GIAC Intrusion Detection Curriculum
Practical Assignment for SNAP San Jose

10 Network Detects with Analysis

Derek L. Cherneski - 15 June 2000

Detect #1 - 5 June 2000

```
23:43:14.469110 208.220.120.13.53 > x.x.x.1.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.470394 208.220.120.13.53 > x.x.x.2.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.471618 208.220.120.13.53 > x.x.x.3.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.472840 208.220.120.13.53 > x.x.x.4.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.474063 208.220.120.13.53 > x.x.x.5.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.475336 208.220.120.13.53 > x.x.x.6.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.479570 208.220.120.13.53 > x.x.x.7.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.496038 208.220.120.13.53 > x.x.x.8.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.515857 208.220.120.13.53 > x.x.x.9.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
23:43:14.536492 208.220.120.13.53 > x.x.x.10.53: SF 892767610:892767610(0) win 1028 (ttl 26, id 39426)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low. The IP address traces back to venus.e-helpnet.com.

4. Description of attack:
   A very fast Syn-Fin scan of all our class-C addresses targeting DNS servers. This scan covered 2,234 addresses between 23:43:14 & 23:46:48. It also cycled through 48 distinct sequence numbers, and would change after 50 occurrences.

5. Attack mechanism:
   Syn-Fin scanning of DNS servers.

6. Correlations:
   This attack occurred only once toward our network, no further detects have been encountered. This scan is very similar to the scan that Erik Fitchner reported in http://www.sans.org/y2k/032000.htm.

7. Evidence of active targeting:
   Yes, this scanned more than 30 of our class C's.

8. Severity: (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (5 + 4) - (5 + 5) = -1
   Criticality: 5 - DNS severs
   Lethality: 4 - DoS
   System Countermeasures: 5 - Current NOS, all patches applied
   Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
   Attack was blocked by firewall.

10. Multiple choice question:
    This detect shows:
    a) DNS Inverse Mapping
    b) DNS Zone Transfer
    c) DNS Buffer Overflow
    d) DNS Server to Server host query
    Answer: C

Detect #2 - 5-12 June 2000

```
{5 June 2000}
01:56:48.126822 200.250.113.60.3944 > my.class.c.1.53: 43531 inv_q+ [b2&3=0x980] A? . (27) (ttl 49, id
32040)
                              4500 0037 7d28 0000 3111 fc02 c8fa 713c
                              xxxx xxxx 0f68 0035 0023 b872 aa0b 0980
                              0000 0001 0000 0000 0000 0100 0100 007a
                              6900 0404 0302
{6 June 2000}
23:50:01.419095 200.250.113.60.2183 > another.class.c.1.53: 42847 inv_q+ [b2&3=0x980] A? . (27) (ttl 49, id
51732)
                              4500 0037 ca14 0000 3111 b216 c8fa 713c
                              xxxx xxxx 0887 0035 0023 c4ff a75f 0980
                              0000 0001 0000 0000 0000 0100 0100 007a
                              6900 0404 0302

{12 June 2000)
14:23:22.618931 200.250.113.247.2825 > yetanother.class.c.1.53: 9145 inv_q+ [b2&3=0x980] A? . (27) (ttl 49,
id 62007)
                              4500 0037 f237 0000 3111 8a38 c8fa 71f7
                              xxxx xxxx 0b09 0035 0023 4669 23b9 0980
                              0000 0001 0000 0000 0000 0100 0100 007a
                              6900 0404 0302

{12 June 2000)
16:01:43.290300 200.250.113.247.2660 > stillmore.class.c.1.53: 12052 inv_q+ [b2&3=0x980] A? . (27) (ttl 49,
id 60809)
                              4500 0037 ed89 0000 3111 8ce6 c8fa 71f7
                              xxxx xxxx 0a64 0035 0023 39b3 2f14 0980
                              0000 0001 0000 0000 0000 0100 0100 007a
                              6900 0404 0302

