Global Information Assurance Certification Paper

Detect 1

```
18May2000 15:01:30 drop domain-tcp 207.173.117.12  my-class-b.51.97    tcp 73
18May2000 15:01:30 drop domain-tcp 207.173.117.12  my-class-b.51.98    tcp 73
18May2000 15:01:30 drop domain-tcp 207.173.117.12  my-class-b.51.100   tcp 73
18May2000 15:01:30 drop domain-tcp 207.173.117.12  my-class-b.51.101   tcp 73
.
.
.
18May2000 15:01:31 drop domain-tcp 207.173.117.12  my-class-b.52.23    tcp 73
18May2000 15:01:31 drop domain-tcp 207.173.117.12  my-class-b.52.24    tcp 73
18May2000 15:01:31 drop domain-tcp 207.173.117.12  my-class-b.52.25    tcp 73
18May2000 15:01:31 drop domain-tcp 207.173.117.12  my-class-b.52.26    tcp 73
.
.
```

1. Source of Trace
   a. My network

2. Detect was generated by:
   a. Check Point FireWall 1 Logs
   b. Explanation of fields
   18May2000[date] 15:01:30[timestamp] drop[action] domain-tcp[service] 207.173.117.12[source] my-class-b.51.97[destination] tcp[protocol] 73[rule]

3. Probability the source address was spoofed.
   a. Low. IP address was traced to a company in Arizona. The address belongs to a block owned by USWest.

4. Description of Attack
   a. Attacker was scanning hosts for DNS zone transfer
   b. This is a reconnaissance attack

5. Attack Mechanism
   a. Attacker attempted to loop through our class B address for vulnerable DNS servers. Notice the sequential nature of the scanned hosts.

6. Correlations:
   a. This attack was also reported by our vendor ISS and described it as IP HalfScan.
   b. This was also described in SANS2000 class in San Jose by S. Northcutt.

7. Evidence of active targeting
   a. This attack was generated at our US site

8. Severity
   a. (critical + Lethal) – (System + Net Countermeasures) = Severity
   b. (5+4) – (5+5) = 1

9. Defensive recommendations
    a. Defenses are fine as seen by the actions taken by the Firewall.

10. Multiple choice question:
    This trace is best described as
        a. IP Half Scan
        b. Smurf attack
        c. Host scanning
        d. Port scanning
    Answer : HalfScan

Detect 2

22May2000 23:59:02 accept domain-tcp 195.116.231.162 external-dns-server tcp 58
22May2000 23:59:04 accept domain-tcp 195.116.231.162 external-dns-server tcp 58
23May2000 0:00:02 accept domain-tcp 195.116.231.162 external-dns-server tcp 58
23May2000 0:00:04 accept domain-tcp 195.116.231.162 external-dns-server tcp 58
.
.
.

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Check Point FireWall 1
    b. Explanation of fields
    0[record #] 22May2000[date] 23:59:02[timestamp] accept[action] domain-tcp[service] 195.116.231.162[source] my-internal-nt-dns-server[destination] tcp[protocol] 58[rule]

3. Probability the source address was spoofed.
    a. Low. IP address was traced to an ISP in Poland.

4. Description of Attack
    a. Attacker was attempting to do a zone transfer from our external dns server
5. Attack mechanism
    a. Attacker attempted to do a zone transfer from our extern dns continuously hoping to gain a window of vulnerability.

6. Correlations:
    a. This attack was described in the SAN2000 Intrusion Detection Class in San Jose..

7. Evidence of active targeting
    b. This attack was generated at our US site with a very specific target

8. Severity
    a. (critical + Lethal) – (System + Net Countermeasures) = Severity
    b. (5+3) – (5+0) = 3

9. Defensive recommendations
    a. Proper defensive mechanism was in place since the zone transfer requests were rejected by the DNS server..

10. Multiple choice question:
    This trace is best described as
    a. Zone Transfer Attack
    b. Port Scanning
    c. Denial of Service
    d. Smurf Attack
    Answer : a.

