP address	type of alarm/exploit	whois
155	168.120.16.250	WINGATE 1080	ASSUMPTION UNIVERSITY, TH
104	208.240.218.220	WINGATE 1080	PROF. COMPUTER SERVICES
1145	128.231.171.123	WINGATE 8080	National Inst of Health (1 DEST)
275	24.3.26.53	WINGATE	@ HOME MD, CATV (1 Dest)
222	216.0.124.26	WINGATE	DIGEX INC, MD
208	24.3.42.201	WINGATE	@HOME, MD

Number of alerts	IP address	type of alarm/exploit	whois
150	255.254.60.16	WINGATE 1080	
241	255.254.60.8	WINGATE 1080	
285	255.254.60.11	WINGATE 1080	
2854	255.254.253.105	WINGATE (51 SOURCES)	

Scans for port 1080 are actually looking for WinGate, a popular firewall/proxy for Windows.
Port 8080 is also a scan for proxy servers..

Relevent CVE's:

CVE-1999-0290

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

CVE-1999-0291

The WinGate proxy is installed without a password, which allows remote attackers to redirect connections without authentication.
CVE-1999-0441
Remote attackers can perform a denial of service in WinGate machines using a buffer overflow in the Winsock Redirector Service.

NMAP

```
07/28-23:32:23.408944  [**] NMAP TCP ping! [**] 216.127.150.136:57882 ->
MY.NET.253.114:1
08/04-08:01:02.191197  [**] NMAP TCP ping! [**] 195.25.86.2:80 -> MY.NET.179.77:80
08/04-10:49:10.811041  [**] NMAP TCP ping! [**] 205.128.11.157:80 -> MY.NET.1.8:53
08/04-10:49:10.811088  [**] NMAP TCP ping! [**] 205.128.11.157:53 -> MY.NET.1.8:53
08/04-11:18:28.348261  [**] NMAP TCP ping! [**] 205.128.11.157:80 -> MY.NET.1.8:53
08/04-11:18:28.348302  [**] NMAP TCP ping! [**] 205.128.11.157:53 -> MY.NET.1.8:53
```

NMAP is a powerful intelligence gathering tool, it provides information about the status of ports and what services are running on them.
Example:

```
The TCP connect scan took 1 seconds to scan 1489 ports.
Interesting ports on  (XXX.XX.XX.X):
Port    State      Protocol  Service
21     open       tcp       ftp
23     open       tcp       telnet
25     open       tcp       smtp
79     open       tcp       finger
80     open       tcp       http
98     open       tcp       linuxconf
111     open       tcp       sunrpc
113     open       tcp       auth
513     open       tcp       login
514     open       tcp       shell
515     open       tcp       printer
985     open       tcp       unknown
1024     open       tcp       unknown
```

From this an attack can narrow the attack concentrating on open ports and known services.

```
07/29-16:24:37.660049  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:37.681154  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:37.886257  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:42.003947  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:43.950767  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
```

```
Y.NET.98.145:32771
07/29-16:24:48.732229  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:50.394313  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:50.395577  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:51.127465  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:51.872439  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:51.879197  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
07/29-16:24:53.247324  [**] SUNRPC highport access! [**] 205.188.3.205:5190 -> M
Y.NET.98.145:32771
```

Port
32771-Ghost portmapper. Many routers do not block high ports, even if port 111 is blocked access can be obtained through this port.

```
08/05-02:47:09.846709  [**] SUNRPC highport access! [**] 192.102.249.3:25 -> MY.
NET.130.94:32771
08/05-02:47:09.972830  [**] SUNRPC highport access! [**] 192.102.249.3:25 -> MY.
NET.130.94:32771
08/05-02:47:10.049275  [**] SUNRPC highport access! [**] 192.102.249.3:25 -> MY.
NET.130.94:32771
```