{12 June 2000)
16:51:52.392280 200.250.113.247.2983 > thelast.class.c.1.53: 14312 inv_q+ [b2&3=0x980] A? . (27) (ttl 49, id
20715)
                              4500 0037 50eb 0000 3111 2885 c8fa 71f7
                              xxxx xxxx 0ba7 0035 0023 2e9c 37e8 0980
                              0000 0001 0000 0000 0000 0100 0100 007a
                              6900 0404 0302
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:

Medium, nslookup on 200.250.113.60 reports port60.foz.net, this ip address is not within reach of pinging yet a traceroute returns netserver.foznet.com.br and 200.250.6.25 as the correct ip. When I ran nslookup on the second ip address 200.250.113.247 I was given port247.foz.net which was quite pingable.

4. Description of attack:
The attacker in this case is softly sending a packet to the first address in five of our class C network addresses in the hopes of hitting a real live DNS server at these addresses.

5. Attack mechanism:
This directed search asks a DNS server to find a hostname associated with a given supplied argument. None of the addresses targeted ever had DNS servers…

6. Correlations:
The Domain Inverse Query was described in detail in the SANS course material (IDS 2.3; Pg 230). More details are available in CVE-1999-0010 & CERT CA-98.05

7. Evidence of active targeting:
This appears to be a very specific and subtle scan that spanned 7 days with only five packets delivered.

8. Severity:
(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
(5 + 4) - (5 + 5) = -1
Criticality: 5 - DNS severs
Lethality: 4 - DoS
System Countermeasures: 5 - Current NOS, all patches applied
Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
Attack was blocked by firewall.

10. Multiple choice question:
This detect shows:
a. DNS Inverse Mapping
b. DNS Zone Transfer
c. DNS Buffer Overflow
d. DNS Server to Server host query
Answer: a

Detect #3 - 9 June 2000

```
05:46:47.685845 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 110, id 57733)
05:46:49.171860 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 11910)
05:46:50.667664 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 30598)
06:26:42.058075 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 36173)
06:26:43.561284 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 110, id 51533)
06:26:45.099182 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 110, id 846)
06:12:59.534954 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 14580)
06:46:15.305642 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 110, id 13986)
06:46:16.792407 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 19362)
06:46:18.292729 195.58.198.158.137 > my.network.C.130.137: udp 50 (ttl 109, id 27042)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low, no host info through nslookup, however IANA ipv4 reference list shows address space to be RIPE NCC-Europe so off I went to lookup http://www.ripe.net/cgi-bin/whois?query=195.58.198.130 … the United Kingdom.

4. Description of attack:
   A host in the UK is trying to resolve a NETBIOS name of a workstation on our network, with no luck.

5. Attack mechanism:
   Wrong number

6. Correlations:
   The evidence in this trace appears to support the wrong number determination detailed in the SANS course materials (IDS 2.4/2.5; Pg 309)

7. Evidence of active targeting:
   Not likely, however may be worth keeping a eye on connections to this internal host in the future.

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (2 + 1) - (5 + 5) = -7
   Criticality: 2 - User Workstation
   Lethality: 1 - Very unlikely to succeed
   System Countermeasures: 5 - Current NOS, all patches applied
   Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
   Attack was blocked by firewall.

10. Multiple choice question:
   This detect shows:
   a. Stealthy Socks scan
   b. Wrong number
   c. Stealthy network mapping
   d. NETBIOS DoS attack

Answer: b

Detect #4 - 11 June 2000

```
21:30:38.328448 194.80.106.143.761 > network.backbone.0.111: S 1942310694:1942310694(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40345)
21:30:38.330375 194.80.106.143.762 > network.backbone.2.111: S 1942406563:1942406563(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40365)
21:30:38.331742 194.80.106.143.763 > network.backbone.1.111: S 1942471763:1942471763(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40405)
21:30:38.332812 194.80.106.143.764 > network.backbone.5.111: S 1942526859:1942526859(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40455)
```