Detect 3

24May2000 23:59:07 drop domain-udp 63.97.240.3 Unix-dns-server udp 73
24May2000 23:59:27 drop domain-udp 63.97.240.3 NT-dns-server udp 73
24May2000 23:59:32 drop domain-udp 63.97.240.3 Unix-dns-server udp 73
24May2000 23:59:37 drop domain-udp 63.97.240.3 NT-dns-server udp 73
.
.
.
25May2000 11:36:11 drop domain-udp 63.97.240.3 Unix-dns-server udp 73
25May2000 11:36:16 drop domain-udp 63.97.240.3 NT-dns-server udp 73

1. Source of trace
    a. My network

2. Detect was generated by
    a. Check Point FireWall 1 logs
    b. Explanations of fields
    24May2000[date] 23:59:07[timestamp] drop[action] domain-udp[service]
    63.97.240.3[source] Unix-dns-server[destionation] udp[protocol] 73[rule]

3. Probabiltiy of source address was spoofed
    a. Low. After ISP was contacted, attacked stopped. Address belonged to a block owned by Innova.net in Brazil.

4. Description of attack

Attacker was alternating his attacks between the Unix and NT internal DNS servers every 5-20 seconds using UDP port 53 for domain name queries.

5. Attack mechanism
   The attack worked by continuously querying the two internal dns servers hoping for a window of vulnerability thus returning useful information. This can be viewed as a reconnaissance for internal hosts.

6. Correlations
   a. This incident was correlated with our vendor ISS's detection device. Attacker was traced to
   b. Attack ceased after ISP was notified

7. Evidence of active targeting
   This attack was especially troubling as attacker gained knowledge of our internal DNS servers. The attack was narrow and specific.

8. Severity
   a. (critical + Lethal) – (System + Net Countermeasures) = severity
   b. (5 + 5) – (5 + 5) = 0

9. Defensive measures
   Defenses are fined as evidenced by the dropped packets.

10. Multiple choice questions:
    The trace is best described as:
    a. Information gathering
    b. Host scanning
    c. Looking for Trojan
    d. Zone transfer
    Answer : a

Detect 4

08:41:10.618565 194.204.12.94.54641 > my-class-b.206.27.33116: R 0 : 0 (0) ack 330459
08:41:16.160735 194.204.12.94.4675 > my-class-b.32.78.62465 : R 0 : 0 (0) ack 93311185
08:41:17.310642 194.204.12.94.33555 > my-class-b.211.63.50213 : R 0 : 0 (0) ack 130164
08:41:24.708704 194.204.12.94.37165 > my-class-b.211.100.27656 : R 0 : 0 (0) ack 29467
08:41:32.113738 194.204.12.94.60986 > my-class-b.127.85.48873 : R 0 : 0 (0) ack 255698
08:41:49.033203 194.204.12.94.62312 > my-class-b.109.113.19178: R 0 : 0 (0) ack 23743
08:42:44.936225 194.204.12.94 62312 > my-class-b.114.0.14692: R 0 : 0 (0) ack 2080387
.
.
.
11:26:06.621016 194.204.12.94.621016 > my-class-b.44.59.7583: R 0 : 0 (0) ack 16145167

11:26:09.763500 194.204.12.94.763500 > my-class-b.254.79.5111: R 0 : 0 (0) ack 1775089
11:26:12.154449 194.204.12.94.3179 > my-class-b.81.39.15417: R 0 : 0 (0) ack 21447030
11:26.25.111342 194.204.12.94.6562 > my-class-b.118.118.12147: R 0 : 0 (0) ack 121476

1. Source of trace
   a. My network

2. Detect was generated by:
   a. tcpdump on firewall
   b. Explanation of fields:
   08:41.10.618565[timestamp] 194.204.12.94.54641[source] my-class-b.206.27.33116[target] R[reset] 0 : 0 (0) sequence number ack [ack flag] 330459[sequence#]

3. Probability the source address was spoofed.
   Low. The address was traced to an ISP in Estonia.

4. Description of Attack
   a. Attacker was scanning our class B network fast and furious for several hours.
   b. This is a reconnaissance attack.

5. Attack mechanism
   Attacker crafted these packets hoping the router would return error messgages from the router if any of the hosts existed.

