William Majewski submits these 10 traces for the practical examination following the Intrusion Detection (Track II) course curriculum attended at SANS2000, San Jose.

Detect 1

```
May 18 19:09:03 hostd in.ftpd[7353]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:09:43 hostz ftpd[32675]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:09:43 hosts ftpd[1965]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:46:50 dns1 ftpd[251521]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:46:51 dns2 in.ftpd[9543]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:46:54 dns3 in.ftpd[10792]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:47:37 dns1 ftpd[240348]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:47:43 hostk in.ftpd[13687]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
May 18 19:47:46 hostl proftpd[17619] locust.cns.vt.edu
  (msx-ode-17-11.ppp.cybercity.dk[212.242.7.139]):
  connected - local : 198.82.250.222:21
May 18 19:47:46 hostl proftpd[17619] locust.cns.vt.edu
  (msx-ode-17-11.ppp.cybercity.dk[212.242.7.139]):
  connected - remote : 212.242.7.139:2615
May 18 19:47:46 hostl proftpd[17619] locust.cns.vt.edu
  (msx-ode-17-11.ppp.cybercity.dk[212.242.7.139]):
  received: USER anonymous
May 18 19:47:46 hostl proftpd[17619] locust.cns.vt.edu
  (msx-ode-17-11.ppp.cybercity.dk[212.242.7.139]):
  FTP session closed.
May 18 19:47:48 hostc in.ftpd[14923]:
  refused connect from msx-ode-17-11.ppp.cybercity.dk
```

1. Source of trace
    a. http://www.sans.org/y2k/052300-0800.htm

2. Detect was generated by:
    a. FTP Log
    b. Explanation of fields:

```
May 18 19:09:03 [Timestamp] hostd in.ftpd[7353]:
[Destination][daemon][Port] refused connect [Action] from msx-
ode-17-11.ppp.cybercity.dk [Source]{Hostname may signify the
following}[17th Modem, 11th Bank]
```

3. Probability the source address was spoofed

    a. Low. More than likely used a hack tool or even a simple script that would do nslookup on the entire block of IP's and see what the hostnames were, or just attacked by IP.

4. Description of attack:

FTP Probe against random nodes inside the network after the attacker has dialed-in.

5. Attack mechanism:

The attack works by sending FTP connect statements to the nodes inside the network and gets "refused connect" as the response. If a connection is successful the session is immediately closed and continues its probe.

I&W Semantic Model: This is reconnaissance and planning work to see if common exploitable usernames and passwords allow access (i.e. Guest account logged into)

6. Correlations:

This particular detect has been seen before. FTP probes are consistently seen across the internet for reconnaissance purposes. Similar attack located at http://www.sans.org/y2k/052300-0800.htm against Intermedia Internet Service, Kingsport TN, USA on the same day.

7. Evidence of active targeting:

General scan of entire network as seen by the multiple Host and DNS nodes in the log.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (3 + 4) – (3 + 2) = 2

Criticality =3 Mix of Hosts Lethality = 4 User Access (Guest account found, could be knowledge for a follow-on exploit)

System = 3 (Guest Account should not have been left available)

Net Countermeasures = 2 (Behind firewall, internal probe from dial-up user)

Additional comments are as follows:

The severity depends a lot on the particular use of the network. If this network belongs to an ISP, this kind of attack is expected and guarded against, making it a relatively minor matter since it is known that the machines are on the outside and subject to attack. If machines are inside a firewall and that attack was a surprise, then either the firewall admin needs to get on the ball, or ftp is left open and the same precautions should be taken as for machines outside the firewall.

9. Defensive recommendation:

- Install latest versions of ftpd on machines that need ftp access
- Disable ftpd on machines where it is not required
- Disable guest accounts and anonymous access unless explicitly required

- Make sure powerful accounts such as root on UNIX and administrator on NT, DO not have ftp access.
- Run crack on all account passwords to ensure that attackers cannot guess the password from the username.
- Make sure that ftpd is configured correctly and that all accounts are chrooted to prevent anyone from getting your password file via ftp, authorized or not.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

This trace is best described as:

a) Distributed Denial of Service
b) Map Open Hosts on a Network
c) Spoofed IP Address
d) Mis-configured FTP Server

Answer: B

Detect 2

```
May 10 09:20:33.328 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.1.2.73(0) -> 192.231.90.254(0), 1 packet
May 10 09:26:04.564 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.1.2.73(0) -> 192.231.90.254(0), 4 packets
May 10 09:26:34.260 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.0.0.57(0) -> 192.231.90.254(0), 1 packet
May 10 09:32:04.708 UTC: %SEC-6-IPACCESSLOGP: list 100 denied tcp
10.0.0.57(0) -> 192.231.90.254(0), 20 packets
```

1. Source of trace

a. http://www.sans.org/y2k/050900.htm

2. Detect was generated by:

b. CISCO router ACL log

c. Explanation of fields

```
May 10 09:20:33.328 [Timestamp] UTC: %SEC-6-IPACCESSLOGP: list 100
[Router ACL responsible for action] denied [Action] tcp [transport
protocol] tcp 10.1.2.73(0) -> [Source Address and Port]
192.231.90.254(0) [Destination Address and Port], 1 Packet [#of
packets]
```

3. Probability the source address was spoofed

Medium. Outbound filters have been reported to prevent private IP address from getting out. However, the private addresses are seen outside the firewall. Need further evidence from a TCP Dump to analyze sequence numbers for more credibility.

4. Description of attack:

Attack against TCP port 0 on a CISCO Border router; this is a reserved TCP port.

5. Attack mechanism:

The attack works by sending packets of data from multiple sources on port zero to the same destination on port zero. The reason why an attacker would send packets of data to source port zero would be to find a backdoor or an alternative way around your firewall via the border router. The ACL prevented this action, however, it is a significant detect because it may have found a way in if there are multiple routers involved that do not contain this ACL list.

I&W Semantic Model: This trace identifies that the adversary is in the pre-attack phase due to the trace showing that the attacker is aware of an exploit, and testing to see if the user network is vulnerable.

6. Correlations:

A similar source port zero detect has been seen before on GIAC (May 15, 2000) with Stephen Northcutt as the handler on duty.

CVE Correlation: A similar attack utilizing UDP is referenced at: http://www.cve.mitre.org/ CAN-1999-0675 (under review) reports a denial of service via UDP packets that are sent through VPN-1 to port 0 of a host.

7. Evidence of active targeting:

Attacker is going after a particular port on particular host. 192.231.90.254(0)

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (2 + 1) – (4 + 4) = -5

c. Explanation:

Criticality =2 (Specific node address reported in log) Lethality = 1 (Attack unlikely to succeed due to reported block in log)

System = 4 (Detailed system logging identifies the system monitored and maintained regularly)

Net Countermeasures = 4 (ACL prevented attack)

9. Defensive recommendation:

ACL provided necessary defense here. Recommend reviewing all routers on the network to ensure the preventive ACL is provided. Also recommend looking at other router logs to correlate similar log statements. (No router should EVER let non-routable private address space such as 10.1.1.* or 192.168.1.* in from the outside.)

10. Multiple choice test question.

Port Zero is best described as?

a) Reserved port for TCP

b) Reserved port for UDP
c) Reserved port for TCP and UDP
d) Reserved port

Answer: C

Detect 3

```
May 22 15:33:29 : SYN FIN Scan: 216.17.180.143:53 -> 192.168.1.99:53
May 22 15:33:29 : SYN FIN Scan: 216.17.180.143:53 -> 192.168.1.109:53
May 22 15:33:29 : SYN FIN Scan: 216.17.180.143:53 -> 192.168.1.100:53
May 22 15:33:29 : SYN FIN Scan: 216.17.180.143:53 -> 192.168.1.105:53
```

1. Source of trace

http://www.sans.org/y2k/052300-0800.htm

2. Detect was generated by:

TCP Dump

```
May 22 15:33:29 : [Timestamp] SYN FIN Scan [Segment Flags]:
216.17.180.143:53 [Source Address and Port] ->
192.168.1.99:53[Destination Address and Port]
```

3. Probability the source address was spoofed:

Low. Attacker chooses to scan using SYN FIN flags. If the address were spoofed, trust would be a characteristic to look for (SYN FIN is an impossible flag combination and will never be generated under normal trusted conditions.)

4. Description of attack:

Scan against TCP port 53, this is a Scan for DNS. SYN FIN packets generally elude packet filters and other ID systems that are looking for SYN only connections. As noted in the GIAC manual 2.2 on page 114, the attacked may be looking for a Linux operating system that will respond to a SYN-FIN with a SYN-FIN-ACK.

5. Attack mechanism:

The scan works by sending multiple SYN FIN packets to destination port 53. The destination IP addresses are randomized. The TCP three-way handshake will not complete.

This attack is significant because the attacker is attempting to elude IDS' with a specific probe to the DNS port 53.

I&W Semantic Model: Reconnaissance and Planning

6. Correlations:

This detect was reported by Vicki Irwin/Hal Pomeranz on page 114 (2.2) in Intrusion Detection and Packet Filtering: How it Really Works.

CVE correlation: CVE 1999-0275 Denial of Service in Windows NT DNS servers by flooding port 53 with too many characters.

7. Evidence of active targeting:

This scan was a general scan of the entire network for port 53 in a randomized manner.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (4 + 3) – (3 + 2) = 2

c. Explanation:

Criticality = 4 (DNS port 53 is being scanned for in the log. 5 would have been given if the DNS was found and was attacked explicitly)

Lethality = 3 (SYN-FIN attack successfully scanning for port 53.)

System = 3 (host based security could deny access to this port)

Net Countermeasures = 2 (Permissive firewall allowed this traffic to go through)

9. Defensive recommendation:

Evidently, monitoring was performed for SYN-FIN packets. Recommend, inserting a rule into your router ACL that would prevent 216.17.180.143 any inbound traffic since this attack can be explicitly pointed back to a host. (Typically, packet filters will not prevent the SYN FIN scan.)