```
21:30:38.335276 194.80.106.143.765 > network.backbone.6.111: S 1942553860:1942553860(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40485)
21:30:38.370278 194.80.106.143.766 > network.backbone.3.111: S 1942557105:1942557105(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40505)
21:30:38.387980 194.80.106.143.767 > network.backbone.8.111: S 1942566126:1942566126(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40535)
21:30:38.460130 194.80.106.143.768 > network.backbone.4.111: S 1942693452:1942693452(0) win 8760 <mss 1460>
(DF) (ttl 240, id 40605)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low. nslookup points to a host called virology3.nimr.mrc.ac.uk = 194.80.106.143 and this also confirms with http://www.ripe.net/cgi-bin/whois?query=194.80.106.143 as it does appear to be a medical research facility.

4. Description of attack:
   This appears to be a RPC port probe attempting to access our SUN Remote Procedure Call (rpcbind, and portmapper) services

5. Attack mechanism:
   Network vulnerability scanning/mapping; potential vulnerability as per CVE-1999-0168 in our environment

6. Correlations:
   This trace type was covered in the SANS course material (IDS 2.4/2.5; Pg 269)

7. Evidence of active targeting:
   This appears to be an automated scan, not likely directly targeted on our network.

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (4 + 3) - (5 + 5) = -3
   Criticality: 4 - SUN database sever
   Lethality: 3 - User access
   System Countermeasures: 5 - Current NOS, all patches applied
   Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
   Attack was blocked by firewall.

10. Multiple choice question:
    This detect shows:
    a. An ICMP portscan
    b. An probe for SGI workstations
    c. A SUN RPC probe
    d. An REXEC probe
    Answer: c

Detect #5 - 11 June 2000

```
05:17:10.889764 212.150.30.68.137 > my.class.c.1.137: udp 50 (ttl 113, id 24365)
05:17:12.369700 212.150.30.68.137 > my.class.c.1.137: udp 50 (ttl 113, id 24621)
05:17:13.885492 212.150.30.68.137 > my.class.c.1.137: udp 50 (ttl 113, id 24877)
05:17:24.390440 212.150.30.68.137 > my.class.c.2.137: udp 50 (ttl 113, id 29485)
05:17:26.191437 212.150.30.68.137 > my.class.c.2.137: udp 50 (ttl 113, id 29741)
...
06:01:58.541108 212.150.30.68.137 > my.class.c.253.137: udp 50 (ttl 113, id 34358)
06:01:59.722873 212.150.30.68.137 > my.class.c.253.137: udp 50 (ttl 113, id 34614)
06:02:07.240847 212.150.30.68.137 > my.class.c.254.137: udp 50 (ttl 113, id 35894)
06:02:09.051298 212.150.30.68.137 > my.class.c.254.137: udp 50 (ttl 113, id 36150)
06:02:10.236452 212.150.30.68.137 > my.class.c.254.137: udp 50 (ttl 113, id 36406)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low, no host info through nslookup, however IANA ipv4 reference list shows address space to be RIPE NCC-Europe so off I went to lookup http://www.ripe.net/cgi-bin/whois?query=212.150.30.68 … Israel, very interesting.

4. Description of attack:
   Scanning one entire class C address for NetBIOS in-use services

5. Attack mechanism:
   This may be a recon exercise in information gathering as described in SANS course material (IDS 2.4/2.5; Pg 293)

6. Correlations:
   This trace occurred for this one occasion only… no further incidents on other monitored networks. No response received from emails sent out.

7. Evidence of active targeting:
   This attack was specifically targeted at this one subnet.

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (2 + 1) - (5 + 5) = -7
   Criticality: 2 - W95/98 Hosts
   Lethality: 1 - Attack is very unlikely to succeed
   System Countermeasures: 5 - Current NOS, all patches applied
   Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
   Attack was blocked by firewall, yet again!

10. Multiple choice question:
    This detect shows:
    e. Network mapping using Inverse Domain Queries
    f. Network mapping using NETBIOS services
    g. Network mapping using SNMP
    h. Network mapping using UDP echo requests

Answer: b

Detect #6 - 14 June 2000