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

Possible Denial of Service
8/5/00

A distributed denial of service attack possibly occurred between 08/05/00 1830:02, many thousands of alarms detected from numerous source IP addresses. In between the ICMP alarms are Napster alarms. Napster consumes much bandwidth , however the destination of the Napster alarms are not to the same destination IP address as the ICMP alarms (MY.NET.98.178) Additionally the destination of the large UDP packet alarms is different from the ICMP alarms

```
08/05-18:30:02.238620  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:02.363375  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:02.406802  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
08/05-18:30:02.462952  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:02.467568  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:02.619108  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
```

```
08/05-18:30:02.683382  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:02.805540  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:03.032120  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:03.264610  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:03.268228  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
08/05-18:30:03.331103  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:03.331542  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:03.466717  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:03.472446  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
08/05-18:30:03.557528  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:03.561212  [**] PING-ICMP Destination Unreachable [**] 209.86.165.105 ->
MY.NET.70.121
08/05-18:30:03.665329  [**] PING-ICMP Destination Unreachable [**] 216.127.194.37 ->
MY.NET.70.121
08/05-18:30:03.715992  [**] PING-ICMP Destination Unreachable [**] 209.178.160.203 ->
MY.NET.70.121
08/05-18:30:03.777730  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214:29536 -
>MY.NET.98.179:6970
08/05-18:30:03.835886  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214:29536 ->
MY.NET.98.179:6970
05-18:30:10.125959  [**] Napster 8888 Data [**] 208.184.216.191:8888 ->
MY.NET.201.2:1463
08/05-18:30:10.162613  [**] PING-ICMP Destination Unreachable [**]
MY.NET.70.121 -> 24.168.8.137
08/05-18:30:10.164073  [**] PING-ICMP Destination Unreachable [**]
MY.NET.70.121 -> 24.4.52.197
08/05-18:30:10.193654  [**] PING-ICMP Destination Unreachable [**]
MY.NET.70.121 -> 24.129.222.8
08/05-18:30:24.096348  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214
:29536 -> MY.NET.98.179:6970
08/05-18:30:24.098000  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214
:29536 -> MY.NET.98.179:6970
08/05-18:30:24.100646  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214
:29536 -> MY.NET.98.179:6970
08/05-18:30:29.402872  [**] IDS247 - MISC - Large UDP Packet [**] 211.40.176.214
:29536 -> MY.NET.98.179:6970
```

```
08/05-19:03:45.028697  [**] PING-ICMP Time Exceeded [**] 198.32.248.61 ->
MY.NET
.140.9
08/05-19:03:45.283695  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 ->
MY.NET
.140.9
08/05-19:03:45.283891  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 ->
MY.NET
.140.9
08/05-19:03:45.284581  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 ->
MY.NET
.140.9
08/05-19:03:45.290169  [**] PING-ICMP Time Exceeded [**] 206.196.177.9 ->
MY.NET
.140.9
08/05-19:03:45.297401  [**] PING-ICMP Time Exceeded [**] 206.196.177.9 ->
MY.NET
.140.9
08/05-19:03:45.327004  [**] PING-ICMP Time Exceeded [**] 198.32.8.45 ->
MY.NET.1
40.9
08/05-19:03:45.338953  [**] PING-ICMP Time Exceeded [**] 198.32.8.45 ->
MY.NET.1
40.9
08/05-19:03:45.372818  [**] PING-ICMP Time Exceeded [**] 198.32.8.65 ->
MY.NET.1
40.9
08/05-19:03:45.409750  [**] PING-ICMP Time Exceeded [**] 198.32.8.65 ->
MY.NET.1
40.9
08/05-19:03:45.522918  [**] IDS08 - TELNET - daemon-active [**]
MY.NET.99.51:23
-> 24.25.111.117:1029
08/05-19:03:45.633509  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 ->
MY.NET
```

```
[navcirt@thematrix ~]$ more SnortMergA.txt | grep 08/05-19:03:45 | more
08/05-19:03:45.028697  [**] PING-ICMP Time Exceeded [**] 198.32.248.61 -> MY.NET
.140.9
08/05-19:03:45.283695  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 -> MY.NET
.140.9
08/05-19:03:45.283891  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 -> MY.NET
.140.9
08/05-19:03:45.284581  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 -> MY.NET
.140.9
08/05-19:03:45.290169  [**] PING-ICMP Time Exceeded [**] 206.196.177.9 -> MY.NET
.140.9
08/05-19:03:45.297401  [**] PING-ICMP Time Exceeded [**] 206.196.177.9 -> MY.NET
.140.9
```

```
08/05-19:03:45.327004  [**] PING-ICMP Time Exceeded [**] 198.32.8.45 -> MY.NET.1
40.9
08/05-19:03:45.338953  [**] PING-ICMP Time Exceeded [**] 198.32.8.45 -> MY.NET.1
40.9
08/05-19:03:45.372818  [**] PING-ICMP Time Exceeded [**] 198.32.8.65 -> MY.NET.1
40.9
08/05-19:03:45.409750  [**] PING-ICMP Time Exceeded [**] 198.32.8.65 -> MY.NET.1
40.9
08/05-19:03:45.522918  [**] IDS08 - TELNET - daemon-active [**] MY.NET.99.51:23
-> 24.25.111.117:1029
08/05-19:03:45.633509  [**] PING-ICMP Time Exceeded [**] 206.196.178.5 -> MY.NET
```