10. Multiple choice test question.

This trace is best described as:

a) Attack to elude detection
b) SYN – FIN impossible flag combination
c) DNS attack
d) All of the above

Answer: D

Detect 4

```
May 16 18:57:27 dns1 portsentry[438328]: attackalert:
Connect from host: sv.maxell.co.jp/210.189.72.11
to TCP port: 1080
May 16 18:57:27 dns1 snort[51901]: MISC-WinGate-1080-Attempt:
210.189.72.11:13806 -> z.y.w.34:1080
--------
[**] MISC-WinGate-1080-Attempt [**]
05/16-18:57:27.013702 210.189.72.11:13806 -> z.y.w.34:1080
TCP TTL:47 TOS:0x0 ID:3420
**S***** Seq: 0xB56208CB Ack: 0x0 Win: 0x200
TCP Options => MSS: 1460
00 00 ..

May 16 18:57:27 dns3 snort[3439]: MISC-WinGate-1080-Attempt:
210.189.72.11:13805 -> z.y.w.98:1080
May 16 18:57:32 dns3 portsentry[6017]: attackalert:
Connect from host: sv.maxell.co.jp/210.189.72.11
```

```
to TCP port: 1080
--------
[**] MISC-WinGate-1080-Attempt [**]
05/16-18:57:27.005778 210.189.72.11:13805 -> z.y.w.98:1080
TCP TTL:48 TOS:0x0 ID:3419
**S***** Seq: 0xD37EC9FE Ack: 0x0 Win: 0x200
TCP Options => MSS: 1460
00 00 ..

May 17 03:58:51 dns1 portsentry[438328]: attackalert:
Connect from host: sv.maxell.co.jp/210.189.72.11
to TCP port: 1080
May 17 03:58:51 dns1 snort[51901]: MISC-WinGate-1080-Attempt:
210.189.72.11:20622 -> z.y.w.34:1080
--------
[**] MISC-WinGate-1080-Attempt [**]
05/17-03:58:51.067633 210.189.72.11:20622 -> z.y.w.34:1080
TCP TTL:48 TOS:0x0 ID:59383
**S***** Seq: 0x47AEF370 Ack: 0x0 Win: 0x200
TCP Options => MSS: 1460
00 00 ..

May 17 03:58:51 dns3 portsentry[6017]: attackalert:
Connect from host: sv.maxell.co.jp/210.189.72.11
to TCP port: 1080
May 17 03:58:51 dns3 snort[3439]: MISC-WinGate-1080-Attempt:
210.189.72.11:20621 -> z.y.w.98:1080
--------
[**] MISC-WinGate-1080-Attempt [**]
05/17-03:58:51.056915 210.189.72.11:20621 -> z.y.w.98:1080
TCP TTL:47 TOS:0x0 ID:59382
**S***** Seq: 0x8734DD8B Ack: 0x0 Win: 0x200
TCP Options => MSS: 1460
00 00 ..
```

1. Source of trace

http://www.sans.org/y2k/052000.htm

2. Detect was generated by:

Snort intrusion detection system.

```
[**] MISC-WinGate-1080-Attempt [**]
05/17-03:58:51.056915 [Timestamp] 210.189.72.11:20621 [Source Address
and Port] -> z.y.w.98:1080 [Destination Port and Address]
TCP [Protocol] TTL:47 [Time to Live}] TOS:0x0 [Type of Service]
ID:59382 [Identification] **S***** Seq: 0x8734DD8B [Sequence Number]
Ack: 0x0[Acknowledgement] Win: 0x200 [Window Size]
```

3. Probability the source address was spoofed

Low. Attack method does not require a spoof, but rather a tool to generate connect request statements.

4. Description of attack:

Stealthy attack against TCP port 1080 for SOCKS Servers. This is scanning a network for SOCKS servers via connect system calls; likely performed from a Unix system. These packets require no special privileges to create and send. A normal scan for socks servers would indicate multiple successive attempts (same day, same hour, within seconds of each other) to port 1080 on a network. This is stealthy due to the attacker sending a few connect request statements and then leaving to come back another day. (Reference p. 113 GIAC 2.2 Intrusion Detection and Packet Filtering: How it really works.)

5. Attack mechanism:

The attack works by sending SYN requests to port 1080 among various nodes on a network. The attacker is scanning for a possible response for a confirmed proxy service. (1080 is a common location for proxy.) A proxy server could be used by the source to assist in masking the sources action.

I&W Semantic Model: Pre-Attack (Specific scan for port 1080)

6. Correlations:

This attack was reported by Vicki Irwin and Hal Pomeranz, Tuesday May 9th Intrusion Detection course and is documented on p. 113 GIAC 2.2 Intrusion Detection and Packet Filtering: How it really works.

Cert Advisory 98.03 and http://wingate.deerfield.com/helpdesk/secure-wingate.cfm identifies services to lock down to minimize exposure (with reference to port 1080).

7. Evidence of active targeting:

Going after a specific port (1080) on a specific network (z.y.w.98:1080 and z.y.w.34:1080). The attack appears to select nodes at random.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (4 + 2) – (3 + 2) = 1

c. Explanation:

Criticality = 4 (Socks Server attacked)

Lethality = 2 (Confidentiality of a known SOCKS server could be obtained)

System = 3 (rule on host could lockdown port to prevent scan)

Net Countermeasures = 2 (Permissive firewall allowed this scan to occur)

9. Defensive recommendation:

Insert a rule in firewall or router to protect system from this attack. Specifically, the attack originates from a single source and this source could be specified in the rule.

Do not run Telnet or SOCKS servers with public access. If needed, restrict what requests the server will perform. Require users of these services to be authenticated. (Reference: http://wingate.deerfield.com/helpdesk/secure-wingate.cfm)

10. Multiple choice test question.

This log can best be described as?

a) SNORT Scan for SOCKS Server
b) TCPDUMP for SOCKS Server
c) SNORT Scan for TRINOO
d) SNORT Scan for Squid Proxy

Answer: A

Detect 5

```
May 5 10:35:29 158.152.158.148:30974 ->
xxx.yyy.135.170:16404 INVALIDACK 21S*RPAU RESERVEDBITS
May 5 10:35:29 158.152.158.148:1832 ->
xxx.yyy.135.170:80 SYN **S*****
( Try it again? 30975 decimal, LSBs are 11111111 and all flags are set, 11111111 )
May 5 10:35:37 158.152.158.148:30975 ->
xxx.yyy.135.170:32788 FULLXMAS 21SFRPAU RESERVEDBITS
May 5 10:35:42 158.152.158.148:30974 ->
xxx.yyy.135.170:16404 INVALIDACK 21S*RPAU RESERVEDBITS
```

1. Source of trace

http://www.sans.org/y2k/051700.htm

2. Detect was generated by:

Snort Intrusion Detection System

May 5 10:35:29 [Timestamp] 158.152.158.148:1832 -> [Source Address and Port] xxx.yyy.135.170:80 [Destination Address and Port] SYN **S***** [TCP Flags]

3. Probability the source address was spoofed

Low. This attack was a crafted packet from the source. Spoof attempt would look subtler with the normal 3-way handshake attempts.

4. Description of attack:

NMAP scan used to send impossible packets, otherwise known as “Christmas Tree”.

5. Attack mechanism:

The attack works by continuously sending impossible packets to a particular hosts ports.

The significance of these impossible packets is to generate responses from the various ports, in the sense that no response is seen from open ports, and closed ports generate a response packet.

I&W Semantic Model: Reconnaissance and Planning. (This action could serve as reconnaissance for a follow-on attack.)

6. Correlation:

This attack was reported by Vicki Irwin and Hal Pomeranz, Tuesday May 9th Intrusion Detection course and is documented on p. 137 GIAC 2.2 Intrusion Detection and Packet Filtering: How it really works.

7. Evidence of active targeting:

Going after a specific host xxx.yyy.135.170. The ports seen in the trace (30974 and 30975) are unassigned.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (2 + 2) – (3 + 2) = -1

c. Explanation:

Criticality =2 (Specific node address reported in log)

Lethality = 2 Attacking a hosts ports, no evidence of further breach)

System = 3 (rule on host could lockdown port to prevent scan)

Net Countermeasures = 2 (Permissive firewall allowed this scan to occur)

9. Defensive recommendation:

An established rule in the router will block these scans.

10. Multiple choice test question:

Which of the following best describes a XMAS tree scan:

a) FIN PUSH and Urgent flags are set.
b) Cannot be blocked by an established ACL
c) Cannot be generated by NMAP
d) All of the above

Answer: A

Detect 6

```
17:38:43.881085 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.893904 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.900769 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.917082 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.919305 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
```

```
17:38:43.922072 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.929369 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.974449 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:43.981770 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:45.085487 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:45.109610 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:55.398081 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255:
icmp: echo request
17:38:55.399878 sdn-ar-003orportP110.dialsprint.net > 255.255.255.255: icmp: echo request
```

1. Source of trace

   My Network

2. Detect was generated by:

   WINDUMP.

```
20:43:48.492453 [Timestamp] my.grandad.has.bigboobies.co.uk [Source]>
255.255.255.255: [destination] icmp: [protocol] echo request [stimulus]
```

3. Probability the source address was spoofed

   Good.   The source IP address is spoofed, and the echo requests are directed to the 255 style broadcast.

4. Description of attack: Coordinated DOS attack using ICMP echo request scripts.

5. Attack mechanism:

   The attack works by multiple attackers sending subnet-directed broadcast packets to my network (unfortunately). The directed broadcasts were successfully translated to hardware broadcasts on the local LAN, causing the individual hosts to respond.

   This is significant, because it creates a bottleneck on all of my remaining routers. Routing is slowed significantly, and have to utilize more resources to deliver their packets. Email delivery was significantly slower (3hrs roundtrip time).

   I&W Semantic Model: Attack (The broadcasts are coming in from various sources and are significantly reducing bandwidth)

6. Correlations:

   This particular detect has been seen before.   Broadcast floods have been previously recorded on my network on this same day (as documented below).

```
18:45:32.489142 members.it.tripod.de > 255.255.255.255: icmp: echo
request
18:45:32.811367 members.it.tripod.de > 255.255.255.255: icmp: echo
request
```

```
18:45:32.929595 members.it.tripod.de > 255.255.255.255: icmp: echo
request
18:45:33.023059 members.it.tripod.de > 255.255.255.255: icmp: echo
request
18:45:33.026791 members.it.tripod.de > 255.255.255.255: icmp: echo
request

20:43:45.149421 my.grandad.has.bigboobies.co.uk > 255.255.255.255:
icmp: echo request
20:43:45.165895 my.grandad.has.bigboobies.co.uk > 255.255.255.255:
icmp: echo request
20:43:45.175281 my.grandad.has.bigboobies.co.uk > 255.255.255.255:
icmp: echo request
```

Page 64 in 2.2 of Intrusion Detection and Packet Filtering described this DOS.