```
12:17:44.729299 internal.host > internal.ids: (frag 1109:9@65520)
                               4500 001d 0455 1ffe f211 a491 1848 14ed
                               xxxx xxxx 04d3 0082 0009 0000 6100 0000
                               0000 0000 0000 0000 0000 0000 0000
12:17:44.729366 internal.host > internal.ids: (frag 1109:9@65520)
                               4500 001d 0455 1ffe f211 a491 1848 14ed
                               xxxx xxxx 04d3 0082 0009 0000 6100 0000
                               0000 0000 0000 0000 0000 0000 0000
12:17:44.729399 internal.host > internal.ids: (frag 1109:9@65520)
                               4500 001d 0455 1ffe f211 a491 1848 14ed
                               xxxx xxxx 04d3 0082 0009 0000 6100 0000
                               0000 0000 0000 0000 0000 0000 0000
12:17:44.730091 internal.host > internal.ids: (frag 1109:9@65520)
                               4500 001d 0455 1ffe f211 a491 1848 14ed
                               xxxx xxxx 04d3 0082 0009 0000 6100 0000
                               0000 0000 0000 0000 0000 0000 0000
12:17:44.730169 internal.host > internal.ids: (frag 1109:9@65520)
                               4500 001d 0455 1ffe f211 a491 1848 14ed
                               xxxx xxxx 04d3 0082 0009 0000 6100 0000
                               0000 0000 0000 0000 0000 0000 0000
```

1. Source of trace:
   My internal network

2. Detect was generated by:
   windump sensor host inside firewall

3. Probability that the source address was spoofed:
   None, this was an internal host. The sensor outside the firewall did not have any of the traffic the inner sensor detected.

4. Description of attack:
   Teardrop-style attack using crafted UDP fragmentation packets against our internal commercial content filter/IDS.

5. Attack mechanism:
   DoS attempt to either crash host system (Windows 2000) or cause it to overload the IDS's blocking capabilitities.

6. Correlations:
   See http://www.microsoft.com/technet/security/bulletin/ms00-029.asp & CVE CAN-2000-0305.

7. Evidence of active targeting:
   This internal host was actively targeting the commercial IDS system that provides real-time blocking of inappropriate web-content & other non-work related internet services.

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

(2 + 4) - (5 + 1) = 0
Criticality: 2 - IDS system
Lethality: 4 - DoS
System Countermeasures: 5 - Current NOS, all current patches applied
Network Countermeasures: 1 - Internal IDS not protected from internal friendly hosts

9. Defensive recommendation:
W2K machine hardened against DoS vulnerabilities because current patches were applied. Enforcement of computer usage policy to disconnect offensive internal host implemented.

10. Multiple choice question:
This example shows:
a. MSCAN Attack
b. LAND Attack
c. Fragmented ICMP DoS Attack
d. Fragmented UDP DoS Attack
Answer: d

Detect #7 - 10 June 2000