Note that the TELNET daemon active hidden in the PING-ICMP time exceeded.
*****Telnet daemon indicates successful telnet connection has been established from outside local network**

NAPSTER

NAPSTER (port 6699)

```
08/01-01:52:09.897907  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.38.141:2792 -> MY.NET.217.38:6699
```

```
Jul 27 12:45:02 24.112.193.183:6699 -> MY.NET.182.71:2334 NOACK 2*S*R*** RESERVEDBITS
Jul 27 13:32:23 24.166.184.108:2116 -> MY.NET.98.107:6699 INVALIDACK ****R*AU

08/05-18:30:07.112277  [**] Napster 8888 Data [**] MY.NET.201.2:1463 -> 208.184.216.191:8888

Aug  4 12:35:38 193.150.235.135:52547 -> MY.NET.20.10:8888 SYN **S*****
Aug 10 17:34:03 64.244.202.66:62949 -> MY.NET.179.86:8888 SYN **S*****

08/05-18:34:08.606042  [**] Napster 7777 Data [**] MY.NET.97.229:49153 -> 208.184.216.178:7777
08/05-18:34:09.147293  [**] Napster 7777 Data [**] 208.184.216.178:7777 -> MY.NET.97.229:49153

Jul  9 21:26:06 165.138.228.4:7777 -> MY.NET.97.68:2077 UDP
Jul  9 21:26:06 165.138.228.4:7777 -> MY.NET.97.68:2079 UDP
```

Possibly being exploited – foreign source (Israel) attempting to connect to Napster client. Users share MP3 files from Napster.com. Destination port 6699 is common.
Napster uses TCP for client to server communication. Typically the servers run on ports 8888 and 7777.

SNMP public access

Number of alerts	IP address	type of alarm/exploit	whois
1147	255.254.101.192	SNMP PUBLIC ACCESS	

Number of alerts	IP address	type of alarm/exploit	whois
31	255.254.97.237	SNMP PUBLIC ACCESS	
159	255.254.97.80	SNMP PUBLIC ACCESS	
208	255.254.97.186	SNMP PUBLIC ACCESS	

```
07/14-08:13:19.325170  [**] SNMP public access [**] MY.NET.97.237:1042 ->
MY.NET.101.192:161
07/14-08:13:26.293120  [**] SNMP public access [**] MY.NET.97.237:1044 ->
MY.NET.101.192:161
```