6. Correlations:
   This attack was described in Stephen Northcutt's class in SANS2000 in San Jose.

7. Evidence of active targeting
   a. The attack was generated at this site.

8. Severity
   a. (critical + lethal) – (system + net countermeasures) = severity
   b. (5 + 4) – (3+5) = 1

9. Defensive recommendations
   a. These packets were dropped by the Firewall. Defenses are therefore fine.

10. Multiple choice question:
    This trace is best described as:
    a. Host scanning
    b. TCP port scanning
    c. Reset Network Scanning
    d. Denial of Service
    Answer: c

Detect 5

08:40:51.826971 205.243.56.59.137 > my-class-b.200.25.137: udp 50 (ttl 125, id 23299)
08:40:51.985040 205.243.56.59.137 > my-class-b.248.185..137: udp 50 (ttl 125, id 24325)
08:41:13.413883 205.243.56.59.137 > my-class-b.200.25.137: udp 50 (ttl 125, id 45573)
08:41:13.559059 205.243.56.59.137 > my-class-b.248.185.137: udp 50 (ttl 125, id 45873)
.
.
.
11:10:57.919093 205.243.56.59.137 > my-class-b.200.25.137: udp 50 (ttl 125, id 32315)
11:10:58.971591 205.243.56.59.137 > my-class-b.248.185.137: udp 50 (ttl 125, id 32819)
11:11:58.001238 205.243.56.59.137 > my-class-b.200.25.137: udp 50 (ttl 125, id 49204)
11:11:58.670653 205.243.56.59.137 > my-class-b.248.185 .137:udp 50 (ttl 125, id 49468)
.
.
.

1. Source of trace
   a. My network

2. Detect was generated by:
   a. tcpdump on my firewall
   b. Explanation of fields:
   08:40:51.826971[timestamp] 205.243.56.59.137[source address, port#] my-class-b.200.25.137[destination address, port#] udp [protocol]

3. Probability the source address was spoofed
   Low. It was traced to Sprintlink.

4. Description of attack:
   a. Information gathering using Netbios name service

5. Attack mechanism:
   a. Attack is reconnaissance to gather information of our internal network. UDP 137 is used for name resolution by Windows systems. Based on the length and frequency of the attack, it can be deduced that attacker was hoping that targets existed and they were Windows NT systems and offered windows for exploitation later..

6. Correlations:
   a. This scanning technique was discussed in Stephen Northcutt's class during the SANS200 Intrusion Detection Track in San Jose.

7. Evidence of active targeting:
   a. Attacker is targeting known NT servers

8. Severity:

a. (critical + lethality) – (system + net countermeasures) = severity
b. –1

9. Defensive recommendations:
Defenses are fine since these packets were dropped by our firewall.

10. Multiple choice question:
This trace can best be described as:
a. Denial of service
b. Port scanning
c. Information gathering
d. Trolling for trojan
Answer: c

Detect 6

26May2000 8:38:23 accept udp-137 206.243.56.71 my-class-b.200.25 udp
26May2000 8:41:08 accept udp-137 206.243.56.71 my-class-b.200.25 udp
26May2000 8:41:11 accept udp-137 206.243.56.71 my-class-b.200.25 udp
26May2000 8:41:12 accept udp-137 206.243.56.71 my-class-b.200.24 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.193.7 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.63.76 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.101.23 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.20.127 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 10.122.1.1 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.92.63 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.108.246 udp
26May2000 8:41:24 accept udp-137 206.243.56.71 my-class-b.175.249 udp
.
.
.
26May2000 8:41:24 accept udp-139 206.243.56.71 my-class-b.200.24 udp
26May2000 8:41:32 accept udp-139 206.243.56.71 my-class-b.200.24 udp
26May2000 8:41:36 accept udp-139 206.243.56.71 my-class-b.248.201 udp
26May2000 8:41:47 accept udp-139 206.243.56.71 10.121.195.168 udp
26May2000 8:43:07 accept udp-137 206.243.56.71 my-class-b.200.25 udp
26May2000 8:43:07 accept udp-137 206.243.56.71 my-class-b.248.185 udp
26May2000 8:43:07 accept udp-137 206.243.56.71 my-class-b.200.30 udp
.
.
.

1. Source of trace
a. My network

2. Detect was generated by:
   a. Check Point Firewall 1 logs
   b. Explanation of fields:
   26May2000 8:41:12[timestamp] accept[action] udp-137[service]
   206.243.56.71[source address] my-class-b.200.25[destination address] udp[protocol]

3. Probability the source address was spoofed:
   Low. Address was part of block owned by AT&T

4. Description of attack:
   a. It appeared attacker was scanning for an NT host to return desired info.
   b. It also appeared that attacker attempted to authenticate himself to several hosts.
   c. The log did not show what rule allowed these packets through the firewall. Quite troublesome!