```
08:56:24.151810 pcaw.remote.1042 > pcaw.host.5632: udp 2 (ttl 115, id 53248)
08:56:24.152976 pcaw.remote.1042 > pcaw.host.22: udp 2 (ttl 115, id 53504)
08:56:24.182342 pcaw.host.5632 > pcaw.remote.1042: udp 5 (ttl 126, id 58354)
08:56:24.820943 pcaw.remote.1043 > pcaw.host.5631: S 160379:160379(0) win 8192 <mss 1460,nop,nop,sackOK>
(DF) (ttl 115, id 53760)
08:56:24.847390 pcaw.host.5631 > pcaw.remote.1043: S 326485612:326485612(0) ack 160380 win 8760 <mss
1460,nop,nop,sackOK> (DF) (ttl 126, id 58610)
08:56:24.956379 pcaw.remote.1043 > pcaw.host.5631: . ack 1 win 8760 (DF) (ttl 115, id 54016)
08:56:24.960317 pcaw.remote.1043 > pcaw.host.5631: P 1:5(4) ack 1 win 8760 (DF) (ttl 115, id 54272)
08:56:25.080854 pcaw.host.5631 > pcaw.remote.1043: . ack 5 win 8756 (DF) (ttl 126, id 58866)
08:56:26.788583 pcaw.host.5631 > pcaw.remote.1043: P 1:37(36) ack 5 win 8756 (DF) (ttl 126, id 59122)
08:56:27.645363 pcaw.remote.1043 > pcaw.host.5631: P 5:8(3) ack 37 win 8724 (DF) (ttl 115, id 54528)
```

1. Source of trace:
My network

2. Detect was generated by:
windump

3. Probability that the source address was spoofed:
Low. Ping, traceroute & match

4. Description of attack:
PcAnywhere host detection (udp 22) and subsequent connection to pcAnywhere host.

5. Attack mechanism:
PcAnywhere ping (UDP 22)

6. Correlations:
This trace occurs regularly as there are users with pcAnywhere remote working in various mobile locations. This detect is similar to the detect submitted by Fred Kolbrener
http://www.sans.org/y2k/practical/Fred_Kolbrener.doc

7. Evidence of active targeting:
Yes, the pcaw.host is targeted by the remote user.

8. Severity:

```
(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
( 2 + 3 ) - ( 5 + 2 ) = -2
Criticality: 2 - W95/98 Workstation
Lethality:  3 - Sniffed passwords vulnerability
System Countermeasures:  5 - Current NOS, all patches applied
Network Countermeasures:  2 - Permissive firewall rule for pcAnywhere
```

9. Defensive recommendation:
Although pcAnywhere's default password encryption is "clear-text", the next option of pcAnywhere encryption is not much more secure. If you must use pcAnywhere, enable Symmetric encryption on both the host and the remote system and force it to use these settings so it does not fall back to clear-text password negotiation. Also, do not synchronize your pcAnywhere authentication to your NT domain unless you would like to risk giving out the encrypted Administrator password to the "black-hat" on the cable-modem next to you. Also, see CVE CAN-2000-0324 for more information on the reliability of pcAnywhere v8/9.

10. Multiple choice question:
This detect shows:

a. Default pcAnywhere v2.0 connection
b. Default pcAnywhere v7.0 connection
c. Default pcAnywhere v7.5 connection
d. Default pcAnywhere v8/9 connection
Answer: d

Detect #8 - 10 June 2000

```
18:43:31.390054 207.71.92.221.1292 > internal.host.73.143: S 529492340:529492340(0) win 8192 <mss 1460> (DF)
(ttl 111, id 44781)
18:43:31.890167 207.71.92.221.1292 > internal.host.73.143: S 529492340:529492340(0) win 8192 <mss 1460> (DF)
(ttl 111, id 8686)
18:43:32.392050 207.71.92.221.1292 > internal.host.73.143: S 529492340:529492340(0) win 8192 <mss 1460> (DF)
(ttl 111, id 37102)
18:43:32.891161 207.71.92.221.1292 > internal.host.73.143: S 529492340:529492340(0) win 8192 <mss 1460> (DF)
(ttl 111, id 9199)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low. Ping, traceroute & nslookup trace the ip back to shieldsup.grc.com, a site used to check for security vulnerabilities (see www.grc.com)

4. Description of attack:
   This is a IMAP scan that was initiated a trusted user on the LAN

5. Attack mechanism:
   The signature is the fact that the seq/ack numbers are identical, as described in the SANS training materials (IDS 2.4/2.5; Pg 203)

6. Correlations:
   This trace is a bit of a recurring theme… as the folks at GRC update their techniques these scans get requested by our internal users to see if the latest methods get by our corporate firewall. Recommendation: Add a filter to not list this host 207.71.92.221 as it is constant noise on the hourly activity reports.

7. Evidence of active targeting:
   This scan is specifically requested by a LAN user.

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (2 + 1) - (5 + 5) = -7
   Criticality: 2 - W95/98 User
   Lethality: 1 - Security scan, not malicious
   System Countermeasures: 5 - Current NOS, all patches applied
   Network Countermeasures: 5 - Validated restrictive firewall

9. Defensive recommendation:
   Attack was blocked by firewall, once again.

10. Multiple choice question:
    This detect shows:
    a. Socks scan
    b. IMAP scan
    c. Echo request
    d. SNMP probe

Answer: b

Detect #9 - 10 June 2000

```
17:20:37.963507 10.1.1.24.68 > 255.255.255.255.67: hlen:16 xid:0xef4a1010 [|bootp]
17:20:42.969237 10.1.1.24.68 > 255.255.255.255.67: hlen:16 xid:0xef4a1010 secs:1280 [|bootp]
17:20:49.969197 10.1.1.24.68 > 255.255.255.255.67: hlen:16 xid:0xef4a1010 secs:3072 [|bootp]
17:21:04.970299 10.1.1.24.68 > 255.255.255.255.67: hlen:16 xid:0xef4a1010 secs:6912 [|bootp]
```

1. Source of trace:
   My xDSL workstation

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low

4. Description of attack:
   Potential exploit against server local/var/bootfiles/some_name

5. Attack mechanism:
   As described in the SANS course material (IDS 2.4/2.5; Pg 310)

6. Correlations:
   This xDSL technology implements UDP broadcasts that are sent to all connected stations using Cisco's Generic Routing Encapsulation (GRE).

7. Evidence of active targeting:
   None

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (2 + 2) - (4 + 3) = -3
   Criticality: 2 - W2K Workstation
   Lethality: 2 - Null session
   System Countermeasures: 4 - Current NOS, most patches applied
   Network Countermeasures: 3 - BlackIce Defender

9. Defensive recommendation:
   None, traffic ignored

10. Multiple choice question:
    This detect shows:
    a. Bootp service encapsulated in GRE
    b. UDP flooding
    c. ICMP flooding
    d. GRE packets encapsulated in bootp
    Answer: a

Detect #10 - 10 June 2000

```
21:21:03.156012 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 14414)
21:21:04.401946 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 14416)
21:21:05.854055 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 14417)
22:46:11.464108 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 16442)
22:46:12.920040 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 16443)
22:46:14.423102 inet.router1 > inet.router2: icmp: host inet.router1 unreachable - admin prohibited filter
(ttl 251, id 16444)
```

1. Source of trace:
   My network

2. Detect was generated by:
   windump

3. Probability that the source address was spoofed:
   Low.

4. Description of attack:
   ICMP packets between internet routers not allowed

5. Attack mechanism:
   Cisco ACL

6. Correlations:
   SANS course material 2.4/2.5; Pg 253.

7. Evidence of active targeting:
   Yes, pings not being accepted by inet.router1

8. Severity:
   (Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
   (5 + 4) - (5 + 5) = -1
   Criticality: 5 - Main internet routers
   Lethality: 4 - DoS
   System Countermeasures: 5 - Current IOS
   Network Countermeasures: 5 - Validated ACL's

9. Defensive recommendation:
   Attack was blocked, implementation of Silent Drop would also eliminate some unnecessary messages.

10. Multiple choice question:
    This detect shows:
    a. ICMP host ping
    b. Fragmented ICMP
    c. Teardrop
    d. Host scanning

```
Answer:  a
```