CVE 1999-0514 UDP messages to broadcast addresses

Cert Incident note IN-99-07 report of intruders installing distributed denial of service tools.

7. Evidence of active targeting:

This denial of service was a broadcast of the entire network.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (5 + 3) – (4 + 2) = 2

c. Explanation:

Criticality =5 (one of my core routers)

Lethality = 3 (DOS, network was very sluggish)

System = 4 (modern OS, most patches applied)

Net Countermeasures = 2 (Permissive firewall allowed this DOS to occur)

9. Defensive recommendation:

Setup ICMP Echo Traffic Filters in the routers. Specifically, I recommend blocking inbound echo requests and echo-replies from passing through the router. Ideally, you want to allow ICMP to your router for general troubleshooting. (i.e access-list 142 deny icmp my.network.0.0 0.0.255.255 any echo-reply and echo).

10. Multiple choice test question.

Which statement describes the security needed to prevent this DOS?

a) deny inbound echo-replies at the router
b) deny inbound echo-requests at the router
c) Both A & B
d) none of the above, this is a misconfigured router – reload router config files

Answer:C

Detect 7

```
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33438 L=38 S=0x00 I=54992 F=0x0000
T=1 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33439 L=38 S=0x00 I=54993 F=0x0000
T=1 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33440 L=38 S=0x00 I=54994 F=0x0000
T=1 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33441 L=38 S=0x00 I=54995 F=0x0000
T=2 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33442 L=38 S=0x00 I=54996 F=0x0000
T=2 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33443 L=38 S=0x00 I=54997 F=0x0000
T=2 (#35)
May 31 19:31:07 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33444 L=38 S=0x00 I=54998 F=0x0000
T=3 (#35)
May 31 19:31:12 chopper kernel: Packet log: output REJECT eth0 PROTO=17
mynet.130:61062 216.111.65.217:53 L=58 S=0x00 I=41641 F=0x0000 T=63
(#43)
May 31 19:31:12 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33445 L=38 S=0x00 I=54999 F=0x0000
T=3 (#35)
May 31 19:31:17 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33446 L=38 S=0x00 I=55000 F=0x0000
T=3 (#35)
May 31 19:31:22 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33447 L=38 S=0x00 I=55001 F=0x0000
T=4 (#35)
May 31 19:31:22 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33448 L=38 S=0x00 I=55002 F=0x0000
T=4 (#35)
May 31 19:31:22 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33449 L=38 S=0x00 I=55003 F=0x0000
T=4 (#35)
May 31 19:31:22 chopper kernel: Packet log: output ACCEPT eth0 PROTO=17
mynet.130:61076 attackednetwork.250:33450 L=38 S=0x00 I=55004 F=0x0000
T=5 (#35)
```

1. Source of trace

   My Network

2. Detect was generated by:

   Coyote Linux Firewall Log

May 31 19:31:22 [timestamp] chopper kernel [Firewall Name]: Packet log: output ACCEPT [is what the rule said to do to the packet] eth0 [interface name] PROTO=17 [means that the packet was protocol 17] mynet.130:61076 [source address and port] attackednetwork.250:33450 [destination address and port] L=38 [means that packet was a total of 34 bytes long] S=0x00 [means the Type of Service field (divide by 4 to get the Type of Service] I=55004[is the IP ID] F=0x0000 [0x0000 is the 16-bit fragment offset plus flags] T=5 [is the Time To Live of the packet]

3. Probability the source address was spoofed

   Low. My firewall box (outbound traffic) logged this scan from a known host inside my network.

4. Description of attack:

   Internal host most likely using NMAP or MSCAN to probe attackednetwork.com. Ports are being scanned sequentially on the attacked network. The scan is neither obscure nor stealthy. Rather, the attacker is blatant and probably understands that our network is undermanned (as an internal host) and can afford to probe freely.

5. Attack mechanism:

   The attack works by the host using a common (Unix based) mapping tool known as network mapping (NMAP) or multiscan (MSCAN). Specifically, the NMAP/MSCAN tool is used here by the attacker identifying a hosts IP address, and then scan's the hosts port numbers beginning at 33438 (the Multiscan).

   This probe sequentially tested upper level ports on one of the attacked networks hosts. This is significant because the attacker (on my net) is looking for vulnerabilities. Once a vulnerable port is identified, a more advanced tool can be run against that port!

   I&W Semantic Model: Reconnaissance and Planning. Currently, this probe is in the reconnaissance and planning stage based on the sequential port scans seen above.

6. Correlations:

   This particular detect has been seen before. The NMAP/MSCAN tool is used often for reconnaissance and pre-attack purposes. SANS GIAC 2.5, pages 261-263 describe this attack.

   CVE - CAN 1999-0454

7. Evidence of active targeting:

   The log specifically identifies a particular hosts ports being scanned for. The host is attackednetwork.250. The ports on this host are scanned for sequentially beginning at 33438.

8. Severity:

   a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

   b. (2+ 2) – (4 + 2) = -2

   c. Explanation:

   Criticality =2 (host system)

   Lethality = 2 (Reconnaissance, no system access exploit, (yet).

   System = 4 (modern OS, most patches applied)

Net Countermeasures = 2 (Permissive firewall allowed this DOS to occur)

9. Defensive recommendation:

This is a host based issue, and could easily turn into a larger network problem if the attacker finds an exploit. Since one of my nodes is the culprit, I will curtail the action by shutting down my friendly attacker. To prevent follow-on attacks, I would block outgoing traffic at the router from this subnet to the attacked network.

10. Multiple choice test question:

What stage most likely describes this attack? (choose two)

a) Reconnaissance and Planning
b) Pre-Attack
c) Attack
d) Post Attack

Answer: A & B

```
20:23:09.394166 mail.clutter.com.61104 > mynetwork.com.2112: S
1582078045:1582078045(0) win 3072
20:23:09.394320 mynetwork.com.2112 > mail.clutter.com.61104: R 0:0(0)
ack 1582078046 win 0
20:23:09.396484 mail.clutter.com.61109 > mynetwork.com.5998: S
1582078045:1582078045(0) win 3072
20:23:09.396561 mynetwork.com.5998 > mail.clutter.com.61109: R 0:0(0)
ack 1582078046 win 0
20:23:09.398378 mail.clutter.com.61110 > mynetwork.com.9876: S
1582078045:1582078045(0) win 3072
20:23:09.398453 mynetwork.com.9876 > mail.clutter.com.61110: R 0:0(0)
ack 1582078046 win 0
20:23:09.798533 mail.clutter.com.61122 > mynetwork.com.1518: S
1582078045:1582078045(0) win 3072
20:23:09.798699 mynetwork.com.1518 > mail.clutter.com.61122: R 0:0(0)
ack 1582078046 win 0
20:23:09.801058 mail.clutter.com.61124 > mynetwork.com.1663: S
1582078045:1582078045(0) win 3072
20:23:09.801139 mynetwork.com.1663 > mail.clutter.com.61124: R 0:0(0)
ack 1582078046 win 0
20:23:10.529323 mail.clutter.com.61141 > mynetwork.com.5236: S
1582078045:1582078045(0) win 3072
20:23:10.529477 mynetwork.com.5236 > mail.clutter.com.61141: R 0:0(0)
ack 1582078046 win 0
20:23:10.530617 mail.clutter.com.61146 > mynetwork.com.2012: S 1582078045:1582078045(0) win 3072
```

Detect 8

1. Source of trace

My Network

2. Detect was generated by:

WINDUMP

20:23:10.529323 [timestamp] mail.clutter.com.61141 [source address and port] > mynetwork.com.5236:[destination address and port] S [SYN flag] 1582078045:1582078045(0)[sequence numbers] win 3072 [window size]

3. Probability the source address was spoofed.

Low. This is reconnaissance work captured on a node running WINDump outside my firewall. The node is used for testing and attracts various exploits, a good "honey pot". Port scanning was performed and does not require a spoofed IP. The source IP address was valid and confirmed activity was also validated.

4. Description of attack:

Random NMAP scan against a host outside the firewall on my network.

5. Attack mechanism:

This NMAP works by the attacker sending SYN's to my accessible node soliciting for a SYN + ACK on accessible ports. Scanned ports are randomly selected. Window size and sequence were constant throughout the attack. No SYN + ACK's were documented in my WINDUMP log, however, a log of Resets has been recorded. A reset was sent in response to each of the SYN's to indicate a closed port.

The result of running nmap is a list of ports and machines which are scanned to determine their availability with responding information such as: open, filtered and unfiltered. This would be a good tool for pre-attack and reconnaissance purposes to see what types of things are available for follow-on exploits using more powerful tools.

I&W Semantic Model: Reconnaissance and Planning. (Typical NMAP scan)

6. Correlations:
This particular detect has been seen before and is well documented on the Internet. A good URL that provides assistance with NMAP includes:
http://www.securiteam.com/tools/Nmap_Port_scanner.htm

7. Evidence of active targeting:

Yes, the node running WINDUMP was scanned randomly for available ports.

8. Severity:

d. (Critical + Lethal) – (System + Net Countermeasures) = Severity

e. (2+ 2) – (4 + 0) = 0

f. Explanation:

Criticality =2 (host WINDUMP system)

Lethality = 2 (Reconnaissance, no system access exploit, (yet).

System = 4 (modern OS, most patches applied)

Net Countermeasures = 0 (No firewall -allowed this DOS to occur purposely)

9. Defensive recommendation: Set certain TCP/IP filters that will make automatic detection more difficult. Test the nodes open to outside users to determine if they openly show the OS they are running. Since this system was on an NT platform I would setup my registry to reflect the recommendation stated at:
http://www.securiteam.com/windowsntfocus/Preventing_nmap_OS_detection_for_Windows_NT.html

The registry edits located at this URL prevent NMAP from easily detecting the OS type.

10. Multiple choice test question.
Which statement accurately describes this scan?
a) Ping o' Death
b) Stealthy Network Mapping
c) Denial of Service
d) NMAP

Answer: D

```
15:59:04.764875 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:04.765016 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:05.265518 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:05.265656 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:05.766122 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:05.766278 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:06.266732 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:06.266868 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:06.339649 Entry.West.mynetwork.com > 10.24.0.88: icmp: host
c.root-servers.net unreachable - admin prohibited
15:59:06.767397 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:06.767514 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:07.268008 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:07.268149 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:07.768666 DISGRUNTLED_COMPUTERSCIENTIST > VICTIMS-LAPTOP: icmp:
echo request
15:59:07.768786 TARGET_NODE> DISGRUNTLED_COMPUTERSCIENTIST: icmp: echo
reply
15:59:07.963543 Entry.West.mynetwork.com > 10.24.0.89: icmp: host
f.root-servers.net unreachable - admin prohibited
```

Detect 9

1. Source of trace

My Internal Network

2. Detect was generated by:

   Windump

   15:59:07.768786 [Timestamp]TARGET_NODE[source address]> DISGRUNTLED_COMPUTERSCIENTIST [destination address]: icmp[protocol]: echo reply [response]

3. Probability the source address was spoofed

   Moderate. This was an internal problem. Internal IP addresses, architecture, and available services are well known, however spoofing was not necessarily needed to perform this DOS, but could have easily been done based on available network knowledge.

4. Description of attack:

   ICMP denial of service. Utility used to generate ping - ICMP echo requests / echo replies between two hosts. (This is not Ping O' Death, impossible packets size are not generated)

5. Attack mechanism:

   The attack works by sending a single ICMP packet from one host to another multiple times (echo request); each time the attacked host responds with a (echo reply). These packets are not fragmented and reassembled. They reach the destination IP, and cause a significant bandwidth reduction.

   Specifically, a shareware ping utility was used here to automatically generate these echo requests.

   The significance of this attack would cause the bandwidth of the network to be saturated. The attacked computer was a Windows NT implementation with SP3, however, all systems on the network are affected because they all see this broadcast ICMP. Additionally, the addressed machine is now a participant in saturating the bandwidth with an echo reply to each echo request.

   I&W Semantic Model: Attack (The action was deliberate and specifically addressed to a particular node)

6. Correlations:

   This detect has been seen before. GIAC – SANS manual 2.2 on pages 65-67 describe this attack.

7. Evidence of active targeting:

   Yes, ICMP echo requests were directed toward a single host. Both the source and destination hosts were in my internal network. Additionally, the log file also shows an attempt to send an ICMP echo request to one of my border routers. (admin prohibited) However, I explicitly deny ping inbound and outbound ICMP (pings) to it, therefore no attack was successful there.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (4+ 4) – (3 + 2) = 3

c. Explanation:

Criticality =4 (All hosts on my internal subnet affected)

Lethality = 4 (DOS was achieved, bandwidth saturated, network slowed significantly)

System = 3 (Service Pack 3 used, older SP.)

Net Countermeasures = 2 (Permissive internal router allowed this DOS to occur)

9. Defensive recommendation:

Since this was an internal problem, we shutdown the attacker's node, added new policy to our network guidelines, and kindly provided the policy to all personnel.

If this attack originated from outside my network, I would deny ping for a period of time since this could breakdown several nodes quickly and is not required for any applications we support. (Denying ping is difficult due to so many clients being familiar, and making use of the ping utility) Then allow ping after a period of time and attentively monitor ICMP for this exploit.

10. Multiple choice test question.

Which of the following best describes the Ping o' Death attack?

a) Impossible Packet
b) Crafted Packets
c) Reassembled Packets
d) All of the above

Answer: D

```
22:50:53.943414 207-172-111-243.s243.tnt1.ann.va.dialup.rcn.com.32043 >
mynet.com.2933: S 899364:899364(0) win 8192 <mss 536,nop,nop,sackOK>
(DF)
22:50:53.943568 mynet.com.2933 > 207-172-111-
243.s243.tnt1.ann.va.dialup.rcn.com.32043: R 0:0(0) ack 1 win 0
22:50:53.967534 209.164.53.221.80 > mynet.com.2008: S
3548912393:3548912393(0) ack 41169178 win 32120 <mss
1460,nop,nop,sackOK> (DF)
22:50:53.967681 mynet.com.2008 > 209.164.53.221.80: . ack 1 win 8760
(DF)
22:50:54.055416 mynet.com.2008 > 209.164.53.221.80: P 1:380(379) ack 1
win 8760 (DF)
22:50:54.297873 209.164.53.221.80 > mynet.com.2008: . ack 380 win 31741
(DF)
22:50:54.311451 209.164.53.221.80 > mynet.com.2008: P 1:1461(1460) ack
380 win 32120 (DF)
22:50:54.323013 209.164.53.221.80 > mynet.com.2008: P 1461:2921(1460)
ack 380 win 32120 (DF)
22:50:54.323150 mynet.com.2008 > 209.164.53.221.80: . ack 2921 win 8760
(DF)
22:50:54.404522 mynet.com.137 > myrouter.137: udp 50
```

```
22:50:54.429035 207-172-111-243.s243.tnt1.ann.va.dialup.rcn.com.32069 >
mynet.com.2882: S 895444:895444(0) win 8192 <mss 536,nop,nop,sackOK>
(DF)
22:50:54.429158 mynet.com.2882 > 207-172-111-
243.s243.tnt1.ann.va.dialup.rcn.com.32069: R 0:0(0) ack 1 win 0
22:50:54.566476 209.164.53.221.80 > mynet.com.2008: P 2921:4381(1460)
ack 380 win 32120 (DF)
22:50:54.580226 209.164.53.221.80 > mynet.com.2008: P 4381:5841(1460)
ack 380 win 32120 (DF)
22:50:54.580366 mynet.com.2008 > 209.164.53.221.80: . ack 5841 win 8760
(DF)
22:50:54.588454 209.164.53.221.80 > mynet.com.2008: P 5841:7301(1460)
ack 380 win 32120 (DF)
22:50:54.756017 mynet.com.2008 > 209.164.53.221.80: . ack 7301 win 8760
(DF)
22:50:54.955483 207-172-111-243.s243.tnt1.ann.va.dialup.rcn.com.32027 >
mynet.com.2892: S 895584:895584(0) win 8192 <mss 536,nop,nop,sackOK>
(DF)
22:50:54.955603 mynet.com.2892 > 207-172-111-
243.s243.tnt1.ann.va.dialup.rcn.com.32027: R 0:0(0) ack 1 win 0
/*(last time I see ann.va.dialup.rcn.com)
22:50:55.906063 mynet.com.137 > myrouter.137: udp 50
22:50:56.435705 209.164.53.221.80 > mynet.com.2008: P 7301:8761(1460)
ack 380 win 32120 (DF)
22:50:56.556040 mynet.com.2008 > 209.164.53.221.80: . ack 8761 win 8760
(DF)
22:50:56.854341 209.164.53.221.80 > mynet.com.2008: P 8761:10221(1460)
ack 380 win 32120 (DF)
22:50:56.863800 209.164.53.221.80 > mynet.com.2008: P 10221:11681(1460)
ack 380 win 32120 (DF)
22:50:56.863923 mynet.com.2008 > 209.164.53.221.80: . ack 11681 win 8760
(DF)
```