5. Attack mechanism
   a. Attack appeared to be first information gathering
   b. Then attempted to break in.
   c. Attacker resumed information gathering again using the once attacked hosts again

6. Correlations:
   a. Unable to corrrelate with any known techniques discussed in SANS2000
   b. Further investigation revealed source address assigned to one of the company's programming partners
   c. It also revealed that the partner came over a VPN connection, thus explaining the lack of rule field in the logfile
   d. The bizarre behavior was caused by a programming error

7. Evidence of active targeting:
   a. 'Attacker' appeared to target known NT servers

8. Severity:
   0

9. Defensive recommendation
   None. This is a false positive even though the behavior did raise a red flag at first glance

10. Multiple choice question
    This trace was best described as:
    a. Information gathering
    b. Host scanning
    c. Misbehaved program
    d. None of the above
    Answer: c

Detect 7

12:40:02.499603 internal.prober.2242 > dns.server.21: S 70038:70038 (0) win 8192 <mss 1460> (DF)
12:40:02 511476 internal.prober.2244 > dns.server.23: S 70053:70053 (0) win 8192 <mss 1460> (DF)
12:40:02.526359 internal.prober.2245 > dns.server.25: S 70055:70055 (0) win 8192 <mss 1460> (DF)
12:40:02.544662 internal.prober.2247 > dns.server.53: S 70072:70072 (0) win 8192 <mss 1460> (DF)
12:40:02.653195 internal.prober.2258 > dns.server.5190: S 70147:70147 (0) win 8192 <mss 1460> (DF)
12:40:02:979899 internal.prober.2245 > dns.server.25: S 70055:70055 (0) win 8192 <mss 1460> (DF)
12:40:03.143545 internal.prober.2258 > dns.server.5190: S 70147:70147 (0) win 8192 <mss 1460> (DF)
12:40:03.440793 internal.prober.2245 > dns.server.25: S 70055:70055 (0) win 8192 <mss1460> (DF)
12:40:03.642447 internal.prober.2258 > dns.server.25: S 70147:70147 (0) win 8192 <mss 1460> (DF)

1. Source of trace
   a. My network

2. Detect was generated by:
   a. tcpdump running on my dns server
   b. Explanation of fields:
   12:40:02.499603[timestamp] internal.prober.2242[source address,port#] dns.server.21[destination address,port#] S[syn flag] 70038:70038[sequence #] (0)[# of bytes] win 8192 [window size] <mss 1460>[ethernet] (DF)[do not fragment flag]

3. Probability IP address was spoofed
   Low. nslookup produced valid name. It was traced to a workstation inside the company.

4. Attack mechanism
   a. Attacker was probing for answers from selected well known ports, except for port 5190.

5. Description of attack
   a. Attacker crafted probing packets as evidenced by the sameness of the sequence numbers. Only selected well known ports such as ftp, telnet, sendmail, domain lookup.
   b. A cursory look indicated that attacker might be looking for a trojan (port 5190).
   c. The time sequence indicated these packets were generated programmatically.

6. Correlations
   a. The scan was similar to many port scanning discussed in SANS2000. However, it also revealed some subtle differences.
   b. Upon investigation, it was traced to a workstation technician running a probing software called "Port Looker". It turned out that he was looking for machines that have antivirus software and Dr. Watson. He was curious as to what the dns server would return. He was quite sheepish when I confronted him with the trace..

7. Evidence of active targeting
   Actvities were generated within our site.

8. Severity
   2

9. Defensive recommendation
   This is an internal probing. Apparently, the prober did obtain information he was looking for. Recommend that all unnecessary services be turned off.

10. Multiple choice question
    This trace can best be described as:
    a. Port Scanning
    b. Looking for trojan
    c. DOS
    d. None of the above
    Answer: a

Detect 8

09:12:00.019967 arp who-has my-class-b.12.10 tell 63.97.240.3
09:12:00.020972 arp who-has my-class-b.12.11 tell 63.97.240.3
09:12:00.021860 arp who-has my-class-b.12.12 tell 63.97.240.3
09:12:00.022856 arp who-has my-class-b.12.13 tell 63.97.240.3
09:12:00.023858 arp who-has my-class-b.12.14 tell 63.97.240.3
09:12:00.024856 arp who-has my-class-b.12.15 tell 63.97.240.3
09:12:00.025858 arp who-has my-class-b.12.16 tell 63.97.240.3
09:12:00.026854 arp who-has my-class-b.12.17 tell 63.97.240.3
09:12:00.027858 arp who-has my-class-b.12.18 tell 63.97.240.3
09:12:02.405418 arp who-has my-class-b.12.19 tell 63.97.240.3
.
.
.
09:12:13.182489 arp who-has my-class-b.12.100 tell 63.97.240.3
09:12:13.183702 arp who-has my-class-b.12.101 tell 63.97.240.3

