



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

GIAC Certified Intrusion Analyst Practical

For SANS Parliament Hill 2000

Dave Eberlein

Contents:

- Assignment 1- Network Detects
- Assignment 2 - Evaluate an Attack
- Assignment 3 - "Analyze This" Scenario
- Assignment 4 - Analysis Process

Detect #1 (DNS Query ID=0)

```
----- Frame 1 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
1 200.211.187.194  MY.NET.6.8  118 000:00:00.000 09/20/2000 08:44:21 AM DNS: C ID=0 OP=QUERY
ADDR  HEX
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .....I....E.
0010: 00 68 83 24 00 00 f2 06 f4 2b c8 d3 bb c2 xx xx | .hf$.....+.....
0020: 06 08 08 98 00 35 05 d8 b2 5b 00 00 00 00 50 02 | .....5.....P.
0030: 08 00 95 62 00 00 00 00 00 00 00 00 00 00 00 00 | ...b.....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

```
----- Frame 2 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
2 200.211.187.194  MY.NET.6.8  118 000:00:00.000 09/20/2000 08:44:21 AM DNS: C ID=0 OP=QUERY
ADDR  HEX
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .....I....E.
0010: 00 68 00 a6 00 00 f2 06 76 aa c8 d3 bb c2 xx xx | .h.....v.....
0020: 06 08 08 99 00 35 54 15 f0 c9 00 00 00 00 50 02 | .....5T.....P.
0030: 08 00 08 b6 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

```
----- Frame 3 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
3 200.211.187.194  MY.NET.6.8  118 000:00:00.000 09/20/2000 08:44:21 AM DNS: C ID=0 OP=QUERY
ADDR  HEX
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .....I....E.
0010: 00 68 39 de 00 00 f2 06 3d 72 c8 d3 bb c2 xx xx | .h9.....=r.....
0020: 06 08 08 9a 00 35 79 d1 7f 29 00 00 00 00 50 02 | .....5y..)....P.
0030: 08 00 54 99 00 00 00 00 00 00 00 00 00 00 00 00 | ..T.....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

```
----- Frame 4 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
4 MY.NET.6.8  200.211.187.194  60 000:00:00.001 09/20/2000 08:44:21 AM TCP: D=2200 S=53 SYN
ACK=98087516 SEQ=3543398039 LEN=0 WIN=9112
ADDR  HEX
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ...I....._...E.
0010: 00 2c 73 9b 40 00 fd 06 b8 f0 xx xx xx xx c8 d3 | .,s.@.ý.....
0020: bb c2 00 35 08 98 d3 33 f6 97 05 d8 b2 5c 60 12 | ...5...3.....\`.
0030: 23 98 9c 0d 00 00 02 04 02 18 36 03 | #.....6.
```