Detect 10

1. Source of trace

My Network

2. Detect was generated by:

WINDUMP

```
22:32:49.936971 [Timestamp] mail.clutter.com.63254[source address and
port] > mynet.com.23[destination address and port]: S [SYN
flag]11049458:11049458(0)[sequence numbers] win 8192[window size] <mss
1460> [max segment size](DF)[do not fragment flag]
```

3. Probability the source address was spoofed

Good. The start of the trace identifies my network sending packets with a R (reset flag) to a destination (VA User), which looks like a dial-up user (this traffic is rampant – multiple packets over several seconds/minutes). (One of my hosts complains with the R, in essence, saying what are you talking about?)

VA host attacks with SYN's and Resets. 209.164.53.221 is sent a SYN from a host on my network. (Handshake takes place, then the UDP flood starts)

Then, host address 209.164.53.221 shows up with a host on my network sending it a SYN. 209.164.53.221 appears to be a trusted host because one of my hosts pushes data to 209.164.53.221. (Expected sequence number calculated by VA dial-in user and then handed off to 209.164.53.221 to send a UDP flood) The next thing I know a host on my network is sending my router a continuous stream of UDP packets (1 minute apart), with a size of 50!

4. Description of attack:

Spoofed IP address, then follow-on UDP flood from a host on my network to my router.

5. Attack mechanism:

At first, a host on my network was spoofed. Several SYN, RESETS were exchanged between the attacker (Host in Virginia) and my host. This occurred for a couple hours. (Knowledge now obtained by the attacker. i.e. sequence numbers – Pre-attack) The ip address of 209.164.53.221 (California Internet company) shows up (VA dial-up user abruptly stops) and sends a stimulus to my network (SYN). We respond (ack) and begin a push. Now a continuous flood of UDP packets occurs between a host on my network a my router. 209.164.53.221.80 stays involved as shown below:

209.164.53.221.80 > mynet.com.2008: P 8761:10221(1460) ack 380 win 32120 (DF).

The significance of this attack was that is was an obscure DOS that saturated my router. One of my hosts and router are repetitively sending the following:

22:50:55.906063 mynet.com.137 > myrouter.137: **udp 50**

which is slowing down the routing capabilities on the net.

Excel was extremely helpful in identifying this attack. After observing similar UDP packet sizes in a single column (for many pages) was I able to determine this attack.

I&W Semantic Model: At first pre-attack with a spoofed IP, then attack with UDP flood)

6. Correlations:

This particular detect has been seen before. Specifically, spoofing IP addresses are addressed in SANS GIAC 2.4 Network Based Intrusion Detection Analysis pages 98-107.

CVE 1999-0103 Echo and chargen, or other combinations of UDP services, can be used in tandem to flood the server, a.k.a. UDP bomb or UDP packet storm.

7. Evidence of active targeting:

Two hosts were the target of this attack. A host on my network was attacked from the VA dial-in user. Then, a follow-on UDP flood occurred from a California Internet Company occurred and my router was attacked from a host on my network.

8. Severity:

a. (Critical + Lethal) – (System + Net Countermeasures) = Severity

b. (5+ 3) – (4 + 2) = 2

c. Explanation:

Criticality =5 (main router)

Lethality = 3 (DOS, network was very sluggish, spoofed IP)

System = 4 (modern OS, most patches applied)

Net Countermeasures = 2 (Permissive firewall allowed this DOS to occur)

9. Defensive recommendation:
ftp://info.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial describes UDP flooding defensive recommendations.

Ensure echo and chargen are not being used. I would re-run inetd.conf to make sure this file is re-read.
Investigate the use of a proxy service to screen the use of UDP services.
Rather than shutting down UDP immediately; monitor the network for UDP services and closely watch how they are being used.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

Which services are most often associated with UDP flooding? (Choose two)

a) chargen
b) ftp
c) echo
d) telnet

Answer: A & B