09:12:13.183773 arp who-has my-class-b.12.102 tell 63.97.240.3
09:12:13.184223 arp who-has my-class-b.12.103 tell 63.97.240.3
09:12:13.220330 arp who-has my-class-b.12.104 tell 63.97.240.3
09:12:13.221139 arp who-has my-class-b.12.105 tell 63.97.240.3
09:12:13.222322 arp who-has my-class-b.12.106 tell 63.97.240.3
09:12:13.222924 arp who-has my-class-b.12.107 tell 63.97.240.3
09:12:13.224923 arp who-has my-class-b.12.108 tell 63.97.240.3
09:12:13:225118 arp who-has my-class-b.12.109 tell 63.97.240.3
.
.
.

1. Source of trace
   a. My network

2. Detect was generated by:
   a. tcpdump on my firewall
   b. Explanation of fields:
   09:12:00.019967[timestamp] arp who-has my-class-b.12.10 tell 63.97.240.3[broadcast asking for host that has that ip address to return the mac address]

3. Probability the source address is spoofed
   Low. The address block was registered to uu.net

4. Description of Attack
   a. Network mapping

5. Attack mechanism
   a. Attack is reconnaissance. This technique provides valuable information regarding identity of existing hosts which replies to the broadcast.
   b. It is very apparent that this was generated by a program that just spits out broadcast fast and furious. It emitted roughly 50-60 broadcast messages every second.
   c. This technique is not very subtle and not very elegant. It could easily flooded our network if we did not have a firewall dropping these packets.
6. Correlations
   a. This scan was discussed in SANS2000 in San Jose as this scan goes host by host looking to map the infracstructure of our network.

7. Evidence of active targeting
   a. It was targeting our class-b address space.

8. Severity
   -1

9. Defensive recommendations
   Defenses are fine as these packets were dropped by the firewall

10. Multiple choice question
This trace was best described as:
a. Denial of Service
b. Network scanning
c. Information gathering
d. Buffer overflow
Answer: b

Detect 9

```
10:31:48.896733 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 20736)
10:31:48.898616 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 20992)
10:33:08.151994 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 26112)
10:33:08.153982 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 26368)
10:35:08.566135 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 37376)
11:05:18.662940 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 44035)
11:07:19.294792 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 48131)
.
.
.

11:09:19.876343 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 52483)
11:09:19.876891 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 52739)
11:11:21.198551 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 56579)
11:11:21.199100 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 56835)
11:13:21.694408 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 62723)
11:13:21.695628 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 62979)
11:15:22.637052 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 2052)
11:15:22.637679 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 2308)
11:17:22.752159 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 9476)
11:17:22.757284 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 9732)
11:19:23.175846 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 12292)
11:19:23.176729 24.132.32.161.2078 > 146.240.229.70.2078: udp 20 (ttl 15,
id 12548)
```

1. Source of detect
   a. My network

2. Detect generated by
   a. tcpdump on my firewall
   b. Explanation of fields
      11:07:19.296180[timestamp] 24.132.32.161.2078[source address.port#] > my-class-b.229.70.2078[destination address.port#]: udp[protocol] 20[header size] (ttl 15, id 48387)

3. Probability ip address is spoofed
   Low. Using dig and whois, the ip address was traced to a company called Unisource in the Netherlands.

4. Description of attack
   a. Attacker attempted to contact internal workstation via udp protocol, using port 2078.
   b. An alternate answer is that this might not be an attack. It might be caused by a program anomaly.

5. Attack mechanism
   a. Attack was slow and consistent. Every 2 minutes, 2 udp contacts were attempted
   b. Ephemeral port 2078 were used for both source and destination addresses
   c. Attack continued for over 48 minutes

6. Correlations
   a. This signature was not discussed in the SANS2000 Intrusion Detection class
   b. Searching SANS archive and the internet did not turn up any mention of Port 2078 attack
   c. Using nmap to scan internal host revealed that it is an NT4 workstation, and port 135 was the only active port
   d. Contacting the user revealed that he is not an active internet user. The only internet usage, besides web browsing is ICQ
   e. The activity was not detect again
   f. Sent detect to Stephen Northcutt. He indicated he has not seen any kind of attack using port 2078.