```
----- Frame 5 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
5 MY.NET.6.8  200.211.187.194  60 000:00:00.002 09/20/2000 08:44:21 AM TCP: D=2201 S=53 SYN
ACK=1410724042 SEQ=3543399870 LEN=0 WIN=9112
ADDR  HEX
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ...I....._...E.
0010: 00 2c 73 9c 40 00 fd 06 b8 ef xx xx xx xx c8 d3 | .,s.@.ý.....
0020: bb c2 00 35 08 99 d3 33 fd be 54 15 f0 ca 60 12 | ...5...3ý.T....`.
```

0030: 23 98 08 3a 00 00 02 04 02 18 36 03 | #...6.

----- Frame 6 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
6 MY.NET.6.8 200.211.187.194 60 000:00:00.003 09/20/2000 08:44:21 AM TCP: D=2202 S=53 SYN
ACK=2043772714 SEQ=3543445173 LEN=0 WIN=9112

ADDR HEX ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ...I.....E.
0010: 00 2c 73 9d 40 00 fd 06 b8 ee xx xx xx c8 d3 | .,s.@.ý.....
0020: bb c2 00 35 08 9a d3 34 ae b5 79 d1 7f 2a 60 12 | ...5...4..y..*`.
0030: 23 98 a3 25 00 00 02 04 02 18 36 03 | #...%.....6.

----- Frame 7 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
7 200.211.187.194 MY.NET.6.8 60 000:00:00.600 09/20/2000 08:44:21 AM TCP: D=53 S=2200 RST WIN=0

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 17 84 00 00 33 06 1f 0d c8 d3 bb c2 xx xx | .(.,.3.....
0020: 06 08 08 98 00 35 05 d8 b2 5c 00 00 00 50 04 |5...\....P.
0030: 00 00 9d 9f 00 00 00 00 00 00 00 00 |

----- Frame 8 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
8 200.211.187.194 MY.NET.6.8 60 000:00:00.611 09/20/2000 08:44:21 AM TCP: D=53 S=2201 RST WIN=0

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 17 86 00 00 33 06 1f 0b c8 d3 bb c2 xx xx | .(.,.3.....
0020: 06 08 08 99 00 35 54 15 f0 ca 00 00 00 50 04 |5T.....P.
0030: 00 00 10 f3 00 00 00 00 00 00 00 00 |

----- Frame 9 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
9 200.211.187.194 MY.NET.6.8 60 000:00:00.611 09/20/2000 08:44:21 AM TCP: D=53 S=2202 RST WIN=0

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 17 88 00 00 33 06 1f 09 c8 d3 bb c2 xx xx | .(.,.3.....
0020: 06 08 08 9a 00 35 79 d1 7f 2a 00 00 00 50 04 |5y..*....P.
0030: 00 00 5c d6 00 00 00 00 00 00 00 00 | ..\.....

----- Frame 10 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
10 200.211.187.194 MY.NET.6.8 60 000:00:00.615 09/20/2000 08:44:21 AM TCP: D=53 S=2200 RST
ACK=3543398040 WIN=2048

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 7e 2c 00 00 f2 06 f9 63 c8 d3 bb c2 xx xx | .(~,....ùc.....
0020: 06 08 08 98 00 35 05 d8 b2 5c d3 33 f6 98 50 14 |5...\3..P.
0030: 08 00 cb c2 00 00 00 00 00 00 00 00 |

----- Frame 11 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
11 200.211.187.194 MY.NET.6.8 60 000:00:00.615 09/20/2000 08:44:21 AM TCP: D=53 S=2201 RST
ACK=3543399871 WIN=2048

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 df 85 00 00 f2 06 98 0a c8 d3 bb c2 xx xx | .(.....
0020: 06 08 08 99 00 35 54 15 f0 ca d3 33 fd bf 50 14 |5T....3ý.P.
0030: 08 00 37 ef 00 00 00 00 00 00 00 00 | ..7.....

----- Frame 12 -----

Frame Source Address Dest. Address Size Rel. Time Abs. Time Summary
12 200.211.187.194 MY.NET.6.8 60 000:00:00.616 09/20/2000 08:44:21 AM TCP: D=53 S=2202 RST
ACK=3543445174 WIN=2048

ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E.
0010: 00 28 2c 22 00 00 f2 06 4b 6e c8 d3 bb c2 xx xx | .(,"....Kn.....
0020: 06 08 08 9a 00 35 79 d1 7f 2a d3 34 ae b6 50 14 |5y..*4..P.
0030: 08 00 d2 da 00 00 00 00 00 00 00 00 |

1. Source of trace

This trace was from taken from my work network.

2. Detect was generated by:

This detect was generated using a NAI Sniffer detecting traffic to and from my DNS located outside of my Internet gateway router. There were filters set to capture TCP packets with port 53 on the DNS and a port greater then 1023 at the other end of the session. I was looking for high port zone transfers at the time

3. Probability the source address was spoofed.

Two-way communications took place so on the surface it looks like the source address was not spoofed however there are interesting implications when examining the packets more closely. Some of these packets may be spoofed but if so the spoofed address would belong to the attacker as well.

4. Description of attack.

This is an effort to try and find the optimum route from load balancing servers to a DNS server. This same sequence is seen coming from multiple IP addresses (20) and is continuous in nature.

5. Attack mechanism

The attacker starts out by sending three crafted Syn packets with 64 octets of null data added. By itself this is unusual behavior because an initial SYN is normally sent without a payload. The reason for the payload could be to give a truer representation of response time with a larger packet size. At the IP level all of the packets that I captured had IP source ports from 2000 to 4000 in increments of 100. The source port would increment by one for the three Syn packets. The initial packets are received at the trace tool with less then one millisecond separating them. On the trace the summery information calls these packets DNS query requests with an ID=0. The reason for this is the tool will try to interpret the data as a DNS query because of the destination port 53. In fact this is not a DNS query but simply a TCP Syn packet with 64 octets of null data (all zeros).

The DNS then sends back a Syn/Ack packet for each of the packets it has received. The initial sequence number of the first packet sent from the attacker is 98087515 (**05 d8 b2 5b**). The acknowledgement number from the DNS is 98087516 indicating that the DNS has ignored the 64 octets of data and is simply proceeding as if a normal Syn packet had come in.

The attacker then sends a reset packet for each of the sessions that it has started. These packets all have the proper sequence number and are completely valid packets. An interesting point to note is that the TTL value on the initial Syn packets was set to a high number 242 in this particular trace. On the reset packets the TTL is set to 51. This difference of 191 hops on the TTL plays out through all the traces I have gathered. This could be explained in two ways:

- 1) The tool used to generate the packets has this parameter set.
- 2) There are more then one IP stacks involved in the attack.

I have not been able to figure out the meaning of the different TTL's but it may be significant.

The DNS will then reply with a reset acknowledgment packet and the attack is concluded.

6. Correlations:

The "global load balancing" concept is described by Howard Kash in his "Analysis of the Type0 (Class 0) DNS that has been detected, version 1.0" located at: <http://www.sans.org/newlook/resources/IDFAQ/DNS.htm>

7. Evidence of specific targeting:

Twenty machines ran this exact scan to my DNS in an eight hour period, Yes the DNS was targeted.

8. Severity

(Critical + Lethal) – (System + Network Countermeasures) = Severity
(5 + 1) – (4 + 1) = 1

Critical = 5 – DNS

Lethal = 1 – attack succeeded (only intel gained).

System = 4 – system and patches up to date.

Network = 1 – attack got through in its entirety.

9. Defensive recommendation:

This attack would not have succeeded if a firewall or router were filtering on TCP traffic coming in to the port 53 on the DNS from a high (>1023) port. This same filter would also shut down DNS High port zone transfers.

10. Question

| Frame | Source Address | Dest. Address | Size | Rel. Time | Abs. Time | Summary |
|-------|-----------------|---------------|------|---------------|------------------------|----------------------|
| 1 | 200.211.187.194 | MY.NET.6.8 | 118 | 000:00:00.000 | 09/20/2000 08:44:21 AM | DNS: C ID=0 OP=QUERY |

| ADDR | HEX | ASCII |
|-------|---|---------------|
| 0000: | 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 |I....E. |
| 0010: | 00 68 83 24 00 00 f2 06 f4 2b c8 d3 bb c2 xx xx | .hf\$.++++. |
| 0020: | 06 08 08 98 00 35 05 d8 b2 5b 00 00 00 00 50 02 |5.....P. |
| 0030: | 08 00 95 62 00 00 00 00 00 00 00 00 00 00 00 | ...b..... |
| 0040: | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0050: | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0060: | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 0070: | 00 00 00 00 00 00 | |

Given that the preceding packet has only the Syn flag set, and has 64 bytes of data we would expect the receiving host to:

- Discard the packet
- Respond with a reset packet
- Respond with an acknowledgment number of one greater than the sequence number.
- Respond with an acknowledgment number of 65 greater than the sequence number.

Answer c - Data will not be passed at this point of a session setup.

Detect #2 (IPID 0)

| Source Address | Dest. Address | Size | Rel. Time | Abs. Time | Summary |
|----------------|---------------|------|---------------|---------------|--|
| 64.37.200.46 | MY.NET.6.8 | 60 | 000:00:00.000 | 9/14/00 11:47 | TCP: D=1024 S=29462 SYN ACK=13182988 SEQ=13182989 LEN=0 WIN=4128 |
| 64.37.200.46 | MY.NET.6.8 | 60 | 000:00:00.001 | 9/14/00 11:47 | TCP: D=1024 S=29463 SYN ACK=13182989 SEQ=13182990 LEN=0 WIN=4128 |
| 64.37.200.46 | MY.NET.6.8 | 60 | 000:00:00.001 | 9/14/00 11:47 | TCP: D=1024 S=29464 SYN ACK=13182990 SEQ=13182991 LEN=0 WIN=4128 |
| 216.35.167.58 | MY.NET.6.8 | 60 | 000:00:00.017 | 9/14/00 11:47 | TCP: D=1024 S=21281 SYN ACK=15197557 SEQ=15197558 LEN=0 WIN=4128 |
| 216.35.167.58 | MY.NET.6.8 | 60 | 000:00:00.018 | 9/14/00 11:47 | TCP: D=1024 S=21282 SYN ACK=15197558 SEQ=15197559 LEN=0 WIN=4128 |
| 216.35.167.58 | MY.NET.6.8 | 60 | 000:00:00.018 | 9/14/00 11:47 | TCP: D=1024 S=21283 SYN ACK=15197559 SEQ=15197560 LEN=0 WIN=4128 |
| 209.249.97.40 | MY.NET.6.8 | 60 | 000:00:00.038 | 9/14/00 11:47 | TCP: D=1024 S=65506 SYN ACK=15540596 SEQ=15540597 LEN=0 WIN=4128 |
| 209.249.97.40 | MY.NET.6.8 | 60 | 000:00:00.038 | 9/14/00 11:47 | TCP: D=1024 S=65507 SYN ACK=15540597 SEQ=15540598 LEN=0 WIN=4128 |
| 209.249.97.40 | MY.NET.6.8 | 60 | 000:00:00.038 | 9/14/00 11:47 | TCP: D=1024 S=65508 SYN ACK=15540598 SEQ=15540599 LEN=0 WIN=4128 |
| 208.184.162.71 | MY.NET.6.8 | 60 | 000:00:00.041 | 9/14/00 11:47 | TCP: D=1024 S=11305 SYN ACK=9834134 SEQ=9834135 LEN=0 WIN=4128 |
| 208.184.162.71 | MY.NET.6.8 | 60 | 000:00:00.043 | 9/14/00 11:47 | TCP: D=1024 S=11306 SYN ACK=9834135 SEQ=9834136 LEN=0 WIN=4128 |
| 208.184.162.71 | MY.NET.6.8 | 60 | 000:00:00.043 | 9/14/00 11:47 | TCP: D=1024 S=11307 SYN ACK=9834136 SEQ=9834137 LEN=0 WIN=4128 |
| 64.14.200.154 | MY.NET.6.8 | 60 | 000:00:00.046 | 9/14/00 11:47 | TCP: D=1024 S=44793 SYN ACK=13423515 SEQ=13423516 LEN=0 WIN=4128 |
| 64.14.200.154 | MY.NET.6.8 | 60 | 000:00:00.046 | 9/14/00 11:47 | TCP: D=1024 S=44794 SYN ACK=13423516 SEQ=13423517 LEN=0 WIN=4128 |
| 64.14.200.154 | MY.NET.6.8 | 60 | 000:00:00.047 | 9/14/00 11:47 | TCP: D=1024 S=44795 SYN ACK=13423517 SEQ=13423518 LEN=0 WIN=4128 |
| 216.34.68.2 | MY.NET.6.8 | 60 | 000:00:00.053 | 9/14/00 11:47 | TCP: D=1024 S=57374 SYN ACK=13743431 SEQ=13743432 LEN=0 WIN=4128 |
| 216.34.68.2 | MY.NET.6.8 | 60 | 000:00:00.053 | 9/14/00 11:47 | TCP: D=1024 S=57375 SYN ACK=13743432 SEQ=13743433 LEN=0 WIN=4128 |
| 216.34.68.2 | MY.NET.6.8 | 60 | 000:00:00.054 | 9/14/00 11:47 | TCP: D=1024 S=57376 SYN ACK=13743433 SEQ=13743434 LEN=0 WIN=4128 |
| 212.78.160.237 | MY.NET.6.8 | 60 | 000:00:00.075 | 9/14/00 11:47 | TCP: D=1024 S=63104 SYN ACK=9509066 SEQ=9509067 LEN=0 WIN=4128 |
| 212.78.160.237 | MY.NET.6.8 | 60 | 000:00:00.075 | 9/14/00 11:47 | TCP: D=1024 S=63105 SYN ACK=9509067 SEQ=9509068 LEN=0 WIN=4128 |

212.78.160.237 MY.NET.6.8 60 000:00:00.076 9/14/00 11:47 TCP: D=1024 S=63106 SYN ACK=9509068 SEQ=9509069 LEN=0 WIN=4128

62.26.119.34 MY.NET.6.8 60 000:00:00.115 9/14/00 11:47 TCP: D=1024 S=26586 SYN ACK=15467027 SEQ=15467028 LEN=0 WIN=4128

62.26.119.34 MY.NET.6.8 60 000:00:00.116 9/14/00 11:47 TCP: D=1024 S=26587 SYN ACK=15467028 SEQ=15467029 LEN=0 WIN=4128

62.26.119.34 MY.NET.6.8 60 000:00:00.116 9/14/00 11:47 TCP: D=1024 S=26588 SYN ACK=15467029 SEQ=15467030 LEN=0 WIN=4128

MY.NET.6.8 62.26.119.34 60 000:00:00.121 9/14/00 11:47 TCP: D=26586 S=1024 RST WIN=0

MY.NET.6.8 62.26.119.34 60 000:00:00.121 9/14/00 11:47 TCP: D=26587 S=1024 RST WIN=0

MY.NET.6.8 62.26.119.34 60 000:00:00.122 9/14/00 11:47 TCP: D=26588 S=1024 RST WIN=0

194.205.125.26 MY.NET.6.8 60 000:00:00.126 9/14/00 11:47 TCP: D=1024 S=38238 SYN ACK=9748938 SEQ=9748939 LEN=0 WIN=4128

194.205.125.26 MY.NET.6.8 60 000:00:00.126 9/14/00 11:47 TCP: D=1024 S=38236 SYN ACK=9748936 SEQ=9748937 LEN=0 WIN=4128

194.205.125.26 MY.NET.6.8 60 000:00:00.126 9/14/00 11:47 TCP: D=1024 S=38237 SYN ACK=9748937 SEQ=9748938 LEN=0 WIN=4128

194.213.64.150 MY.NET.6.8 60 000:00:00.266 9/14/00 11:47 TCP: D=1024 S=33715 SYN ACK=15526415 SEQ=15526416 LEN=0 WIN=4128

194.213.64.150 MY.NET.6.8 60 000:00:00.266 9/14/00 11:47 TCP: D=1024 S=33716 SYN ACK=15526416 SEQ=15526417 LEN=0 WIN=4128

194.213.64.150 MY.NET.6.8 60 000:00:00.266 9/14/00 11:47 TCP: D=1024 S=33717 SYN ACK=15526417 SEQ=15526418 LEN=0 WIN=4128

64.37.200.46 MY.NET.6.8 60 000:00:01.997 9/14/00 11:47 TCP: D=1024 S=29462 SYN ACK=13182988 SEQ=13182989 LEN=0 WIN=4128

64.37.200.46 MY.NET.6.8 60 000:00:01.998 9/14/00 11:47 TCP: D=1024 S=29463 SYN ACK=13182989 SEQ=13182990 LEN=0 WIN=4128

64.37.200.46 MY.NET.6.8 60 000:00:01.998 9/14/00 11:47 TCP: D=1024 S=29464 SYN ACK=13182990 SEQ=13182991 LEN=0 WIN=4128

MY.NET.6.8 64.37.200.46 60 000:00:02.002 9/14/00 11:47 TCP: D=29462 S=1024 RST WIN=0

MY.NET.6.8 64.37.200.46 60 000:00:02.002 9/14/00 11:47 TCP: D=29463 S=1024 RST WIN=0

MY.NET.6.8 64.37.200.46 60 000:00:02.003 9/14/00 11:47 TCP: D=29464 S=1024 RST WIN=0

216.35.167.58 MY.NET.6.8 60 000:00:02.014 9/14/00 11:47 TCP: D=1024 S=21281 SYN ACK=15197557 SEQ=15197558 LEN=0 WIN=4128

216.35.167.58 MY.NET.6.8 60 000:00:02.014 9/14/00 11:47 TCP: D=1024 S=21282 SYN ACK=15197558 SEQ=15197559 LEN=0 WIN=4128

216.35.167.58 MY.NET.6.8 60 000:00:02.014 9/14/00 11:47 TCP: D=1024 S=21283 SYN ACK=15197559 SEQ=15197560 LEN=0 WIN=4128

MY.NET.6.8 64.37.200.46 60 000:00:02.024 9/14/00 11:47 TCP: D=29462 S=1024 RST WIN=0

MY.NET.6.8 64.37.200.46 60 000:00:02.028 9/14/00 11:47 TCP: D=29463 S=1024 RST WIN=0

MY.NET.6.8 64.37.200.46 60 000:00:02.030 9/14/00 11:47 TCP: D=29464 S=1024 RST WIN=0

209.249.97.40 MY.NET.6.8 60 000:00:02.036 9/14/00 11:47 TCP: D=1024 S=65506 SYN ACK=15540596 SEQ=15540597 LEN=0 WIN=4128

209.249.97.40 MY.NET.6.8 60 000:00:02.036 9/14/00 11:47 TCP: D=1024 S=65507 SYN ACK=15540597 SEQ=15540598 LEN=0 WIN=4128

209.249.97.40 MY.NET.6.8 60 000:00:02.036 9/14/00 11:47 TCP: D=1024 S=65508 SYN ACK=15540598 SEQ=15540599 LEN=0 WIN=4128

208.184.162.71 MY.NET.6.8 60 000:00:02.038 9/14/00 11:47 TCP: D=1024 S=11305 SYN ACK=9834134 SEQ=9834135 LEN=0 WIN=4128

208.184.162.71 MY.NET.6.8 60 000:00:02.038 9/14/00 11:47 TCP: D=1024 S=11306 SYN ACK=9834135 SEQ=9834136 LEN=0 WIN=4128

208.184.162.71 MY.NET.6.8 60 000:00:02.039 9/14/00 11:47 TCP: D=1024 S=11307 SYN ACK=9834136 SEQ=9834137 LEN=0 WIN=4128

64.14.200.154 MY.NET.6.8 60 000:00:02.042 9/14/00 11:47 TCP: D=1024 S=44793 SYN ACK=13423515 SEQ=13423516 LEN=0 WIN=4128

64.14.200.154 MY.NET.6.8 60 000:00:02.043 9/14/00 11:47 TCP: D=1024 S=44794 SYN ACK=13423516 SEQ=13423517 LEN=0 WIN=4128

64.14.200.154 MY.NET.6.8 60 000:00:02.043 9/14/00 11:47 TCP: D=1024 S=44795 SYN ACK=13423517 SEQ=13423518 LEN=0 WIN=4128

MY.NET.6.8 64.14.200.154 60 000:00:02.046 9/14/00 11:47 TCP: D=44793 S=1024 RST WIN=0

MY.NET.6.8 64.14.200.154 60 000:00:02.046 9/14/00 11:47 TCP: D=44794 S=1024 RST WIN=0

MY.NET.6.8 64.14.200.154 60 000:00:02.047 9/14/00 11:47 TCP: D=44795 S=1024 RST WIN=0

216.34.68.2 MY.NET.6.8 60 000:00:02.055 9/14/00 11:47 TCP: D=1024 S=57374 SYN ACK=13743431 SEQ=13743432 LEN=0 WIN=4128

216.34.68.2 MY.NET.6.8 60 000:00:02.055 9/14/00 11:47 TCP: D=1024 S=57375 SYN ACK=13743432 SEQ=13743433 LEN=0 WIN=4128

216.34.68.2 MY.NET.6.8 60 000:00:02.055 9/14/00 11:47 TCP: D=1024 S=57376 SYN ACK=13743433 SEQ=13743434 LEN=0 WIN=4128

MY.NET.6.8 216.35.167.58 60 000:00:02.070 9/14/00 11:47 TCP: D=21281 S=1024 RST WIN=0

MY.NET.6.8 216.35.167.58 60 000:00:02.070 9/14/00 11:47 TCP: D=21282 S=1024 RST WIN=0

MY.NET.6.8 216.35.167.58 60 000:00:02.072 9/14/00 11:47 TCP: D=21283 S=1024 RST WIN=0

212.78.160.237 MY.NET.6.8 60 000:00:02.074 9/14/00 11:47 TCP: D=1024 S=63104 SYN ACK=9509066 SEQ=9509067 LEN=0 WIN=4128

212.78.160.237 MY.NET.6.8 60 000:00:02.074 9/14/00 11:47 TCP: D=1024 S=63105 SYN ACK=9509067 SEQ=9509068 LEN=0 WIN=4128

212.78.160.237 MY.NET.6.8 60 000:00:02.075 9/14/00 11:47 TCP: D=1024 S=63106 SYN ACK=9509068 SEQ=9509069 LEN=0 WIN=4128

MY.NET.6.8 209.249.97.40 60 000:00:02.096 9/14/00 11:47 TCP: D=65506 S=1024 RST WIN=0

194.205.125.26 MY.NET.6.8 60 000:00:02.125 9/14/00 11:47 TCP: D=1024 S=38236 SYN ACK=9748936 SEQ=9748937 LEN=0 WIN=4128

194.205.125.26 MY.NET.6.8 60 000:00:02.125 9/14/00 11:47 TCP: D=1024 S=38237 SYN ACK=9748937 SEQ=9748938 LEN=0 WIN=4128

194.205.125.26 MY.NET.6.8 60 000:00:02.126 9/14/00 11:47 TCP: D=1024 S=38238 SYN ACK=9748938 SEQ=9748939 LEN=0 WIN=4128

MY.NET.6.8 209.249.97.40 60 000:00:02.164 9/14/00 11:47 TCP: D=65507 S=1024 RST WIN=0

MY.NET.6.8 209.249.97.40 60 000:00:02.165 9/14/00 11:47 TCP: D=65508 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:02.170 9/14/00 11:47 TCP: D=11305 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:02.175 9/14/00 11:47 TCP: D=11306 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:02.177 9/14/00 11:47 TCP: D=11307 S=1024 RST WIN=0

MY.NET.6.8 64.14.200.154 60 000:00:02.265 9/14/00 11:47 TCP: D=44793 S=1024 RST WIN=0

194.213.64.150 MY.NET.6.8 60 000:00:02.265 9/14/00 11:47 TCP: D=1024 S=33715 SYN ACK=15526415 SEQ=15526416 LEN=0 WIN=4128

194.213.64.150 MY.NET.6.8 60 000:00:02.265 9/14/00 11:47 TCP: D=1024 S=33716 SYN ACK=15526416 SEQ=15526417 LEN=0 WIN=4128

194.213.64.150 MY.NET.6.8 60 000:00:02.265 9/14/00 11:47 TCP: D=1024 S=33717 SYN ACK=15526417 SEQ=15526418 LEN=0 WIN=4128

MY.NET.6.8 64.14.200.154 60 000:00:02.279 9/14/00 11:47 TCP: D=44794 S=1024 RST WIN=0

MY.NET.6.8 64.14.200.154 60 000:00:02.282 9/14/00 11:47 TCP: D=44795 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:02.286 9/14/00 11:47 TCP: D=57374 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:02.286 9/14/00 11:47 TCP: D=57375 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:02.287 9/14/00 11:47 TCP: D=57376 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:02.300 9/14/00 11:47 TCP: D=63104 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:02.301 9/14/00 11:47 TCP: D=63105 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:02.317 9/14/00 11:47 TCP: D=63106 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:02.324 9/14/00 11:47 TCP: D=38238 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:02.325 9/14/00 11:47 TCP: D=38236 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:02.327 9/14/00 11:47 TCP: D=38237 S=1024 RST WIN=0

64.14.200.154 MY.NET.6.8 60 000:00:03.003 9/14/00 11:47 TCP: D=1024 S=44797 SYN ACK=13423519 SEQ=13423520 LEN=0 WIN=4128

208.184.162.71 MY.NET.6.8 60 000:00:03.008 9/14/00 11:47 TCP: D=1024 S=11309 SYN ACK=9834138 SEQ=9834139 LEN=0 WIN=4128

64.37.200.46 MY.NET.6.8 60 000:00:03.011 9/14/00 11:47 TCP: D=1024 S=29466 SYN ACK=13182992 SEQ=13182993 LEN=0 WIN=4128

216.34.68.2 MY.NET.6.8 60 000:00:03.016 9/14/00 11:47 TCP: D=1024 S=57378 SYN ACK=13743435 SEQ=13743436 LEN=0 WIN=4128

216.35.167.58 MY.NET.6.8 60 000:00:03.023 9/14/00 11:47 TCP: D=1024 S=21285 SYN ACK=15197561 SEQ=15197562 LEN=0 WIN=4128

MY.NET.6.8 64.14.200.154 60 000:00:03.069 9/14/00 11:47 TCP: D=44797 S=1024 RST WIN=0

209.249.97.40 MY.NET.6.8 60 000:00:03.069 9/14/00 11:47 TCP: D=1024 S=65510 SYN ACK=15540600 SEQ=15540601 LEN=0 WIN=4128

MY.NET.6.8 208.184.162.71 60 000:00:03.072 9/14/00 11:47 TCP: D=11309 S=1024 RST WIN=0

MY.NET.6.8 64.37.200.46 60 000:00:03.074 9/14/00 11:47 TCP: D=29466 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:03.079 9/14/00 11:47 TCP: D=57378 S=1024 RST WIN=0

212.78.160.237 MY.NET.6.8 60 000:00:03.120 9/14/00 11:47 TCP: D=1024 S=63108 SYN ACK=9509070 SEQ=9509071 LEN=0 WIN=4128

MY.NET.6.8 209.249.97.40 60 000:00:03.133 9/14/00 11:47 TCP: D=65510 S=1024 RST WIN=0

62.26.119.34 MY.NET.6.8 60 000:00:03.152 9/14/00 11:47 TCP: D=1024 S=26590 SYN ACK=15467031 SEQ=15467032 LEN=0 WIN=4128

194.205.125.26 MY.NET.6.8 60 000:00:03.162 9/14/00 11:47 TCP: D=1024 S=38240 SYN ACK=9748940 SEQ=9748941 LEN=0 WIN=4128

MY.NET.6.8 212.78.160.237 60 000:00:03.181 9/14/00 11:47 TCP: D=63108 S=1024 RST WIN=0

MY.NET.6.8 62.26.119.34 60 000:00:03.214 9/14/00 11:47 TCP: D=26590 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:03.221 9/14/00 11:47 TCP: D=38240 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.296 9/14/00 11:47 TCP: D=33715 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.296 9/14/00 11:47 TCP: D=33717 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.296 9/14/00 11:47 TCP: D=33716 S=1024 RST WIN=0

194.213.64.150 MY.NET.6.8 60 000:00:03.305 9/14/00 11:47 TCP: D=1024 S=33719 SYN ACK=15526419 SEQ=15526420 LEN=0 WIN=4128

MY.NET.6.8 216.35.167.58 60 000:00:03.378 9/14/00 11:47 TCP: D=21281 S=1024 RST WIN=0

MY.NET.6.8 216.35.167.58 60 000:00:03.379 9/14/00 11:47 TCP: D=21282 S=1024 RST WIN=0

MY.NET.6.8 216.35.167.58 60 000:00:03.380 9/14/00 11:47 TCP: D=21283 S=1024 RST WIN=0

MY.NET.6.8 209.249.97.40 60 000:00:03.383 9/14/00 11:47 TCP: D=65506 S=1024 RST WIN=0

MY.NET.6.8 209.249.97.40 60 000:00:03.384 9/14/00 11:47 TCP: D=65507 S=1024 RST WIN=0

MY.NET.6.8 209.249.97.40 60 000:00:03.385 9/14/00 11:47 TCP: D=65508 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:03.386 9/14/00 11:47 TCP: D=11305 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:03.386 9/14/00 11:47 TCP: D=11306 S=1024 RST WIN=0

MY.NET.6.8 208.184.162.71 60 000:00:03.387 9/14/00 11:47 TCP: D=11307 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:03.388 9/14/00 11:47 TCP: D=57374 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:03.389 9/14/00 11:47 TCP: D=57375 S=1024 RST WIN=0

MY.NET.6.8 216.34.68.2 60 000:00:03.390 9/14/00 11:47 TCP: D=57376 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:03.391 9/14/00 11:47 TCP: D=63104 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:03.392 9/14/00 11:47 TCP: D=63105 S=1024 RST WIN=0

MY.NET.6.8 212.78.160.237 60 000:00:03.393 9/14/00 11:47 TCP: D=63106 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:03.400 9/14/00 11:47 TCP: D=38236 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:03.400 9/14/00 11:47 TCP: D=38237 S=1024 RST WIN=0

MY.NET.6.8 194.205.125.26 60 000:00:03.400 9/14/00 11:47 TCP: D=38238 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.402 9/14/00 11:47 TCP: D=33715 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.404 9/14/00 11:47 TCP: D=33716 S=1024 RST WIN=0

MY.NET.6.8 194.213.64.150 60 000:00:03.405 9/14/00 11:47 TCP: D=33717 S=1024 RST WIN=0

216.35.167.58 MY.NET.6.8 60 000:00:05.021 9/14/00 11:47 TCP: D=1024 S=21285 SYN ACK=15197561 SEQ=15197562 LEN=0 WIN=4128

MY.NET.6.8 216.35.167.58 60 000:00:05.024 9/14/00 11:47 TCP: D=21285 S=1024 RST WIN=0

212.78.160.237 MY.NET.6.8 60 000:00:05.107 9/14/00 11:47 TCP: D=1024 S=63108 SYN ACK=9509070 SEQ=9509071 LEN=0 WIN=4128

MY.NET.6.8 212.78.160.237 60 000:00:05.109 9/14/00 11:47 TCP: D=63108 S=1024 RST WIN=0

```
194.213.64.150 MY.NET.6.8 60 000:00:05.304 9/14/00 11:47 TCP: D=1024 S=33719 SYN ACK=15526419 SEQ=15526420 LEN=0 WIN=4128
MY.NET.6.8 194.213.64.150 60 000:00:05.306 9/14/00 11:47 TCP: D=33719 S=1024 RST WIN=0
```

These are the same packets with hex added for the first attacker. The frames from the rest of the attackers are constant with this one. Highlighted are IPID, TTL, Flags, Options.

```
----- Frame 1 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
   1 64.37.200.46      MY.DNS.6.8    60 000:00:00.000 09/14/2000 11:47:37 AM TCP: D=1024 S=29462 SYN
ACK=13182988 SEQ=13182989 LEN=0 WIN=4128
ADDR  HEX                               ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R....
0010: 00 2c 00 00 00 00 f4 06 f1 ce 40 25 c8 2e xx xx | .....4.1. .H.F~
0020: 06 08 73 16 04 00 00 c9 28 0d 00 c9 28 0c 60 12 | .....I...I...
0030: 10 20 ed d3 00 00 02 04 02 18 00 00 | ...L.....
```

```
----- Frame 2 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
   2 64.37.200.46      MY.DNS.6.8    60 000:00:00.001 09/14/2000 11:47:37 AM TCP: D=1024 S=29463 SYN
ACK=13182989 SEQ=13182990 LEN=0 WIN=4128
ADDR  HEX                               ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R....
0010: 00 2c 00 00 00 00 f4 06 f1 ce 40 25 c8 2e xx xx | .....4.1. .H.F~
0020: 06 08 73 17 04 00 00 c9 28 0e 00 c9 28 0d 60 12 | .....I...I...
0030: 10 20 ed d0 00 00 02 04 02 18 00 00 | ...}.....
```

```
----- Frame 3 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
   3 64.37.200.46      MY.DNS.6.8    60 000:00:00.001 09/14/2000 11:47:37 AM TCP: D=1024 S=29464 SYN
ACK=13182990 SEQ=13182991 LEN=0 WIN=4128
ADDR  HEX                               ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R....
0010: 00 2c 00 00 00 00 f4 06 f1 ce 40 25 c8 2e xx xx | .....4.1. .H.F~
0020: 06 08 73 18 04 00 00 c9 28 0f 00 c9 28 0e 60 12 | .....I...I...
0030: 10 20 ed cd 00 00 02 04 02 18 00 00 | .....
```

The response to the above packets. Highlighted IPID and TTL.

```
----- Frame 37 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
  37 MY.DNS.6.8      64.37.200.46  60 000:00:02.002 09/14/2000 11:47:39 AM TCP: D=29462 S=1024 RST WIN=0
ADDR  HEX                               ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 28 c8 6a 40 00 f0 06 ed 67 xx xx 06 08 40 25 | ..H .0...F~. .
0020: c8 2e 04 00 73 16 00 c9 28 0c 00 00 00 50 04 | H.....I.....&
0030: 00 00 3a f8 00 00 02 04 02 18 00 00 | ...8.....
```

```
----- Frame 38 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
  38 MY.DNS.6.8      64.37.200.46  60 000:00:02.002 09/14/2000 11:47:39 AM TCP: D=29463 S=1024 RST WIN=0
ADDR  HEX                               ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 28 c8 6b 40 00 f0 06 ed 66 xx xx 06 08 40 25 | ..H, .0...F~. .
0020: c8 2e 04 00 73 17 00 c9 28 0d 00 00 00 50 04 | H.....I.....&
0030: 00 00 3a f6 00 00 02 04 02 18 00 00 | ...6.....
```

```
----- Frame 39 -----
Frame Source Address  Dest. Address  Size Rel. Time  Abs. Time  Summary
  39 MY.DNS.6.8      64.37.200.46  60 000:00:02.003 09/14/2000 11:47:39 AM TCP: D=29464 S=1024 RST WIN=0
ADDR  HEX                               ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 28 c8 6c 40 00 f0 06 ed 65 xx xx 06 08 40 25 | ..H% .0...F~. .
0020: c8 2e 04 00 73 18 00 c9 28 0e 00 00 00 50 04 | H.....I.....&
0030: 00 00 3a f4 00 00 02 04 02 18 00 00 | ...4.....
```


1. Source of trace

This trace was from taken from my work network.

2. Detect was generated by:

This detect was generated using a NAI Sniffer detecting traffic to and from my DNS located outside of my Internet gateway router. There were filters set to discard any packets with a source or destination port of UDP 53. All packets coming in had an initial window size of 4128 and a payload length of 0.

3. Probability the source address was spoofed.

I believe that this is an example of “global load balancing” as described by Howard Kash in his “Analysis of the Type0 (Class 0) DNS that has been detected, version 1.0 “ located at:

<http://www.sans.org/newlook/resources/IDFAQ/DNS.htm>

As such it would not make sense to be using spoofed addresses.

4. Description of attack.

This is a distributed effort to try and find the optimum route to a DNS server.

5. Attack mechanism

This attack requires an exact time synchronization between attackers to succeed. The source IP addresses are registered in California as well as in Europe.

The attack mechanism is a coordinated attack from ten different hosts, using crafted syn/ack IP packets directed at a single host. All the packets have the following in common.

- a) The source TCP port is 1024(ports above 1023 are often allowed into networks).
- b) The IP Identification is equal to zero.
- c) The acknowledgment number is one less then the sequence number.
- d) IP option set – max segment size 536.

The attack starts with all ten hosts sending a set of three packets to the victim. Two seconds later the ten hosts will send the identical packets to the victim (same sequence and acknowledgment numbers as in the first set). One second later nine of the ten attackers send one more packet to the victim with the sequence number incremented by two. Two seconds later three sites send packets. The final three packets appear to be a checking sequence because they are not the prime candidates for closest service.

During the attack process the victim will start sending reset packets to the attacking computers. The victim computer will put in a valid IP Identification number and increment it by one for every reset sent to that particular host. The victim machine also sets its time to live field to the value it receives in the attack packet TTL field. (This number will thus be decremented by four in the trace as the DNS is two hops away)

To understand the true functionality of the attack consider the following table. It is sorted by IPID from lowest too highest. It contains the offset in seconds from when the initial attack packet came in for each of the ten attackers, the IP identification number of the reset packet, the time to live of the reset packet and the attacker address. Although not exact (this is the time offset of the trace machine not the time offset on the actual victim machine) the trend indicates that the IPID is incrementing by 10 for every 10 milliseconds of time. This is consistent with what we see for the highlighted addresses 209.249.97.40 and 208.184.162.71. These packets arrived and were processed by the trace machine within 3 milliseconds of each other. The responses to separate addresses have exactly the same IP identification number.

This in essence sets up a reliable method of determining the time variance of packets arriving at the victim machine.

Resets Sent

| Offset | IPID | TTL | Source |
|--------------|--------------|------------|-----------------------|
| 0.000 | 51303 | 240 | 64.37.200.46 |
| | 51304 | 240 | 64.37.200.46 |
| | 51305 | 240 | 64.37.200.46 |
| | 51306 | 240 | 64.37.200.46 |
| | 51307 | 240 | 64.37.200.46 |
| | 51308 | 240 | 64.37.200.46 |
| | 51309 | 240 | 64.37.200.46 |
| 0.017 | 51323 | 240 | 216.35.167.58 |
| | 51324 | 240 | 216.35.167.58 |
| | 51325 | 240 | 216.35.167.58 |
| | 51326 | 240 | 216.35.167.58 |
| | 51327 | 240 | 216.35.167.58 |
| | 51328 | 240 | 216.35.167.58 |
| | 51329 | 240 | 216.35.167.58 |
| 0.038 | 51343 | 239 | 209.249.97.40 |
| 0.041 | 51343 | 239 | 208.184.162.71 |
| | 51344 | 239 | 209.249.97.40 |
| | 51344 | 239 | 208.184.162.71 |
| | 51345 | 239 | 208.184.162.71 |
| | 51345 | 239 | 209.249.97.40 |
| | 51346 | 239 | 208.184.162.71 |
| | 51346 | 239 | 209.249.97.40 |
| | 51347 | 239 | 209.249.97.40 |
| | 51347 | 239 | 208.184.162.71 |
| | 51348 | 239 | 208.184.162.71 |
| | 51348 | 239 | 209.249.97.40 |
| | 51349 | 239 | 208.184.162.71 |
| | 51349 | 239 | 209.249.97.40 |
| 0.046 | 51353 | 238 | 64.14.200.154 |
| | 51354 | 238 | 64.14.200.154 |
| | 51355 | 238 | 64.14.200.154 |
| | 51356 | 238 | 64.14.200.154 |
| | 51357 | 238 | 64.14.200.154 |
| | 51358 | 238 | 64.14.200.154 |
| | 51359 | 238 | 64.14.200.154 |

| Offset | IPID | TTL | Source |
|--------|-------|-----|----------------|
| 0.053 | 51363 | 240 | 216.34.68.2 |
| | 51364 | 240 | 216.34.68.2 |
| | 51365 | 240 | 216.34.68.2 |
| | 51366 | 240 | 216.34.68.2 |
| | 51367 | 240 | 216.34.68.2 |
| | 51368 | 240 | 216.34.68.2 |
| | 51369 | 240 | 216.34.68.2 |
| 0.075 | 51373 | 233 | 212.78.160.237 |
| | 51374 | 233 | 212.78.160.237 |
| | 51375 | 233 | 212.78.160.237 |
| | 51376 | 233 | 212.78.160.237 |
| | 51377 | 233 | 212.78.160.237 |
| | 51378 | 233 | 212.78.160.237 |
| | 51379 | 233 | 212.78.160.237 |
| | 51380 | 233 | 212.78.160.237 |
| 0.115 | 51423 | 234 | 62.26.119.34 |
| | 51424 | 234 | 62.26.119.34 |
| | 51425 | 234 | 62.26.119.34 |
| | 51426 | 234 | 62.26.119.34 |
| 0.126 | 51433 | 233 | 194.205.125.26 |
| | 51434 | 233 | 194.205.125.26 |
| | 51435 | 233 | 194.205.125.26 |
| | 51436 | 233 | 194.205.125.26 |
| | 51437 | 233 | 194.205.125.26 |
| | 51438 | 233 | 194.205.125.26 |
| | 51439 | 233 | 194.205.125.26 |
| 0.150 | 51573 | 235 | 194.213.64.150 |
| | 51574 | 235 | 194.213.64.150 |
| | 51575 | 235 | 194.213.64.150 |
| | 51576 | 235 | 194.213.64.150 |
| | 51577 | 235 | 194.213.64.150 |
| | 51578 | 235 | 194.213.64.150 |
| | 51579 | 235 | 194.213.64.150 |

6. Correlations:

There are examples of IPID zero scans at the following sites:

<http://www.sans.org/y2k/021000-2300.htm>
<http://www.sans.org/y2k/021100-2300.htm>

The “global load balancing” concept is described by Howard Kash in his “Analysis of the Type0 (Class 0) DNS that has been detected, version 1.0 “ located at:

<http://www.sans.org/newlook/resources/IDFAQ/DNS.htm>

7. Evidence of specific targeting:

There are ten different machines from two separate parts of the world sending packets within a one second time frame. Yes this machine was targeted.

8. Severity

(Critical + Lethal) – (System + Network Countermeasures) = Severity
(5 + 1) – (4 + 1) = 1

Critical = 5 – DNS

Lethal = 1 – attack succeeded (only intel gained).

System = 4 – system and patches up to date.

Network = 1 – attack got through in its entirety.

9. Defensive recommendation:

This attack uses high TCP ports and so will only be stopped with specific firewall or router rule filters.

10. Question

```
Frame Source Address      Dest. Address      Size Rel. Time  Abs. Time      Summary
  1 64.37.200.46          MY.DNS.6.8        60 000:00:00.000 09/14/2000 11:47:37 AM D=1024 S=29462 SYN
ACK=13182988 SEQ=13182989 LEN=0 WIN=4128
ADDR  HEX                ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\.m^.....R.....
0010: 00 2c 00 00 00 00 00 f4 06 f1 ce 40 25 c8 2e xx xx | .....4.1. .H.F~
0020: 06 08 73 16 04 00 00 c9 28 0d 00 c9 28 0c 60 12 | .....I...I...-
0030: 10 20 ed d3 00 00 02 04 02 18 00 00                | ...L.....
```

Given this frame we can determine:

- Because the IP version is 00 that it is a crafted packet.
- This is a TCP packet.
- The sequence and acknowledgement numbers are invalid.
- None of the above.

Answer b - It would have been easier if I hadn't removed the TCP from the summary data.

Detect #3 (Netbios password guessing)

Event: IPHalfScan

| <u>Priority</u> | <u>Date</u> | <u>From</u> | <u>From Port</u> | <u>To</u> | <u>To Port</u> | <u>Information</u> |
|-----------------|-------------|-------------|------------------|-----------|----------------|--------------------|
| High | 8/19/00 | 6:28:48PM | 195.147.146.73 | 4 | MY.NET.6.197 | 80 |
| High | 8/19/00 | 6:28:48PM | 195.147.146.73 | 5 | MY.NET.6.197 | 80 |

From: MY.NET.6.197

| <u>From Port</u> | <u>Priority</u> | <u>Date</u> | <u>To</u> | <u>To Port</u> | <u>EventName</u> | |
|------------------|-----------------|-------------|-----------|----------------|------------------|-------------------------|
| 139 | Medium | 8/19/00 | 6:29:08PM | 195.147.146.73 | 1752 | Netbios_Session_Granted |
| 139 | Medium | 8/19/00 | 6:29:11PM | 195.147.146.73 | 1752 | Netbios_Session_Granted |
| 139 | Medium | 8/19/00 | 6:29:20PM | 195.147.146.73 | 1754 | Netbios_Session_Granted |
| 139 | Medium | 8/19/00 | 6:29:24PM | 195.147.146.73 | 1754 | Netbios_Session_Granted |

Event: SMB_Client_Cleartext_Password

| <u>Priority</u> | <u>Date</u> | <u>From</u> | <u>From Port</u> | <u>To</u> | <u>To Port</u> | <u>Information</u> | | |
|-----------------|-------------|-------------|------------------|-----------|----------------|--------------------|----------------|-------|
| Medium | 8/19/00 | 6:30:00PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | DOMAIN USER | |
| Medium | 8/19/00 | 6:30:04PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | PASS | SHARE |
| Medium | 8/19/00 | 6:30:07PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | DOMAIN USER | WRITE |
| Medium | 8/19/00 | 6:30:11PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | PASS | FULL |
| | | | | | | | DOMAIN USER | |
| | | | | | | | PASS | BOTH |

| | | | | | | | | |
|--------|---------|-----------|----------------|------|--------------|-----|--------------------|-------|
| Medium | 8/19/00 | 6:30:14PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | DOMAIN USER | |
| Medium | 8/19/00 | 6:29:35PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | PASS | READ |
| Medium | 8/19/00 | 6:29:42PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | DOMAIN USER | |
| Medium | 8/19/00 | 6:29:46PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | PASS ADMINISTRATOR | |
| Medium | 8/19/00 | 6:29:46PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | DOMAIN USER | GUEST |
| Medium | 8/19/00 | 6:29:49PM | 195.147.146.73 | 1754 | MY.NET.6.197 | 139 | PASS | ROOT |
| | | | | | | | DOMAIN USER | |

1. Source of trace.

This is a trace from my work network.

2. Detect generated by:

ISS Real Secure Intrusion Detection System. This detect is an example of what this IDS is good at doing.

3. Probability the source was spoofed.

User had made a connection and was actively trying to guess passwords so this was not a spoofed connection.

4. Description of the attack.

This is an attack via netbios port 139 to gain unauthorized access to the victim machine.

5. Attack mechanism:

Attacker starts off by initiating a half scan to port 80 of the victim. This would have been successful since the victim is a Web server. This would allow him to make sure the server was active without giving away any very much information about himself. Next the attacker opens a netbios session to the server. When presented with the ID and Password screen it appears that he only enters a password not an ID. He tries two commonly used passwords, fails and then retries the same process three more times. This attempt would only succeed even with the right password if the machine he was breaking was a Windows 95 machine.

6. Correlations:

This is a very common type of event.

I did find one interesting item for the IP address which looks up as :
p48s02a02.client.global.net.uk

Oxford University Bioinformatics Centre Web page statistics at:

<http://www.molbiol.ox.ac.uk/webstats/weeks/hosts/enterprise.44.total-hosts.html>

Lists this machine having 44 requests but 0 bytes transferred. This may be an indication of the type of half-scanning behavior that we saw at the beginning of this detect.

| | Requests | Bytes Transferred |
|----------------------------------|----------|-------------------|
| p48s02a02.client.global.net.uk : | 44 : | 0 |

7. Evidence of active targeting:

The fact that a half-scan was done only to the victim address and then immediately followed up by the netbios attempt indicate that the victim was targeted. Trace system had just come online so there is no evidence of previous address scans of trolling.

8. Severity

(Critical + Lethal) – (System + Network Countermeasures) = Severity
(5 + 1) – (4 + 1) = 1

Critical = 5 – Main Web Server

Lethal = 1 – No access was gained by the attacker.

System = 4 – system and patches up to date.

Network = 1 – attack got through in its entirety.

9. Defensive recommendations.

Attack could have been prevented by blocking Netbios port 139 at the gateway router.

10. Question:

Event: IPHalfScan

| Priority | Date | From | From Port | To | To Port | Information |
|----------|---------|--------------------------|-----------|--------------|---------|-------------|
| High | 8/19/00 | 6:28:48PM 195.147.146.73 | 4 | MY.NET.6.197 | 80 | |
| High | 8/19/00 | 6:28:48PM 195.147.146.73 | 5 | MY.NET.6.197 | 80 | |

Given the preceding log entry, it could have been:

- generated by normal web traffic.
- generated by a faulty TCP/IP stack.
- generated by an IDS sensor that is not overloaded.
- Both b and c.

Answer: b

Detect #4. (Qpopper with Scan)

Event: DNS_Zone_High_Port

| Priority | Date | From | From Port | To | To Port | Information |
|----------|-------------------|----------------|-----------|------------|---------|------------------|
| High | 9/11/00 4:42:50PM | 211.172.192.71 | 1877 | MY.DNS.1.7 | 53 | DOMAIN MY.DOMAIN |

Event: IPHalfScan

| Priority | Date | From | From Port | To | To Port | Information |
|----------|-------------------|----------------|-----------|-------------|---------|-------------|
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.1 | 110 | |
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.2 | 110 | |
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.5 | 110 | |
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.11 | 110 | |
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.14 | 110 | |
| High | 9/11/00 7:49:51PM | 211.172.192.71 | 110 | MY.NET.6.22 | 110 | |

(Sniffer Trace)

```
----- Frame 1 -----
Frame Source Address   Dest. Address   Size Rel. Time   Delta Time   Abs. Time   Summary
  1 [211.172.192.71] [MY.NET.6.11]   74 000:00:00.000 0.000.000   09/11/2000 10:05:32 PM TCP: D=110
S=2944 SYN SEQ=4138985339 LEN=0 WIN=32120
ADDR HEX                               ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 3c 9d 7f 40 00 31 06 4b 9c d3 ac c0 47 xx xx | ..." .....L.{F~
0020: 06 0b 0b 80 00 06 e6 f6 b3 e7 7b 00 00 00 00 a0 02 | .....>6.X#.....
0030: 7d 78 af 4e 00 00 02 04 05 b4 04 02 08 0a 0c 51 | '...+.....
0040: c4 30 00 00 00 00 01 03 03 00 | D.....

----- Frame 2 -----
Frame Source Address   Dest. Address   Size Rel. Time   Delta Time   Abs. Time   Summary
  2 [MY.NET.6.11] [211.172.192.71] 74 000:00:00.004 0.004.437   09/11/2000 10:05:32 PM TCP: D=2944
S=110 SYN ACK=4138985340 SEQ=2503948209 LEN=0 WIN=10136
ADDR HEX                               ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 3c 91 a5 40 00 fd 06 8b 75 xx xx 06 0b d3 ac | ..jv .....F~..L.
0020: c0 47 00 06 e6 0b 80 95 3f 37 b1 f6 b3 e7 7c a0 12 | {...>..n...6.X@..
```

0030: 27 98 1c 0c 00 00 01 01 08 0a 0f 37 0f eb 0c 51 | .q.....
0040: c4 30 01 03 03 00 02 04 05 b4 | D.....

----- Frame 3 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [211.172.192.71] [MY.NET.6.11] 66 000:00:00.235 0.230.740 09/11/2000 10:05:32 PM TCP: D=110
S=2944 ACK=2503948210 WIN=32120
ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 34 9d a2 40 00 31 06 4b 81 d3 ac c0 47 xx xx | ...saL.{F~
0020: 06 0b 0b 80 00 6e f6 b3 e7 7c 95 3f 37 b2 80 10 |>6.X@n.....
0030: 7d 78 f1 d8 00 00 01 01 08 0a 0c 51 c4 47 0f 37 | '.lQ.....D...
0040: 0f eb | ..

----- Frame 4 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [211.172.192.71] [MY.NET.6.11] 66 000:00:00.236 0.000.944 09/11/2000 10:05:32 PM TCP: D=110
S=2944 FIN ACK=2503948210 SEQ=4138985340 LEN=0 WIN=32120
ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 34 9d a3 40 00 31 06 4b 80 d3 ac c0 47 xx xx | ...tL.{F~
0020: 06 0b 0b 80 00 6e f6 b3 e7 7c 95 3f 37 b2 80 11 |>6.X@n.....
0030: 7d 78 f1 d7 00 00 01 01 08 0a 0c 51 c4 47 0f 37 | '.lP.....D...
0040: 0f eb | ..

----- Frame 5 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 [MY.NET.6.11] [211.172.192.71] 66 000:00:00.237 0.001.291 09/11/2000 10:05:32 PM TCP: D=2944
S=110 ACK=4138985341 WIN=10136
ADDR HEX ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 |R..\m^.....
0010: 00 34 91 a6 40 00 fd 06 8b 7c xx xx 06 0b d3 ac | ..jw@F~..L.
0020: c0 47 00 6e 0b 80 95 3f 37 b2 f6 b3 e7 7d 80 10 | {...>..n...6.X'..
0030: 27 98 47 a1 00 00 01 01 08 0a 0f 37 10 02 0c 51 | .q.~.....
0040: c4 47 | D.

----- Frame 6 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 [MY.NET.6.11] [211.172.192.71] 124 000:00:00.313 0.076.399 09/11/2000 10:05:32 PM POP3: R
PORT=2944 +OK QPOP (version 2.53) at mypop.my.netstarting.
ADDR HEX ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 |R..\m^.....
0010: 00 6e 91 a8 40 00 fd 06 8b 40 xx xx 06 0b d3 ac | .>jy F~..L.
0020: c0 47 00 6e 0b 80 95 3f 37 b2 f6 b3 e7 7d 80 18 | {...>..n...6.X'..
0030: 27 98 4d 72 00 00 01 01 08 0a 0f 37 10 0a 0c 51 | .q(.....
0040: c4 47 2b 4f 4b 20 51 50 4f 50 20 28 76 65 72 73 | D.|...&|&.....
0050: 69 6f 6e 20 32 2e 35 33 29 20 61 74 20 69 73 2d | .?>...../
0060: 6e 65 77 73 2e 67 6f 76 2e 61 62 2e 63 61 20 73 | >.....?..//.../
0070: 74 61 72 74 69 6e 67 2e 20 20 0d 0a | ./...>.....

----- Frame 7 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
7 [211.172.192.71] [MY.NET.6.11] 60 000:00:00.545 0.231.206 09/11/2000 10:05:33 PM TCP: D=110
S=2944 RST WIN=0
ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 28 9d cb 00 00 f0 06 cc 63 d3 ac c0 47 xx xx |0...L.{F~
0020: 06 0b 0b 80 00 6e f6 b3 e7 7d 00 00 00 50 04 |>6.X'.....&
0030: 00 00 65 20 00 00 00 00 00 00 00 00 00 00 00 | |

----- Frame 8 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
8 [211.172.192.71] [MY.NET.6.11] 74 005:43:34.200 20613.655.039 09/12/2000 03:49:06 AM TCP: D=110
S=3972 SYN SEQ=134875509 LEN=0 WIN=32120
ADDR HEX ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 3c 71 52 40 00 31 06 77 c9 d3 ac c0 47 xx xx |IL.{F~
0020: 06 0b 0f 84 00 6e 08 0a 09 75 00 00 00 a0 02 | ...d.>.....
0030: 7d 78 03 64 00 00 02 04 05 b4 04 02 08 0a 0c 71 | '.....
0040: 38 a8 00 00 00 00 01 03 03 00 | .y.....

----- Frame 9 -----
Frame Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
9 [MY.NET.6.11] [211.172.192.71] 74 005:43:34.206 0.006.407 09/12/2000 03:49:06 AM TCP: D=3972
S=110 SYN ACK=134875510 SEQ=947735554 LEN=0 WIN=10136
ADDR HEX ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 |R..\m^.....
0010: 00 3c 2d 49 40 00 fd 06 ef d1 xx xx 06 0b d3 ac |JF~..L.
0020: c0 47 00 6e 0f 84 38 7d 4c 02 08 0a 09 76 a0 12 | {...>.d.'<.....

```
0030: 27 98 43 a4 00 00 01 01 08 0a 0f 56 84 ba 0c 71 | .q.u.....d...
0040: 38 a8 01 03 03 00 02 04 05 b4 | .y.....
```

```
----- Frame 10 -----
Frame Source Address  Dest. Address      Size Rel. Time      Delta Time      Abs. Time      Summary
   10 [211.172.192.71] [MY.NET.6.11]      66 005:43:34.437  0.231.142      09/12/2000 03:49:07 AM TCP: D=110
S=3972      ACK=947735555  WIN=32120
ADDR  HEX                      ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 34 71 67 40 00 31 06 77 bc d3 ac c0 47 xx xx | ....L.{.F~
0020: 06 0b 0f 84 00 6e 08 0a 09 76 38 7d 4c 03 80 10 | ...d.>.....'<...
0030: 7d 78 19 70 00 00 01 01 08 0a 0c 71 38 c0 0f 56 | '.....{..
0040: 84 ba | d.
```

```
----- Frame 11 -----
Frame Source Address  Dest. Address      Size Rel. Time      Delta Time      Abs. Time      Summary
   11 [211.172.192.71] [MY.NET.6.11]      66 005:43:34.438  0.000.421      09/12/2000 03:49:07 AM TCP: D=110
S=3972 FIN ACK=947735555 SEQ=134875510 LEN=0 WIN=32120
ADDR  HEX                      ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 34 71 68 40 00 31 06 77 bb d3 ac c0 47 xx xx | ....L.{.F~
0020: 06 0b 0f 84 00 6e 08 0a 09 76 38 7d 4c 03 80 11 | ...d.>.....'<...
0030: 7d 78 19 6f 00 00 01 01 08 0a 0c 71 38 c0 0f 56 | '.....{..
0040: 84 ba | d.
```

```
----- Frame 12 -----
Frame Source Address  Dest. Address      Size Rel. Time      Delta Time      Abs. Time      Summary
   12 [MY.NET.6.11]    [211.172.192.71]  66 005:43:34.439  0.001.778      09/12/2000 03:49:07 AM TCP: D=3972
S=110      ACK=134875511  WIN=10136
ADDR  HEX                      ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 34 2d 4c 40 00 fd 06 ef d6 xx xx 06 0b d3 ac | ...< ....OF~..L.
0020: c0 47 00 6e 0f 84 38 7d 4c 03 08 0a 09 77 80 10 | {>.d.'<.....
0030: 27 98 6f 38 00 00 01 01 08 0a 0f 56 84 d1 0c 71 | .q?.....dJ..
0040: 38 c0 | .{
```

```
----- Frame 13 -----
Frame Source Address  Dest. Address      Size Rel. Time      Delta Time      Abs. Time      Summary
   13 [MY.NET.6.11]    [211.172.192.71]  124 005:43:34.520  0.080.425      09/12/2000 03:49:07 AM POP3: R
PORT=3972  +OK QPOP (version 2.53) at mypop.my.net starting.
ADDR  HEX                      ASCII
0000: 00 10 0b 49 d9 00 00 e0 1e 94 5f 00 08 00 45 00 | ....R..\m^.....
0010: 00 6e 2d 4e 40 00 fd 06 ef 9a xx xx 06 0b d3 ac | .>.+ .....F~..L.
0020: c0 47 00 6e 0f 84 38 7d 4c 03 08 0a 09 77 80 18 | {>.d.'<.....
0030: 27 98 75 09 00 00 01 01 08 0a 0f 56 84 d9 0c 71 | .q.....dR..
0040: 38 c0 2b 4f 4b 20 51 50 4f 50 20 28 76 65 72 73 | .{.|...|&.....
0050: 69 6f 6e 20 32 2e 35 33 29 20 61 74 20 69 73 2d | .?>...../.....
0060: 6e 65 77 73 2e 67 6f 76 2e 61 62 2e 63 61 20 73 | >.....?..//.../..
0070: 74 61 72 74 69 6e 67 2e 20 20 0d 0a | ./...>.....
```

```
----- Frame 14 -----
Frame Source Address  Dest. Address      Size Rel. Time      Delta Time      Abs. Time      Summary
   14 [211.172.192.71] [MY.NET.6.11]      60 005:43:34.751  0.231.602      09/12/2000 03:49:07 AM TCP: D=110
S=3972 RST WIN=0
ADDR  HEX                      ASCII
0000: 00 e0 1e 94 5f 00 00 10 0b 49 d9 00 08 00 45 00 | .\m^.....R.....
0010: 00 28 71 8e 00 00 f0 06 f8 a0 d3 ac c0 47 xx xx | .....0.8.L.{.F~
0020: 06 0b 0f 84 00 6e 08 0a 09 77 00 00 00 50 04 | ...d.>.....&.
0030: 00 00 2d cd 00 00 00 00 00 00 00 00 00 00 00 | .....
```

1. Source of trace.

This trace came from my network.

2. Detect was generated by:

This detect was generated using a combination of our ISS Realsurecure IDS and a NAI Sniffer capturing on the IP address of my POP3 server. After I saw the sniffer trace I went back and dug up the logs.

3. Probability the source address was spoofed.

By doing a zone transfer and completing the Qpop recognizance indicates that this was not a spoofed address.

4. Description of attack.

The attacker was looking to gain specific information about the version of the Qpopper that my mail server was running. With this information he would be able to determine if it was vulnerable to attack.

5. Attack mechanism

The attack started out with a zone transfer from my DNS. This would have given the attacker solid information about which IP addresses were available to take action against. The attacker then did a POP3 scan against the addresses provided by the zone transfer.

The attacker now opens a connection to the port 110 on the mail server. The server responds with a positive SYN/ACK. The attacker then completes the three-way handshake with an ACK and immediately sends a FIN packet to begin breaking down the connection. The POP server acknowledges the FIN and then turns around and pushes a banner to the attacker with the Qpop version '+OK QPOP (version 2.53) at POP.MY.DOMAIN starting.' At this point the attacker sends a reset and the connection is terminated. The attacker has what he was looking for.

6. Correlations:

http://www.cert.org/advisories/CA-98.08.qpopper_vul.html

7. Evidence of active targeting:

In order for this attack to work the attacker must make a connection to the victim and the victim must be offering the POP3 service.

8. Severity

(Critical + Lethal) – (System + Network Countermeasures) = Severity
(5 + 1) – (4 + 1) = 1

Critical = 5 – POP server

Lethal = 1 – No access was gained by the attacker.

System = 4 – system and patches up to date.

Network = 1 – attack got through in its entirety.

9. Defensive recommendations.

This attack could be prevented by closing POP3 TCP port 110 to the Internet.

The banner could be changed to something (a security message) besides the Qpop version number.

10. Question:

| Frame | Source Address | Dest. Address | Size | Rel. Time | Abs. Time | Summary |
|----------------|------------------|------------------|-----------|---------------|------------------------|-----------------------|
| 1 | [211.172.192.71] | [MY.NET.6.11] | 74 | 000:00:00.000 | 09/11/2000 10:05:32 PM | TCP: D=110 S=2944 SYN |
| SEQ=4138985339 | LEN=0 | WIN=32120 | | | | |
| 2 | [MY.NET.6.11] | [211.172.192.71] | 74 | 000:00:00.004 | 09/11/2000 10:05:32 PM | TCP: D=2944 S=110 SYN |
| ACK=4138985340 | SEQ=2503948209 | LEN=0 | WIN=10136 | | | |
| 3 | [211.172.192.71] | [MY.NET.6.11] | 66 | 000:00:00.235 | 09/11/2000 10:05:32 PM | TCP: D=110 S=2944 |
| ACK=2503948210 | WIN=32120 | | | | | |
| 4 | [211.172.192.71] | [MY.NET.6.11] | 66 | 000:00:00.236 | 09/11/2000 10:05:32 PM | TCP: D=110 S=2944 FIN |
| ACK=2503948210 | SEQ=4138985340 | LEN=0 | WIN=32120 | | | |

Given this trace we can conclude that:

- a) It is normal RPC traffic.
- b) It is abnormal RPC traffic
- c) Port information was passed to the attacker.
- d) This would only occur if the RPC port were open.

Answer c

Assignment 2 - Evaluate an Attack

Cisco HTTP denial of service attack.

This attack affects virtually all unpatched Cisco routers and switches running Cisco IOS software releases 11.1 through 12.1, inclusive that have the HTTP Service enabled.

The Cisco field notice (<http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml>) states that :

The defect appears in a function added in IOS releases 11.1 and 11.2 that parses special characters in a URI of the format "%nn" where each "n" represents a hexadecimal digit. The vulnerability is exposed when an attempt is made to browse to: "http://<router-ip>/%%". Due to the defect, the function incorrectly parses "%%" and it enters an infinite loop. A watchdog timer expires two minutes later and forces the router to crash and reload.

Of note is that this attack is independent of authentication method used by the router.

Attack Scenario

I conducted these tests using a Cisco 2503 router with 4096kbs of memory and running IOS Version 11.2(15a). This was a test router and as such did not have traffic running through it. If it was expected to route a large number of packets the buffers would have probably filled and router would have not been able to start processing packet again.

Attacks were performed using Internet Explorer 5.01 and Nessus 1.0.3
All trace's are done using an NAI (Network General) Sniffer.

For the attack I had a ping, a telnet session, and a console session running to the router.
Miscellaneous pings were also coming from various network management systems.
This attack was done using IE 5.01

| Source Address | Dest. Address | Size | Rel. Time | Summary |
|-----------------|-----------------|------|---------------|---|
| [MY.NET.42.133] | [MY.NET.6.8] | 90 | 000:03:37.438 | NTP/SNTP: Version 3 |
| [MY.NET.6.8] | [MY.NET.42.133] | 90 | 000:03:37.441 | NTP/SNTP: Version 3 |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:07.224 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:07.226 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:08.216 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:08.218 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:09.218 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:09.220 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:10.219 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:10.221 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:11.220 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:11.222 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:12.222 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:04:12.224 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 401 | 000:04:12.716 | TCP: D=80 S=1813 SYN SEQ=277784045 LEN=0 WIN=8192 |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:04:12.719 | TCP: D=1813 S=80 SYN ACK=277784046 SEQ=705381263 LEN=0 WIN=4288 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:12.719 | TCP: D=80 S=1813 ACK=705381264 WIN=8576 |
| [MY.NET.2.119] | [MY.NET.42.133] | 401 | 000:04:12.721 | HTTP: C Port=1813 GET /%% HTTP/1.1 |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:13.223 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:14.285 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:15.286 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 401 | 000:04:15.637 | HTTP: C Port=1813 GET /%% HTTP/1.1 |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:16.288 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:17.289 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:17.295 | Telnet: C PORT=1808 <0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:17.539 | Telnet: C PORT=1808 <0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:18.140 | Telnet: C PORT=1808 <0D0A0D0A0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:18.291 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:19.292 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:19.342 | Telnet: C PORT=1808 <0D0A0D0A0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:20.293 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:21.295 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 401 | 000:04:21.646 | HTTP: C Port=1813 GET /%% HTTP/1.1 |
| [MY.NET.6.130] | [MY.NET.42.133] | 98 | 000:04:21.713 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:04:21.745 | Telnet: C PORT=1808 <0D0A0D0A0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:22.296 | ICMP: Echo |
| [MY.NET.6.130] | [MY.NET.42.133] | 98 | 000:04:22.714 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:23.298 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:24.299 | ICMP: Echo |
| [MY.NET.6.130] | [MY.NET.42.133] | 98 | 000:04:24.725 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:25.300 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:04:26.302 | ICMP: Echo |

• • •

| | | | | |
|----------------|-----------------|----|---------------|------------|
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:17.958 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:18.960 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:19.961 | ICMP: Echo |

From router log: (router log time is not consistent with trace time)

%Software-forced reload

Preparing to dump core

00:15:09: %SYS-2-WATCHDOG: Process aborted on watchdog timeout, Process = HTTP Server

-Traceback= 3186658 31893A4 3183E34 31F7C86 31F7F3C 31F8084 31F8176 31F825C

Even though a reload has been issued the router will remain active for another 90 seconds.

The next record is the reply to the first ICMP echo sent to the router after the attack packet was received. The router then replies to all the frames that it has stored in it's buffers.

Note: The router is replying to the retransmissions of the attack but by this time the HTTP service is dead in the water and will not process the packets.

| | | | | |
|-----------------|-----------------|----|---------------|---|
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.833 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.835 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.836 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.838 | TCP: D=1813 S=80 ACK=277784393 WIN=3941 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.840 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.841 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.844 | TCP: D=1808 S=23 ACK=277459522 WIN=4192 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:20.844 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.846 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.848 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.849 | TCP: D=1808 S=23 ACK=277459526 WIN=4188 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:20.850 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.851 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.853 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.855 | TCP: D=1813 S=80 ACK=277784393 WIN=3941 |
| [MY.NET.42.133] | [MY.NET.6.130] | 98 | 000:06:20.856 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.858 | TCP: D=1808 S=23 ACK=277459526 WIN=4188 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:20.859 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.860 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.6.130] | 98 | 000:06:20.861 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.863 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.867 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.6.130] | 98 | 000:06:20.868 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.870 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.871 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.873 | TCP: D=1808 S=23 ACK=277459526 WIN=4188 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:20.874 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.875 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.876 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.878 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.879 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.881 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.883 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.884 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.886 | TCP: D=1813 S=80 ACK=277784393 WIN=3941 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.888 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.889 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.891 | ICMP: Echo reply |

• • •

| | | | | |
|-----------------|----------------|----|---------------|---|
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.919 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.921 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.922 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:20.924 | TCP: D=1813 S=80 ACK=277784393 WIN=3941 |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.926 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.927 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.6.131] | 98 | 000:06:20.929 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.931 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.6.131] | 98 | 000:06:20.932 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.934 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.935 | ICMP: Echo reply |

At this point the router has replied to all outstanding packets in it's buffer and has re-started normal operation. Unfortunately the core dump and reload commands have been issued so the router is shutting down.

A comparison of CPU and Memory statistics taken at this point in the attack show no marked change from before the attack started.

| | | | | |
|-----------------|-----------------|----|---------------|-----------------------------|
| [MY.NET.42.133] | [MY.NET.6.8] | 90 | 000:06:20.957 | NTP/SNTP: Version 3 |
| [MY.NET.6.8] | [MY.NET.42.133] | 90 | 000:06:20.959 | NTP/SNTP: Version 3 |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:20.962 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:20.965 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | 000:06:21.017 | Telnet: R PORT=1808 <0D0A> |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:21.017 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.2.119] | 61 | 000:06:21.021 | Telnet: R PORT=1808 ppptes# |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | 000:06:21.022 | TCP: D=23 S=1808 RST WIN=0 |
| [MY.NET.42.133] | [MY.NET.6.8] | 90 | 000:06:21.032 | NTP/SNTP: Version 3 |
| [MY.NET.6.8] | [MY.NET.42.133] | 90 | 000:06:21.035 | NTP/SNTP: Version 3 |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:21.964 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:21.966 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:22.965 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:22.968 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:23.966 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:23.972 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:24.968 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:24.970 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:25.969 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:25.971 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:26.971 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:26.973 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:27.972 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:27.974 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:28.973 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:28.975 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:29.975 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:06:29.977 | ICMP: Echo reply |
| [MY.NET.6.130] | [MY.NET.42.133] | 98 | 000:06:30.012 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.6.130] | 98 | 000:06:30.014 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:30.976 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:31.978 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:06:32.979 | ICMP: Echo |

• • •

The router is not buffering the ICMP echo requests any more. Any echo reply sent is in real time. Many echoes are not answered.

| | | | | |
|-----------------|-----------------|----|---------------|------------------|
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:00.017 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:01.018 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:02.020 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:02.023 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:03.021 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:03.319 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:04.023 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:04.291 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:05.024 | ICMP: Echo |

• • •

| | | | | |
|-----------------|-----------------|----|---------------|------------------|
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:43.079 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:44.079 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:44.388 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:45.080 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:45.082 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:46.081 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 74 | 000:07:46.083 | ICMP: Echo reply |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:47.083 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:48.084 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:49.086 | ICMP: Echo |
| [MY.NET.2.119] | [MY.NET.42.133] | 74 | 000:07:50.087 | ICMP: Echo |

The router has reinitialized and will not respond until it has come back online approximately 62 seconds later. Effective time of the denial of service attack: 4 minutes and 39 seconds.

| | | | | |
|-----------------|-----------------|-----|---------------|---|
| [MY.NET.2.119] | [MY.NET.42.133] | 98 | 000:08:52.160 | ICMP: Echo |
| [MY.NET.42.133] | [MY.NET.2.119] | 98 | 000:08:52.162 | ICMP: Echo reply |
| [MY.NET.42.133] | [MY.NET.2.79] | 124 | 000:08:52.206 | "SNMP: Trap-v1 Cold start sysUpTime, cisco.2.1.2.0" |

Targeting

A simple nmap scan with OS finger printing and port 80 specified will give enough information to target this attack. The IOS may be patched but how can you be sure unless you try.

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

```
Interesting ports on ppptest.pwss.gov.ab.ca (MY.NET.42.133):
```

```
Port      State      Service
80/tcp    open      http
```

```
TCP Sequence Prediction: Class=random positive increments
                        Difficulty=1083 (Medium)
```

```
Remote operating system guess: Cisco Router/Switch with IOS 11.2
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

Tool Comparison

A trace of Nessus performing the attack shows two differences from IE 5.01.

The first is that Nessus appears to always have options set in the initial syn packet increasing the packet length to 74 octets. The selected options are not consistent from run to run. The second is no other data besides the "get /%% HTTP/1.0" is pushed while with IE 5.01 a normal browser "GET" request is pushed.

Trace of Nessus performing the attack:

| Source Address | Dest. Address | Size | Summary |
|-----------------|-----------------|------|--|
| [MY.NET.24.201] | [MY.NET.42.133] | 74 | TCP: D=80 S=1028 SYN SEQ=4271231167 LEN=0 WIN=32120 |
| [MY.NET.42.133] | [MY.NET.24.201] | 60 | TCP: D=1028 S=80 SYN ACK=4271231168 SEQ=668706478 LEN=0 WIN=4288 |
| [MY.NET.24.201] | [MY.NET.42.133] | 60 | TCP: D=80 S=1028 ACK=668706479 WIN=32120 |
| [MY.NET.24.201] | [MY.NET.42.133] | 74 | HTTP: C Port=1028 GET /%% HTTP/1.0 |

| ADDR | HEX | ASCII |
|-------|---|------------------|
| 0000: | 00 00 0c 3b a3 de 00 00 0c 07 5e e5 08 00 45 00 |t.....;V.... |
| 0010: | 00 3c 01 4e 40 00 3d 06 a2 65 XX XX XX XX XX XX | ...+ ...s..V.IGN |
| 0020: | XX XX 04 04 00 50 fe 95 d0 c0 27 db a6 af 50 18 | .e...&.n){.w.&. |
| 0030: | 7f b8 ef fc 00 00 47 45 54 20 2f 25 25 20 48 54 | ".....GET /%% HT |
| 0040: | 54 50 2f 31 2e 30 0d 0a 0d 0a | TP/1.0.... |

Trace of Windows Internet Explorer performing the attack:

| Source Address | Dest. Address | Size | Summary |
|-----------------|-----------------|------|--|
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | TCP: D=80 S=1799 SYN SEQ=275231548 LEN=0 WIN=8192 |
| [MY.NET.42.133] | [MY.NET.2.119] | 60 | TCP: D=1799 S=80 SYN ACK=275231549 SEQ=2945175399 LEN=0 WIN=4288 |
| [MY.NET.2.119] | [MY.NET.42.133] | 60 | TCP: D=80 S=1799 ACK=2945175400 WIN=8576 |
| [MY.NET.2.119] | [MY.NET.42.133] | 401 | HTTP: C Port=1799 GET /%% HTTP/1.1 |

| ADDR | HEX | ASCII |
|-------|---|-------------------|
| 0000: | 00 00 0c 3b a3 de 00 00 0c 07 5e e5 08 00 45 00 |t.....;V.... |
| 0010: | 01 83 77 46 40 00 7e 06 00 78 XX XX XX XX XX XX | .c... .=....V..GN |
| 0020: | XX XX 07 07 00 50 10 67 b3 3d af 8b cf 68 50 18 | .e...&.....&. |
| 0030: | 21 80 bf 37 00 00 47 45 54 20 2f 25 25 20 48 54 |GET /%% HT |
| 0040: | 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 | TP/1.1..Accept: |
| 0050: | 69 6d 61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 | image/gif, image |
| 0060: | 2f 78 2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 | /x-xbitmap, imaj |
| 0070: | 65 2f 6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a | e/jpeg, image/pj |
| 0080: | 70 65 67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e | peg, application |
| 0090: | 2f 76 6e 64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 | /vnd.ms-excel, a |
| 00a0: | 70 70 6c 69 63 61 74 69 6f 6e 2f 6d 73 77 6f 72 | pplication/mswor |
| 00b0: | 64 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 | d, application/v |
| 00c0: | 6e 64 2e 6d 73 2d 70 6f 77 65 72 70 6f 69 6e 74 | nd.ms-powerpoint |
| 00d0: | 2c 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 | , /*..accept-La |
| 00e0: | 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 0d 0a 41 | nguage: en-us..A |
| 00f0: | 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 | ccept-Encoding: |
| 0100: | 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 | gzip, deflate..U |
| 0110: | 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c | ser-Agent: Mozil |

```

0120: 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 | la/4.0 (compatib
0130: 6c 65 3b 20 4d 53 49 45 20 35 2e 30 31 3b 20 57 | le: MSIE 5.01; w
0140: 69 6e 64 6f 77 73 20 4e 54 3b 20 43 4e 45 54 48 | indows NT; CNETH
0150: 6f 6d 65 42 75 69 6c 64 30 35 31 30 39 39 29 0d | romeBuild051099).
0160: 0a 48 6f 73 74 3a 20          2e          2e | .Host: XXX.XXX.X
0170: 2e          0d 0a 43 6f 6e 6e 65 63 74 69 6f | X.XXX..Connectio
0180: 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d | n: Keep-Alive...
0190: 0a          | .

```

Assignment 3 “Analyze This”

Background

This is an analysis of the intrusions into your network from the Internet as well as any unusual activity that was initiated from within your network.

Using a Snort intrusion detection system, logs were gathered for a period of forty days. The logs while incomplete offer a good representation of the type of traffic that was expected to be seen on such a large network.

For the purpose of the report, incidents are divided into two categories:

Scanning:

Information gathering such as port scanning or OS fingerprinting.

Alerts:

Unauthorized Access attempts, file retrieval attempts, buffer overflow attempts.

SCANNING

As expected the largest number of alerts were reconnaissance sweep scans of your network. These scans are used by attackers to gain insight into your network structure. Two major types of scans were seen, the first are ‘half open scans’ or Syn scans where the attacker sends an initial packet to a service port on a machine and waits for a response. The response can be in the form of a reset packet if there is a machine at that address and the service is not available or an acknowledgment packet if the service is available. A reset packet tells the attacker that there is a machine running on that IP address while an acknowledgement gives the attacker specific information on how to attack a machine. The second were ‘stealth’ scans that are designed to get by firewalls, IDS’s and blocking routers. These scans have flags set in the IP header that are either illegal or abnormal and are not considered as benign traffic. These are strictly mapping scans because they will never receive a positive response.

We saw close to four hundred different scanners and over four hundred thousand scans of your network during the report period.

Top ten scanned service ports. Total of 1736 ports scanned.

| Port Number | Scans |
|--------------------|--------|
| FTP 21 | 141623 |
| DNS 53 | 57280 |
| SubSeven 27374 | 36818 |
| Linuxconf 98 | 34631 |
| POP3 110 | 1572 |
| Gatecrasher 6970 | 1374 |
| Telnet 23 | 530 |
| Back Orifice 31337 | 473 |
| Unknown 44767 | 430 |
| Netbus 12345 | 225 |

Top ten addresses scanned. Total 29158 addresses scanned.

| Address | Scans |
|--------------|-------|
| MY.NET.70.12 | 1389 |
| MY.NET.97.83 | 1242 |
| MY.NET.253.1 | 1147 |
| MY.NET.98.11 | 1060 |
| MY.NET.181.8 | 903 |
| MY.NET.101.8 | 844 |
| MY.NET.5.4 | 526 |
| MY.NET.98.18 | 360 |
| MY.NET.60.8 | 358 |
| MY.NET.179.5 | 336 |

TOP TWENTY SCANNERS

| Scanner | Total Scans | Scanned Port |
|----------------|-------------|----------------------|
| 62.158.45.121 | 41203 | FTP - TCP 21 |
| 212.170.19.199 | 32379 | FTP - TCP 21 |
| 211.60.222.33 | 23591 | DNS - TCP 53 |
| 24.2.123.9 | 22976 | DNS - UDP 53 |
| 209.61.158.214 | 22114 | Linuxconf - TCP 98 |
| 202.0.178.98 | 20020 | DNS - TCP 53 SYN/FIN |
| 211.38.95.138 | 17977 | FTP - TCP 21 |
| 24.31.224.110 | 15900 | FTP - TCP 21 |
| 4.54.218.36 | 15846 | SubSeven - TCP 27374 |
| 193.251.15.20 | 13727 | FTP - TCP 21 |
| 24.7.157.43 | 12822 | SubSeven - TCP 27374 |
| 211.112.142.2 | 12512 | Linuxconf - TCP 98 |
| 63.29.27.192 | 8574 | FTP - TCP 21 |
| 4.54.218.182 | 5360 | SubSeven - TCP 27374 |
| 200.241.187.2 | 5148 | DNS - TCP 53 |
| 207.155.88.200 | 4786 | DNS - TCP 53 |
| 195.132.120.31 | 3260 | FTP - TCP 21 |
| 63.79.70.130 | 3056 | FTP - TCP 21 |
| 202.147.24.142 | 2634 | FTP - TCP 21 |
| 4.54.218.59 | 2306 | SubSeven - TCP 27374 |

SYN-FIN Scans

Syn-Fin scans are stealth scans used as network reconnaissance and are capable of eluding some firewalls and IDS devices. The syn-fin flag status does not occur in normal TCP/IP traffic.

There were a total of 20895 scans of your class B network coming from 18 different source addresses. Of these the most serious offender 202.0.178.98 scanned port 53 (DNS) of at least 20020 addresses on June 28 between 06:52 AM and 07:14 AM. This scan had source and destination port set to 53 (DNS) which is often allowed into networks. There appear to be gaps in the data so additional addresses may have been scanned.

Fingerprinting

Fingerprinting is the process of sending packets with invalid flags to a machine and then analyzing the responses to determine the type of operating system that is running on the victim machine. With this information the attacker can tailor an appropriate attack for the operating system. The following is a list of addresses involved in fingerprinting scans. More scans were likely but the evidence was not conclusive.

Active Fingerprinting done against your network:

| Source Address | Destination Address |
|-----------------|---------------------|
| 128.194.85.201 | MY.NET.110.57 |
| 132.205.201.12 | MY.NET.182.95 |
| 137.132.46.183 | MY.NET.217.38 |
| 141.24.132.100 | MY.NET.70.119 |
| 144.41.242.217 | MY.NET.110.57 |
| 195.11.224.126 | MY.NET.20.10 |
| 195.11.224.6 | MY.NET.20.10 |
| 195.162.198.85 | MY.NET.130.190 |
| 195.162.199.244 | MY.NET.130.65 |
| 204.214.75.93 | MY.NET.182.94 |
| 207.171.37.127 | MY.NET.100.236 |
| 208.46.220.122 | MY.NET.98.166 |
| 210.121.242.164 | MY.NET.100.236 |
| 212.238.27.23 | MY.NET.181.87 |
| 212.4.207.26 | MY.NET.100.236 |
| 213.224.84.2 | MY.NET.100.236 |
| 24.129.216.167 | MY.NET.100.236 |
| 24.147.11.125 | MY.NET.100.236 |
| 24.15.91.132 | MY.NET.110.249 |
| 24.23.33.140 | MY.NET.5.29 |
| 24.234.91.14 | MY.NET.100.236 |
| 24.24.116.143 | MY.NET.110.249 |
| 24.24.80.165 | MY.NET.181.87 |
| 24.31.235.77 | MY.NET.217.174 |
| 24.51.106.188 | MY.NET.100.236 |
| 24.66.252.137 | MY.NET.70.241 |
| 24.9.250.103 | MY.NET.217.46 |

PC Anywhere

We noticed that host MY.NET.5.37 has PC Anywhere configured to broadcast to the local subnet. You may want to reconfigure this machine so it stops setting off alarms on an IDS.

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

Alerts

| Alert Type | Number of Alerts |
|--|------------------|
| Watchlist 000220 IL-ISDNNET-990517 | 13972 |
| PING-ICMP Destination Unreachable | 12313 |
| PING-ICMP Time Exceeded | 6690 |
| Watchlist 000222 NET-NCFC | 4776 |
| WinGate | 5531 |
| Attempted Sun RPC high port access | 2318 |
| SNMP public access | 1188 |
| IDS247 - MISC - Large UDP Packet | 1170 |
| Napster | 505 |
| SMB Name Wildcard | 240 |
| Wintrino | 392 |
| SUNRPC highport access! | 20 |
| Tiny Fragments - Possible Hostile Activity | 9 |
| External RPC call | 8 |
| IDS127 - TELNET - Login Incorrect | 7 |
| site exec - Possible wu-ftpd exploit - | 5 |
| Happy 99 Virus | 4 |
| Possible wu-ftpd exploit - GIAC000623 | 2 |
| Back Orifice | 1 |

Watchlist 000220 IL-ISDNNET-990517

A watchlist has been implemented that looks at traffic from the range of addresses from 212.179.0.0 to 212.179.127.255. These addresses are administered by Bezeq International of Petach Tikvah Israel . Most of the traffic has TCP ports consistent with file transfer applications such as Napster or Gnutella. Two successful FTP sessions with data transfer were initiated from the watched network.

| time | source | destination |
|-----------------------|----------------------|------------------|
| 06/27-06:37:03.434377 | 212.179.101.218:1219 | MY.NET.181.88:21 |
| 06/27-06:40:17.913519 | 212.179.101.218:1256 | MY.NET.181.88:21 |

PING-ICMP Destination Unreachable PING-ICMP Time Exceeded

Of the 19004 alerts received over 90 percent can be attributed to attacks on other sites using MY.NET.70.121 and MY.NET.140.9 as spoofed addresses.

The other alarms have a source address originating from you network. Eight of your routers are issuing 'ICMP Destination Unreachable' messages and three routers are issuing 'ICMP Time Exceeded' messages. Although these messages are benign in and of themselves, they can be used to map networks using the 'scanning by omission' technique. Your Internet gateway router may be filtering these messages but if it is not you may want to consider such a filter.

Routers issuing 'ICMP Destination Unreachable' messages:

MY.NET.1.8
MY.NET.140.9
MY.NET.2.206
MY.NET.2.207
MY.NET.70.121
MY.NET.97.198
MY.NET.98.111
MY.NET.98.134

Routers issuing 'ICMP Time Exceeded' messages:

MY.NET.14.2
MY.NET.5.35
MY.NET.98.199

Watchlist 000222 NET-NCFC

A watchlist has been implemented that looks at traffic from the class B network 159.226.0.0. This network is administered by the Computer Network Center Chinese Academy of Sciences. There is a small amount of Web traffic and mail traffic which do not appear suspicious but there are two anomalies in the data:

1) Telnet sessions into your network:

| time | Source | destination |
|-----------------------|---------------------|---------------|
| 07/10-07:13:13.980262 | 159.226.45.109:1059 | MY.NET.6.7:23 |
| 08/04-21:25:52.918393 | 159.226.45.108:1028 | MY.NET.6.7:23 |

2) There are a 702 alerts that show a 159.226.*.* address with a source port of 111 going to eight addresses on your network. The destination port addresses are all above 39000. This appears to be the result of an attack on the machines on the 159.226.*.* network with spoofed addresses within your address range.

Wingate

A Wingate server is a proxy server that is designed to allow a host outside of a firewall to connect transparently and securely through the firewall. A total of 5554 Wingate alerts were issued. Most of these appear as scans or proxy checking done by IRC servers. If IRC is accepted practice at you site then no more action needs to be taken.

Hosts MY.NET.253.105 and MY.NET.97.101 appear to be running as proxy servers. If these machines are not proxy servers then please investigate.

Host MY.NET.60.11 may have port 1080 open but is not responding to requests.
Host MY.NET.60.8 may have port 1080 open but is not responding to requests.
Host MY.NET.60.16 may have port 1080 open but is not responding to requests.

Attempted Sun RPC high port access

There were 2318 'Attempted Sun RPC high port access' alerts. Of these 2301 were false positives with signatures that can be attributed to four hosts on your network accessing AOL ICQ sites. Of the four hosts, MY.NET.217.126 registered the most hits with 2240 from August 3 to August 5. If ICQ is accepted practice at you site then no more action needs to be taken.

The seventeen other alerts appear to have been reconnaissance scans against four hosts.

| source | destination |
|---------------|---------------|
| 207.230.26.34 | MY.NET.1.8 |
| 212.62.17.145 | MY.NET.1.10 |
| 24.3.45.104 | MY.NET.115.95 |
| 64.27.29.2 | MY.NET.1.8 |
| 24.4.129.16 | MY.NET.115.91 |

SNMP Public Access

Machine MY.NET.101.192 has numerous access attempts from your internal network via SNMP port 161 using the default read community string 'public'. Since there are no SNMP access attempts to any other machine on your network from the Internet (it is safe to assume that such attempts would be logged because they generally attempt with the 'public' string) there is no breach of security. Please be advised that changing the allowable SNMP read access string is recommended.

IDS247 - MISC - Large UDP Packet

Starting at 08/05-18:30:03 and continuing for thirty minutes a large number of packets were sent from 211.40.176.214 UDP port 29536 to MY.NET.98.179 UDP port 6970. This has all the earmarks of some sort of streaming data. The source address is in Korea and resides on a compromised network according to the Mirkforce / Hack reporting site. (<http://hackreport-us.magicnet.org/>) It would be prudent to make sure the machine is secure.

Napster

Napster is a program that allows the downloading compressed music files to and from the Internet. Generally the songs that are traded on Napster are copyrighted which could raise legal issues for your company if these files are stored on your computers.

Legalities aside there are also security considerations for allowing this practice to continue. You are allowing someone on the Internet access to your computers. For more information see the following Web sites:

<http://archives.neohapsis.com/archives/bugtraq/2000-03/0277.html>
<http://www.zdnet.com/zdnn/stories/news/0,4586,2605466,00.html?chkpt=zdhnews01>

The following is a list of machines that have communicated on the Internet using the port signature of the Napster application:

| IP Address |
|----------------|
| MY.NET.130.65 |
| MY.NET.201.2 |
| MY.NET.97.204 |
| MY.NET.162.200 |
| MY.NET.201.2 |
| MY.NET.98.136 |
| MY.NET.97.204 |
| MY.NET.10.89 |
| MY.NET.217.158 |

SMB Name Wildcard

Most of this traffic was internal to your network and is not unusual. Of note is that there were attempts from two external IP addresses that had virtually the same time stamps. The times are so close that it is inconceivable that these are real addresses. More than likely these addresses are spoofed and the spoofing machine is on the same network as the IDS sensor.

| time | type | source | destination |
|-----------------------|-------------------|---------------------|-------------------|
| 08/04-16:23:34.611008 | SMB Name Wildcard | 132.201.232.167:137 | MY.NET.15.127:137 |
| 08/04-16:23:34.611091 | SMB Name Wildcard | 208.16.237.10:137 | MY.NET.15.127:137 |
| 08/04-16:23:42.770412 | SMB Name Wildcard | 208.16.237.10:137 | MY.NET.15.127:137 |
| 08/04-16:23:42.770527 | SMB Name Wildcard | 132.201.232.167:137 | MY.NET.15.127:137 |
| 08/04-16:23:44.293564 | SMB Name Wildcard | 132.201.232.167:137 | MY.NET.15.127:137 |
| 08/04-16:23:44.293784 | SMB Name Wildcard | 208.16.237.10:137 | MY.NET.15.127:137 |
| 08/04-16:23:50.888340 | SMB Name Wildcard | 132.201.232.167:137 | MY.NET.15.127:137 |
| 08/04-16:23:50.888445 | SMB Name Wildcard | 208.16.237.10:137 | MY.NET.15.127:137 |

Wintrino

Wintrino is a Distributed denial of service attack that operates on compromised Windows computers. There were 392 alarms indicating Wintrino activity. All but three of these alarms had source ports indicating legitimate services SMTP and Authentication. The other three were from IP address 204.137.237.8 which was running a scan against MY.NET.97.112 (for Wintrino as well as SUNRPC highport access and Wingate). Timeframe of this scan was 07/12-03:50:48 - 04:23:15

SUNRPC highport access!

IP Address 205.188.3.205 appears to have succeeded in setting up a connection to port 32771 on MY.NET.98.145. If this is not legitimate traffic MY.NET.98.145 should be investigated.

Tiny Fragments

Tiny fragments may be indicative of stealth activity. There were three incidences comprised of nine alerts. The most significant came from 63.236.34.174 towards MY.NET.1.8 with three packets sent and then two minutes later another three packets. Of all the incidences this appears to be the most malicious.

External RPC call

There is some evidence of active targeting of IP address MY.NET.6.15 on TCP port 111. There were eighteen alerts involving MY.NET.6.15, of these ten were part of larger sweep scans involving TCP ports 21 and 53, the other eight were directed at TCP port 111. No other IP address on you network had attempts on port 111. The initial attempt from 204.176.11.10 is a probe for port 111. Five seconds later there are connection attempts. This indicates that the RPC service may be running on the victim machine. We suggest verifying that the RPC service is running on MY.NET.6.15 and shutting it down if it is not required.

| time | source | destination |
|-----------------------|--------------------|-----------------|
| 06/27-01:01:09.457499 | 207.30.189.91:851 | MY.NET.6.15:111 |
| 06/27-01:01:09.499540 | 207.30.189.91:851 | MY.NET.6.15:111 |
| 06/30-01:59:39.580221 | 204.176.11.10:111 | MY.NET.6.15:111 |
| 06/30-01:59:44.793285 | 204.176.11.10:1556 | MY.NET.6.15:111 |
| 06/30-01:59:44.819258 | 204.176.11.10:1556 | MY.NET.6.15:111 |
| 06/30-01:59:44.819365 | 204.176.11.10:1016 | MY.NET.6.15:111 |
| 06/30-01:59:44.848794 | 204.176.11.10:1016 | MY.NET.6.15:111 |
| 06/30-01:59:44.902365 | 204.176.11.10:1016 | MY.NET.6.15:111 |

IDS127 TELNET - Login Incorrect

All seven alerts came within a time frame of just under 25 minutes. All of the addresses that failed in a logon attempt except one originated on the East coast of the United States. There are two possible explanations for this. First that a group of people tried to access three of your servers. The second and I believe more likely explanation is that one user signed on to multiple dial-up accounts and purposely logged on incorrectly to audit the security system. The system logs from the victim servers as well as extended Snort IDS data may give further clues to this incident.

| time | source | destination |
|-----------------------|-----------------|----------------------|
| 08/05-18:37:37.745999 | MY.NET.60.11:23 | 208.198.33.168:1024 |
| 08/05-18:47:13.982488 | MY.NET.60.8:23 | 207.172.151.22:1674 |
| 08/05-18:47:20.888622 | MY.NET.60.8:23 | 207.172.151.22:1674 |
| 08/05-18:53:09.934812 | MY.NET.60.8:23 | 151.198.144.196:1026 |
| 08/05-18:54:24.387218 | MY.NET.60.11:23 | 24.6.134.169:3452 |
| 08/05-18:56:11.376893 | MY.NET.60.8:23 | 63.24.126.127:1197 |
| 08/05-18:59:23.821523 | MY.NET.6.7:23 | 38.30.171.95:1223 |

Possible wu-ftpd exploit

A buffer overrun exists in wu-ftpd versions prior to 2.6.1. Due to improper bounds checking, SITE EXEC may enable remote root execution, without having any local user account required. Please check servers for version number and patch date.

| time | type | source | destination |
|-----------------------|---|-----------------|-------------------|
| 06/30-16:33:57.773279 | site exec - Possible wu-ftpd exploit - GIAC000623 | 151.164.223.20 | MY.NET.99.16:21 |
| 06/30-16:34:00.037398 | Possible wu-ftpd exploit - GIAC000623 | 151.164.223.20 | MY.NET.99.16:21 |
| 06/30-16:35:11.406398 | site exec - Possible wu-ftpd exploit - GIAC000623 | 151.164.223.20 | MY.NET.144.59:21 |
| 06/30-16:35:13.560305 | site exec - Possible wu-ftpd exploit - GIAC000623 | 151.164.223.20 | MY.NET.144.59:21 |
| 06/30-16:35:13.626498 | Possible wu-ftpd exploit - GIAC000623 | 151.164.223.20 | MY.NET.144.59:21 |
| 07/19-03:53:00.191779 | site exec - Possible wu-ftpd exploit - GIAC000623 | 212.35.163.64:1 | MY.NET.100.165:21 |
| 07/29-12:07:56.525800 | site exec - Possible wu-ftpd exploit - GIAC000623 | 211.38.95.138:3 | MY.NET.156.127:21 |

Happy 99 Virus

Four alerts were found for the Happy 99 virus going to your SMTP servers. If you are not running up to date mail server virus scanning software you should investigate further.

| time | type | source | destination |
|-----------------------|----------------|---------------------|-------------------|
| 07/11-19:28:57.652242 | Happy 99 Virus | 200.223.11.7:4836 | MY.NET.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.6.47:25 |

Back Orifice

Back Orifice is a trojan that that allows remote control of a computer by an attacker. There was a single alert with both the destination and source ports associated with back orifice. The destination address MY.NET.100.130 does not show any alerts that would be associated with having the trojan active. To be on the safe side you can scan the machine with a tool such as Diamond Computer Systems Pty. Ltd. BO2K scanner (<http://www.diamondcs.com.au>).

| time | type | source | destination |
|-----------------------|--------------|----------------------|----------------------|
| 07/12-17:16:32.897041 | Back Orifice | 202.159.46.234:31338 | MY.NET.100.130:31337 |

Conclusion:

There was no evidence to suggest any major security breaches on your network. The amount and type of traffic seen can be considered normal for a network of this size. While there do appear to be some areas of concern, specified in the report, on the whole your network seems secure at this time. The twenty or so alerts discussed in this report are part of a rulebase that currently contains the signatures for over eleven hundred types of scans or attacks.

Installation and monitoring of a permanent Intrusion Detection System.

When installing a permanent IDS we will optimize the tool for your network. This will give the greatest security coverage with the least amount of false alerts. We will also be able to notify you of security events in a timely manner and update the IDS rules whenever a new type of intrusion comes to light.

Assignment #4 – Analyses Process

For the analyses of the data I downloaded all of the files.

I then imported the snort alert files into an MS Access database table parsing the data into four fields.

| ID | time | type | source | destination |
|----|-----------------------|----------------------|----------------------|--------------------|
| 1 | 07/14-00:03:20.138859 | WinGate 1080 Attempt | 168.120.16.250:55067 | MY.NET.97.135:1080 |
| 2 | 07/14-00:04:04.529242 | WinGate 1080 Attempt | 203.155.129.248:4387 | MY.NET.97.135:1080 |
| 3 | 07/14-00:16:55.256883 | WinGate 1080 Attempt | 203.155.129.248:4524 | MY.NET.97.135:1080 |
| 4 | 07/14-00:25:31.576247 | WinGate 1080 Attempt | 168.120.16.250:55837 | MY.NET.97.135:1080 |
| 5 | 07/14-00:25:34.952853 | WinGate 1080 Attempt | 168.120.16.250:55837 | MY.NET.97.135:1080 |
| 6 | 07/14-00:26:17.478113 | WinGate 1080 Attempt | 203.155.129.248:4653 | MY.NET.97.135:1080 |

I ran a duplicate query on the alert type (excluding the spp scan alerts) in the table to give me an idea of the alerts and numbers involved.

| type Field | NumberOfDup |
|--|-------------|
| SYN-FIN scan! | 20067 |
| Watchlist 000220 IL-ISDNNET-990517 | 13972 |
| PING-ICMP Destination Unreachable | 12313 |
| PING-ICMP Time Exceeded | 6690 |
| Watchlist 000222 NET-NCFC | 4776 |
| WinGate 8080 Attempt | 3291 |
| Attempted Sun RPC high port access | 2318 |
| WinGate 1080 Attempt | 2240 |
| SNMP public access | 1188 |
| IDS247 - MISC - Large UDP Packet | 1170 |
| Napster 8888 Data | 323 |
| SMB Name Wildcard | 240 |
| GIAC 000218 VA-CIRT port 34555 | 206 |
| GIAC 000218 VA-CIRT port 35555 | 186 |
| Napster 7777 Data | 170 |
| Null scan! | 98 |
| NMAP TCP ping! | 46 |
| SUNRPC highport access! | 20 |
| Napster Client Data | 12 |
| Queso fingerprint | 11 |
| Tiny Fragments - Possible Hostile Activity | 9 |
| External RPC call | 8 |
| IDS127 - TELNET - Login Incorrect | 7 |
| site exec - Possible wu-ftpd exploit - | 5 |
| IDS246 - MISC - Large ICMP Packet | 5 |
| Happy 99 Virus | 4 |
| Possible wu-ftpd exploit - GIAC000623 | 2 |
| PING-ICMP Source Quench | 1 |
| Probable NMAP fingerprint attempt | 1 |
| FTP-bad-login | 1 |
| Back Orifice | 1 |
| IDS08 - TELNET - daemon-active | 1 |

I then removed all of the alerts for scans and uninteresting traffic and consolidated the rest by type (i.e. all napster alerts) to come up with the alerts table I used in the report.

Then I created another table with all of the 'spp_portscan: End of portscan' type of data and parsed out the IP address. This allowed me to count scan numbers and host numbers.

| ID | Fi | Field2 | Fiel | Field4 | Field5 | Field6 | Field7 | Field8 | Field9 | Field10 | Fi |
|----|----|---------|------|----------|--------------|-----------------|-----------------|---------------|--------|---------|----|
| 2 | 83 | 7/14/06 | 34 | 33.56018 | spp_portscan | End of portscan | 213.33.21.43 | TOTAL HOSTS 1 | TCP 2 | UDP | 0 |
| 4 | 25 | 7/14/11 | 9 | 15.83668 | spp_portscan | End of portscan | 212.58.186.14 | TOTAL HOSTS 1 | TCP 1 | UDP | 0 |
| 6 | 38 | 7/14/12 | 39 | 55.58966 | spp_portscan | End of portscan | 24.232.51.137 | TOTAL HOSTS 1 | TCP 2 | UDP | 0 |
| 8 | 45 | 7/14/13 | 49 | 0.680576 | spp_portscan | End of portscan | MY.NET.1.3 | TOTAL HOSTS 2 | TCP 0 | UDP | 10 |
| 10 | 47 | 7/14/14 | 49 | 17.61770 | spp_portscan | End of portscan | 213.132.131.108 | TOTAL HOSTS 1 | TCP 1 | UDP | 0 |

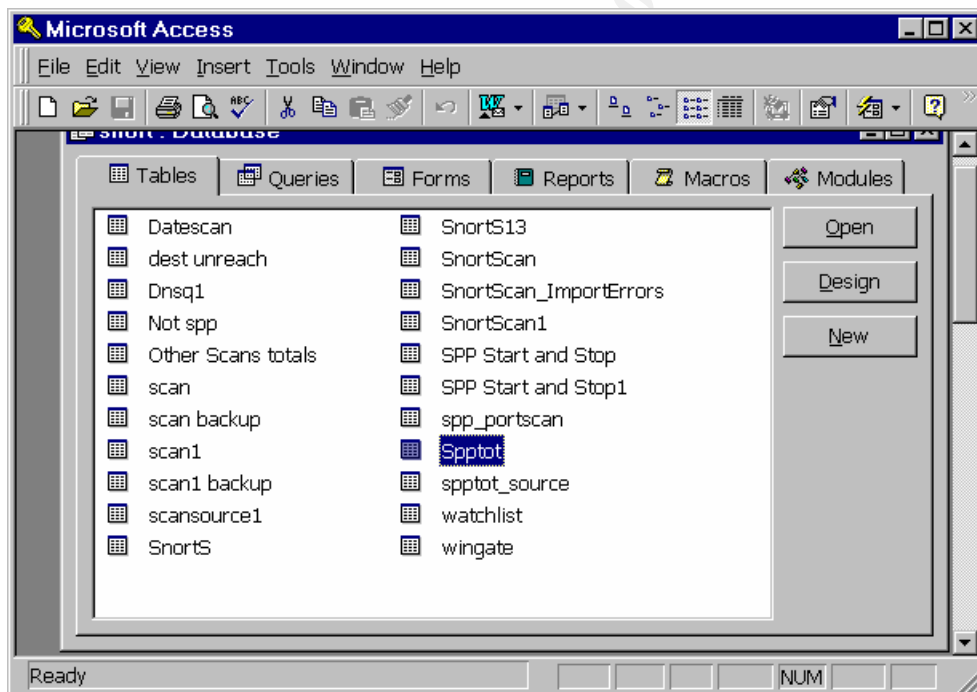
Then I imported the scan files into a table and parsed out the IP address, the port, the type, the flags, and the explanation field.

This allowed me to run queries on all of the pertinent fields.

| Fi | Fiel | Fie | Fie | Fiel | F | Field7 | Field | Fiel | Field10 | Field11 | Field12 | Field13 | Field14 |
|----|------|-----|-----|------|---|----------------|-------|------|--------------|---------|---------|----------|------------|
| 1 | Jul | 27 | 1 | 38 | | 205.188.247.19 | 21 | -> | MY.NET.97.21 | 3991 | UNKNOWN | *1**R*** | RESERVEDBI |
| 2 | Jul | 27 | 2 | 3 | | 211.60.222.33 | 1323 | -> | MY.NET.1.0 | 53 | SYN | **S***** | |
| 3 | Jul | 27 | 2 | 3 | | 211.60.222.33 | 1324 | -> | MY.NET.1.1 | 53 | SYN | **S***** | |
| 4 | Jul | 27 | 2 | 3 | | 211.60.222.33 | 1327 | -> | MY.NET.1.4 | 53 | SYN | **S***** | |
| 5 | Jul | 27 | 2 | 3 | | 211.60.222.33 | 1328 | -> | MY.NET.1.5 | 53 | SYN | **S***** | |

From these tables I was then able to run multiple types of queries to form associations between individual fields. If required I would create new tables and further parse them to understand an alert.

Here is a screen print of the tables created in the analyses.



PING-ICMP Destination Unreachable

PING-ICMP Time Exceeded

Alerts with a MY.NET source address must have been routers. The alerts with the two MY.NET destination addresses had no corresponding scan alerts so it was the result of a spoofed attack elsewhere.

Watchlist 000222 NET-NCFC

Nothing out of the ordinary except for the telnets and the response to the port 111 scans. No scans initiated from inside the network.

Wingate

Ran totals on the destination addresses and a few showed excess activity from different source addresses.

| destination Field | NumberOfDup |
|---------------------|-------------|
| MY.NET.253.105:8080 | 2912 |
| MY.NET.60.11:1080 | 305 |
| MY.NET.60.8:1080 | 262 |
| MY.NET.60.16:1080 | 160 |
| MY.NET.97.101:8080 | 136 |

Attempted Sun RPC high port access

Almost all had source port of 4000 indicating benign activity. Wrote up the others.

SNMP Public Access

All alerts from internal addresses to one specific internal address. No external addresses in any of the alerts.

IDS247 - MISC - Large UDP Packet

All alerts came from one external address. Google search showed up the Mirkforce site.

Napster

Not enough packets to get a radio jingle down let alone a full length song.

SMB Name Wildcard

Weird time signature pops out at you. Something fishy going on here.

Wintrino

GIAC 000218 VA-CIRT port 34555

GIAC 000218 VA-CIRT port 35555

Looks mostly like mail or authentication. Keyed on unusual source ports.

SUNRPC highport access!

Only alerts for the one source address. Did not show up under the 'attempted sun ...' rule. May be looking for UDP.

Tiny Fragments

Alerts show 63.236.34.174 tried twice with a linear time frame. Could have been a bad stack but might as well check it out.

External RPC call

Quick scan from 204.176.11.10 without a retry then attempts with retries. Looks like he found something.

IDS127 TELNET - Login Incorrect

This one is goofy. Who in their right mind would have 5 different current ISP's?????

Possible wu-ftpd exploit

Easiest thing to do is to check the servers version number.

Happy 99 Virus

Check the virus scanners.

Back Orifice

Single packet with BO signature. No other activity from the source or destination IP addresses. Probably a test.

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

Upcoming Training

Click Here to
{Get CERTIFIED!}



| | | | |
|---|------------------------|-----------------------------|----------------|
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, Australia | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| SANS vLive - SEC503: Intrusion Detection In-Depth | SEC503 - 201709, | Sep 11, 2017 - Oct 18, 2017 | vLive |
| Baltimore September 2017 - SEC503: Intrusion Detection In-Depth | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | vLive |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS London September 2017 | London, United Kingdom | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS Scottsdale SEC503 | Scottsdale, AZ | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| SANS October Singapore 2017 | Singapore, Singapore | Oct 09, 2017 - Oct 28, 2017 | Live Event |
| Community SANS Boston SEC503 | Boston, MA | Oct 09, 2017 - Oct 14, 2017 | Community SANS |
| Community SANS Ottawa SEC503 | Ottawa, ON | Oct 16, 2017 - Oct 21, 2017 | Community SANS |
| SANS Seattle 2017 | Seattle, WA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS San Diego 2017 | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | vLive |
| SIEM & Tactical Analytics Summit & Training | Scottsdale, AZ | Nov 28, 2017 - Dec 05, 2017 | Live Event |
| SANS Cyber Defense Initiative 2017 | Washington, DC | Dec 12, 2017 - Dec 19, 2017 | Live Event |
| SANS OnDemand | Online | Anytime | Self Paced |
| SANS SelfStudy | Books & MP3s Only | Anytime | Self Paced |