Trojans and Viruses

```
 07/12-17:16:32.897041  [**] Back Orifice [**] 202.159.46.234:31338 -> MY.NET.100
130:31337
```

```
07/19-04:28:40.867369  [**] Happy 99 Virus [**] 203.251.136.2:4985 -> 255.254.25
3.42:25
07/26-07:50:56.700210  [**] Happy 99 Virus [**] 208.130.42.17:40221 -> 255.254.6
.34:25
08/05-11:22:48.017066  [**] Happy 99 Virus [**] 206.67.51.242:4889 -> 255.254.6.
47:25
07/11-19:28:57.652242  [**] Happy 99 Virus [**] 200.223.11.7:4836 -> 255.254.110
.150:25
07/19-04:28:40.867369  [**] Happy 99 Virus [**] 203.251.136.2:4985 -> MY.NET.253
.42:25
07/26-07:50:56.700210  [**] Happy 99 Virus [**] 208.130.42.17:40221 -> MY.NET.6.
34:25
08/05-11:22:48.017066  [**] Happy 99 Virus [**] 206.67.51.242:4889 -> MY.NET.6.4
7:25
07/11-19:28:57.652242  [**] Happy 99 Virus [**] 200.223.11.7:4836 -> MY.NET.110.
150:25
```

203.251.136.2	HAPPY 99 VIRUS	KOREA TELECOM
200.223.11.7	HAPPY 99 VIRUS	RNP BRAZIL
206.67.51.242	HAPPY 99 VIRUS	MEDIA 3 TECH
208.130.42.17	HAPPY 99 VIRUS	LOGON AMERICA

TRIN00 Possible DDOS

Port 34555 – 196 hits 25 sources – 9 destinations

```
[navcirt@thematrix ~]$ more SnortMerg*.txt |grep 34555 | more
07/14-17:24:07.822935  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:07.836480  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:08.041518  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:08.095022  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:08.217332  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:08.311098  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:08.386778  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:09.818616  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
-> 255.254.253.24:34555
07/14-17:24:09.820191  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.251.8.74:25
```

```
    ➔ 255.254.253.24:34555
--More--
SnortA2.txt          SnortS16.txt
[navcirt@thematrix ~]$ more SnortMerg*.txt |grep 34555 | more
7/27-02:24:55.894950  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:24:56.098479  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:25:24.196893  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:25:24.197032  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
```

```
7/27-02:24:55.894950  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:24:56.098479  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:25:24.196893  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:25
-> 255.254.253.24:34555
07/27-02:25:24.197032  [**] GIAC 000218 VA-CIRT port 34555 [**] 165.166.0.25:2
```

```
07/14-18:22:19.700023  [**] GIAC 000218 VA-CIRT port 35555 [**] 207.69.200.243:1
13 -> MY.NET.253.43:35555
07/17-19:05:44.909909  [**] GIAC 000218 VA-CIRT port 35555 [**] 132.239.1.48:113
 -> MY.NET.100.230:35555
07/14-21:20:26.582141  [**] GIAC 000218 VA-CIRT port 34555 [**] 192.102.249.3:25
 -> MY.NET.130.94:34555
07/14-21:20:26.582230  [**] GIAC 000218 VA-CIRT port 34555 [**] 192.102.249.3:25
 -> MY.NET.130.94:34555
07/14-21:20:26.582286  [**] GIAC 000218 VA-CIRT port 34555 [**] 192.102.249.3:25
 -> MY.NET.130.94:34555
07/14-21:20:26.582385  [**] GIAC 000218 VA-CIRT port 34555 [**] 192.102.249.3:25
 -> MY.NET.130.94:34555
07/19-04:29:13.183069  [**] GIAC 000218 VA-CIRT port 35555 [**] 216.86.47.7:113
MY.NET.6.34:35555
```

In addition to the above IP address the following address sustained alerts:
255.254.254.42.
CAN-2000-0138 (under review)
Description: A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed, such as (1) Trinoo, (2) Tribe Flood Network (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, or (6) shaft.

Analysis Process

The logs for the exercise were downloaded from the following location:
http://www.sans.org/PH2000/snort/index.htm

Snortsnarf was downloaded from the following web site:
www.silicondefense.com/snortsnarf/main.html.

After merging the alert and scan files, snortsnarf was utilized. This format was web based and we were able to examine the contents as separate web pages. Analysis by alarm type, source, destination were conducted and correlations were developed. We utilized grep to examine detailed information from the logs.