7. Evidence of active targeting
   a. The machine targeted exists and it did not appear to be a ramdom act.

8. Severity
   -1.

9. Defensive recommendation
   None as these packets were dropped by the firewall.

10. Multiple choice question

This trace can best be described as

a. Trolling for trojan
b. Host scanning
c. Wrong address
d. None of the above

Answer: d

Detect 10

```
16:23:30.007763 203.129.242.39 > ns2: icmp: echo request (DF) (ttl 39, id
28436)
16:23:30.008297 203.129.242.39 > ns2: icmp: echo request (DF) (ttl 38, id
28436)
16:23:30.008598 203.129.242.39.36697 > ns2.80: . ack 2137793358 win 4096
(DF) (ttl 47, id 28437)
16:23:30.008777 ns2 > 203.129.242.39: icmp: echo reply (DF) (ttl 255, id
22678)
16:23:30.009453 203.129.242.39.36697 > ns2.80: . ack 1 win 4096 (DF) (ttl
46, id 28437)
16:23:30.009575 ns2 > 203.129.242.39: icmp: echo reply (DF) (ttl 254, id
22678)
16:23:30.009795 ns2.80 > 203.129.242.39.36697: R 2137793358:2137793358(0)
win 0 (DF) (ttl 46, id 22679)
16:23:30.010311 ns2.80 > 203.129.242.39.36697: R 2137793358:2137793358(0)
win 0 (DF) (ttl 45, id 22679)
16:23:30.341705 203.129.242.39.43798 > ns2.737: S 2319528110:2319528110(0)
win 8760 <mss 1460> (DF) (ttl 255, id 28438)
16:23:30.344922 203.129.242.39.43799 > ns2.571: S 2319658851:2319658851(0)
win 8760 <mss 1460> (DF) (ttl 255, id 28439)
16:23:30.345193 203.129.242.39.43800 > ns2.2232: S
2319660351:2319660351(0) win 8760 <mss 1460> (DF) (ttl 255, id 28440)
16:23:30.348579 203.129.242.39.43798 > ns2.737: S 2319528110:2319528110(0)
win 8760 <mss 1460> (DF) (ttl 254, id 28438)
16:23:30.348975 ns2.737 > 203.129.242.39.43798: R 0:0(0) ack 2319528111
win 0 (DF) (ttl 254, id 22680)
16:23:30.352133 203.129.242.39.43799 > ns2.571: S 2319658851:2319658851(0)
win 8760 <mss 1460> (DF) (ttl 254, id 28439)
16:23:30.352601 203.129.242.39.43800 > ns2.2232: S
2319660351:2319660351(0) win 8760 <mss 1460> (DF) (ttl 254, id 28440)
16:23:30.353023 ns2.737 > 203.129.242.39.43798: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 22680)
16:23:30.353222 ns2.571 > 203.129.242.39.43799: R 0:0(0) ack 2319658852
win 0 (DF) (ttl 254, id 22681)
16:23:30.353392 ns2.2232 > 203.129.242.39.43800: R 0:0(0) ack 2319660352
win 0 (DF) (ttl 254, id 22682)
16:23:30.353728 203.129.242.39.43801 > ns2.774: S 2319734689:2319734689(0)
win 8760 <mss 1460> (DF) (ttl 255, id 28441)
.
.
.
16:23:35.017641 203.129.242.39.45301 > ns2.982: S 2417441763:2417441763(0)
win 8760 <mss 1460> (DF) (ttl 254, id 29977)
```

```
16:23:35.017993 ns2.982 > 203.129.242.39.45301: R 0:0(0) ack 2417441764
win 0 (DF) (ttl 254, id 24186)
16:23:35.018512 ns2.982 > 203.129.242.39.45301: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 24186)
16:23:35.023832 ns2.347 > 203.129.242.39.45304: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 24189)
16:23:35.040446 203.129.242.39.45305 > ns2.887: S 2417658330:2417658330(0)
win 8760 <mss 1460> (DF) (ttl 255, id 29981)
16:23:35.041225 203.129.242.39.45305 > ns2.887: S 2417658330:2417658330(0)
win 8760 <mss 1460> (DF) (ttl 254, id 29981)
16:23:35.041709 203.129.242.39.45306 > ns2.283: S 2417681168:2417681168(0)
win 8760 <mss 1460> (DF) (ttl 255, id 29982)
16:23:35.042458 203.129.242.39.45306 > ns2.283: S 2417681168:2417681168(0)
win 8760 <mss 1460> (DF) (ttl 254, id 29982)
16:23:35.042703 ns2.887 > 203.129.242.39.45305: R 0:0(0) ack 2417658331
win 0 (DF) (ttl 254, id 24190)
16:23:35.042929 ns2.283 > 203.129.242.39.45306: R 0:0(0) ack 2417681169
win 0 (DF) (ttl 254, id 24191)
16:23:35.043180 203.129.242.39.45307 > ns2.676: S 2417742513:2417742513(0)
win 8760 <mss 1460> (DF) (ttl 255, id 29983)
16:23:35.043350 ns2.887 > 203.129.242.39.45305: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 24190)
16:23:35.043652 ns2.283 > 203.129.242.39.45306: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 24191)
16:23:35.044159 203.129.242.39.45307 > ns2.676: S 2417742513:2417742513(0)
win 8760 <mss 1460> (DF) (ttl 254, id 29983)
16:23:35.044399 ns2.676 > 203.129.242.39.45307: R 0:0(0) ack 2417742514
win 0 (DF) (ttl 254, id 24192)
16:23:35.044940 ns2.676 > 203.129.242.39.45307: R 0:0(0) ack 1 win 0 (DF)
(ttl 253, id 24192)
16:23:35.045862 203.129.242.39.45308 > ns2.6000: S
2417755796:2417755796(0) win 8760 <mss 1460> (DF) (ttl 255, id 29984)
16:23:35.046715 203.129.242.39.45308 > ns2.6000: S
2417755796:2417755796(0) win 8760 <mss 1460> (DF) (ttl 254, id 29984)
16:23:35.047065 203.129.242.39.45309 > ns2.415: S 2417762485:2417762485(0)
win 8760 <mss 1460> (DF) (ttl 255, id 29985)
16:23:35.047212 ns2.6000 > 203.129.242.39.45308: S
3349365413:3349365413(0) ack 2417755797 win 33580 <mss 1460> (DF) (ttl
255, id 24193)
16:23:35.049721 203.129.242.39.45308 > ns2.6000: . ack 1 win 8760 (DF)
(ttl 254, id 29986)
16:23:35.049749 203.129.242.39.45310 > ns2.1503: S
2417839863:2417839863(0) win 8760 <mss 1460> (DF) (ttl 255, id 29987)
16:23:35.049763 ns2.415 > 203.129.242.39.45309: R 0:0(0) ack 2417762486
win 0 (DF) (ttl 253, id 24194)
16:23:35.049780 203.129.242.39.45310 > ns2.1503: S
2417839863:2417839863(0) win 8760 <mss 1460> (DF) (ttl 254, id 29987)
16:23:35.110903 203.129.242.39.45308 > ns2.6000: R
2417755797:2417755797(0) win 8760 (DF) (ttl 255, id 29992)
16:23:35.112074 203.129.242.39.45308 > ns2.6000: R
2417755797:2417755797(0) win 8760 (DF) (ttl 254, id 29992)
```

1. Source of trace
   a. My network

2. Trace was generated by

a. tcpdump
b. Explanation of fields:
16:23:30.007763[timestamp] 203.129.242.39[source addr.port] > ns2[my external dns server]: icmp: echo request[ping] (DF)[do not frag] (ttl 39, id 28436)[time to live and id #]

3. Probability address is spoofed
Low. IP address was traced to a company called Abnic Corp in India.

4. Description of attack
   a. Attack was scanning for ports for OS signature and other port information gatherings
   b. OS fingering and scanning for active ports

5. Attack mechanism
   a. Attacker ping my external DNS server
   b. Attacker send syn packets addressed to various ports under consideration in a relatively random fashion
   c. Attack was fast and furious. The entire scan was finished within 2 minutes.

6. Correlations
   a. This is the classic nmap scan described in Stephen Northcutt's SANS2000 class.

7. Evidence of active targeting
The attack was directed at my external DNS server.

8. Severity
2.

9. Defensive recommendation
This server is in located in our DMZ. It's recommended that this server should be hardened so that it cannot be used as a springboard to our internal network.

10. Multiple choice question
This trace is best described as:
   a. Port scanning
   b. NMAP
   c. Denial of Service
   d. Buffer overflow
Answer: b

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
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 Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	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
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
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 Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced