Global Information Assurance Certification Paper

Level 2 Practical Assignment by:
Samuel Sheinin

Detect #1: Back Orifice Trojan Probe

Ethernet II
  Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
  Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
  Type: IP (0x0800)
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 44
  Identification: 0x7f01
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 29
  Protocol: TCP (0x06)
  Header checksum: 0x495c (correct)
  Source: 63.23.142.99 (63.23.142.99)
  Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 1062 (1062), Dst Port: 31337 (31337), Seq: 10248694, Ack: 0
  Source port: 1062 (1062)
  Destination port: 31337 (31337)
  Sequence number: 10248694
  Header length: 24 bytes
  Flags: 0x0002 (SYN)
    ..0. .... = Urgent: Not set
    ...0 .... = Acknowledgment: Not set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..1. = Syn: Set
    ....0 = Fin: Not set
  Window size: 8192
  Checksum: 0x0196
  Options: (4 bytes)
    Maximum segment size: 1460 bytes

Frame 2592 (58 on wire, 58 captured)
  Arrival Time: May 26, 2000 22:54:51.0859
  Time delta from previous packet: 2.549999 seconds
  Frame Number: 2592
  Packet Length: 58 bytes
  Capture Length: 58 bytes
Ethernet II
  Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
  Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
  Type: IP (0x0800)
Internet Protocol
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Currently Unused: 0
  Total Length: 44
  Identification: 0x7f01
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 29

Protocol: TCP (0x06)
Header checksum: 0x495c (correct)
Source: 63.23.142.99 (63.23.142.99)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 1062 (1062), Dst Port: 31337 (31337), Seq: 10248694, Ack: 0
Source port: 1062 (1062)
Destination port: 31337 (31337)
Sequence number: 10248694
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x0196
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 2593 (58 on wire, 58 captured)
Arrival Time: May 26, 2000 22:54:51.7319
Time delta from previous packet: 0.646000 seconds
Frame Number: 2593
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x8001
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x485c (correct)
Source: 63.23.142.99 (63.23.142.99)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 1062 (1062), Dst Port: 31337 (31337), Seq: 10248694, Ack: 0
Source port: 1062 (1062)
Destination port: 31337 (31337)
Sequence number: 10248694
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x0196
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 2594 (58 on wire, 58 captured)
Arrival Time: May 26, 2000 22:54:51.7560
Time delta from previous packet: 0.024001 seconds
Frame Number: 2594
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4

Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x8001
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x485c (correct)
Source: 63.23.142.99 (63.23.142.99)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 1062 (1062), Dst Port: 31337 (31337), Seq: 10248694, Ack: 0
Source port: 1062 (1062)
Destination port: 31337 (31337)
Sequence number: 10248694
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x0196
Options: (4 bytes)
Maximum segment size: 1460 bytes

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - The address was spoofed
     - The sequence numbers on each of the packets are the same; which tells us they probably came from some kind of packet generator

4. Description of attack:

   a. The attacker is trying to connect to port 31337
   b. One of the most well known Trojans (Back Orifice) operates at port 31337.
   c. This is a Trojan probe

5. Attack mechanism:

   -. Back Orifice is a remote administration program, which once installed on a Windows machine, gives the attacker the ability to completely control the server.

6. Correlations:

   - This is a well known attack and has been seen many times
   - More information can be found at http://www.cert.org/tech_tips/win-95-info.html

7. Evidence of active targeting:

   This attack was targeted towards this specific host

8. Severity:

   - (Critical + Lethal) - (System + Countermeasures) = severity
   - (3 + 5) - (4 + 5) = -1

9. Defensive recommendations:

   - Defenses are fine; attack blocked by firewall
   - Block access to port 31337

10. Test Question:

    This attack would be best described as:

    a) Denial of service
    b) Host scanning
    c) Trojan probe
    d) Covert channel

    Answer is c)

Detect #2: Boink attack

```
Frame 1469 (70 on wire, 70 captured)
   Arrival Time: May 26, 2000 21:21:05.7749
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 1469
   Packet Length: 70 bytes
   Capture Length: 70 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 56
   Identification: 0x0455
   Flags: 0x02
      .0.. = Don't fragment: Not set
      ..1. = More fragments: Set
   Fragment offset: 0
   Time to live: 243
   Protocol: UDP (0x11)
   Header checksum: 0x2ecd (correct)
   Source: 237.141.191.16 (237.141.191.16)
   Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
   Source port: 80 (80)
   Destination port: 80 (80)
   Length: 36
   Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ............

Frame 1470 (70 on wire, 70 captured)
   Arrival Time: May 26, 2000 21:21:05.7799
   Time delta from previous packet: 0.005000 seconds
   Frame Number: 1470
   Packet Length: 70 bytes
   Capture Length: 70 bytes
```

Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x2ecd (correct)
Source: 237.141.191.16 (237.141.191.16)
Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
Source port: 80 (80)
Destination port: 80 (80)
Length: 36
Checksum: 0x0000
Data (28 bytes)

0 0000 0000 0000 0000 0000 0000 0000 0000 ....
10 0000 0000 0000 0000 0000 0000 ....

Frame 1471 (70 on wire, 70 captured)
Arrival Time: May 26, 2000 21:21:05.7799
Time delta from previous packet: 0.000000 seconds
Frame Number: 1471
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..**1. = More fragments: Set**
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x2ecd (correct)
Source: 237.141.191.16 (237.141.191.16)
Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
Source port: 80 (80)
Destination port: 80 (80)
Length: 36
Checksum: 0x0000
Data (28 bytes)

0 0000 0000 0000 0000 0000 0000 0000 0000 ....
10 0000 0000 0000 0000 0000 0000 ....

Frame 1472 (70 on wire, 70 captured)
Arrival Time: May 26, 2000 21:21:05.7799
Time delta from previous packet: 0.000000 seconds
Frame Number: 1472
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)

```
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 56
   Identification: 0x0455
   Flags: 0x02
      .0.. = Don't fragment: Not set
      ..1. = More fragments: Set
   Fragment offset: 0
   Time to live: 243
   Protocol: UDP (0x11)
   Header checksum: 0x2ecd (correct)
   Source: 237.141.191.16 (237.141.191.16)
   Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
   Source port: 80 (80)
   Destination port: 80 (80)
   Length: 36
   Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ............

Frame 1473 (70 on wire, 70 captured)
   Arrival Time: May 26, 2000 21:21:05.7799
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 1473
   Packet Length: 70 bytes
   Capture Length: 70 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 56
   Identification: 0x0455
   Flags: 0x02
      .0.. = Don't fragment: Not set
      ..1. = More fragments: Set
   Fragment offset: 0
   Time to live: 243
   Protocol: UDP (0x11)
   Header checksum: 0x2ecd (correct)
   Source: 237.141.191.16 (237.141.191.16)
   Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
   Source port: 80 (80)
   Destination port: 80 (80)
   Length: 36
   Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ............
```

1. Source of trace:
   - My network
2. Detect was generated by:

3. Probability the source address was spoofed:

   - Highly likely the source address was spoofed since this attack uses a script to craft packets

4. Description of the attack:

   - The boink attack is a denial of service attack against Windows 95/NT

5. Attack Mechanism:

   - The attack works by sending fragments, which are greater in size than the header. When the target machine reassembles the fragments into invalid UDP datagrams, they cause the machine to crash

6. Correlations:

   - This attack has been reported many times. It is very similar to a very well known attack (teardrop)
   - More information can be found at http://www.cert.org/summaries/CS-98.02.html

7. Evidence of active targeting:

   - This is a denial of service attack against this specific host

8. Severity:

   - (Critical + Lethal) – (System + Countermeasures)
   - (3 + 4) – (5 + 5) = -3

9. Defensive recommendations:

   - Apply Microsoft patch
   - Apply filters to your IDS which look for this kind of activity
     a. UDP Packet
     b. Fragment offset > Header Length
   - Defenses are fine; attack blocked by firewall

10. Test question:

    This attack exploits vulnerability in:

    a) Syslog
    b) TCP/IP stack
    c) SATAN
    d) Outlook express

    Answer: b)

Detect #3: OS Fingerprinting (Christmas Tree)

Arrival Time: May 26, 2000 22:46:35.4349
Time delta from previous packet: 0.000999 seconds
Frame Number: 2564
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0xd4d8 (correct)
Source: 133.91.156.151 (133.91.156.151)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 33458 (33458), Dst Port: 53 (53), Seq: 1423245312, Ack: 0
Source port: 33458 (33458)
Destination port: 53 (53)
Sequence number: 1423245312
Acknowledgement number: 0
Header length: 20 bytes
Flags: 0x003f (FIN, SYN, RST, PSH, ACK, URG)
..1. .... = Urgent: Set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .1.. = Reset: Set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 34829
Checksum: 0x65f4
Urgent pointer: 0

Frame 2565 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:46:35.6729
Time delta from previous packet: 0.238000 seconds
Frame Number: 2565
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0x9a8e (correct)
Source: 17.232.74.85 (17.232.74.85)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 11160 (11160), Dst Port: 53 (53), Seq: 2565734400, Ack: 0
Source port: 11160 (11160)
Destination port: 53 (53)
Sequence number: 2565734400
Acknowledgement number: 0
Header length: 20 bytes
Flags: 0x003f (FIN, SYN, RST, PSH, ACK, URG)

..1. .... = Urgent: Set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .1.. = Reset: Set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 3157
Checksum: 0xba63
Urgent pointer: 0

Frame 2566 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:46:35.6959
Time delta from previous packet: 0.023000 seconds
Frame Number: 2566
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0x9a8e (correct)
Source: 17.232.74.85 (17.232.74.85)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 11160 (11160), Dst Port: 53 (53), Seq: 2565734400, Ack: 0
Source port: 11160 (11160)
Destination port: 53 (53)
Sequence number: 2565734400
Acknowledgement number: 0
Header length: 20 bytes
Flags: 0x003f (FIN, SYN, RST, PSH, ACK, URG)
..1. .... = Urgent: Set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .1.. = Reset: Set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 3157
Checksum: 0xba63
Urgent pointer: 0

Frame 2567 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:46:35.7710
Time delta from previous packet: 0.075001 seconds
Frame Number: 2567
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252

Protocol: TCP (0x06)
Header checksum: 0x2491 (correct)
Source: 26.19.184.39 (26.19.184.39)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 44239 (44239), Dst Port: 53 (53), Seq: 81723392, Ack: 0
Source port: 44239 (44239)
Destination port: 53 (53)
Sequence number: 81723392
Acknowledgement number: 0
Header length: 20 bytes
Flags: 0x003f (FIN, SYN, RST, PSH, ACK, URG)
..1. .... = Urgent: Set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .1.. = Reset: Set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 38800
Checksum: 0xcc02
Urgent pointer: 0

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - Highly likely
   - The addresses are different, but the arrival times are so close that this seems like a program which is randomly generating IP addresses

4. Description of attack:

   - TCP fingerprinting (operating system determination, host discovery)
   - Sending packets with every flag set

5. Attack Mechanism

   - Sending packets with certain flag combinations causes some operating systems to react in certain ways
   - Reaction happens whether the port is open or closed
   - Most attackers are blind; knowing a host is there, and determining the operating system enables them to plan attacks specific to that operating system, thus making their life much easier

6. Correlations:

   - This is a well known fingerprinting technique
   - Used by commercial products such as NMAP (http://www.insecure.org/nmap)

7. Evidence of active targeting:

   - It does not appear that the attacker would be targeting just this machine
   - It is not a stealthy scan
   - The attacker is apparently looking for a DNS server

8. Severity:

   - (Critical + Lethal) – (System + Countermeasures) = Severity
   - (3 + 2) – (4 + 5) = -4

9. Defensive Recommendations:

- Defenses are fine, firewall recognized this as Christmas tree packets
- Maintain the latest patches
- Apply filters which look for irregular flag combinations

10. Test question:

OS Fingerprinting targets which of the following operating systems:

a) Solaris 2.6
b) Red Hat Linux 6.1
c) Windows NT
d) All of the above

Answer: d)

Detect #4: Ping Flood

Frame 1494 (42 on wire, 42 captured)
Arrival Time: May 26, 2000 21:34:05.8459
Time delta from previous packet: 0.225999 seconds
Frame Number: 1494
Packet Length: 42 bytes
Capture Length: 42 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 28
Identification: 0x0455
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: ICMP (0x01)
Header checksum: 0x45f9 (correct)
Source: 237.141.191.16 (237.141.191.16)
Destination: 63.23.136.221 (63.23.136.221)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ff
Identifier: 0x0000
Sequence number: 0

Frame 1495 (42 on wire, 42 captured)
Arrival Time: May 26, 2000 21:34:06.4919
Time delta from previous packet: 0.646000 seconds
Frame Number: 1495
Packet Length: 42 bytes
Capture Length: 42 bytes
Ethernet II

Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 28
Identification: 0x0455
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: ICMP (0x01)
Header checksum: 0x45f9 (correct)
Source: 237.141.191.16 (237.141.191.16)
Destination: 63.23.136.221 (63.23.136.221)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ff
Identifier: 0x0000
Sequence number: 0

Frame 1496 (42 on wire, 42 captured)
Arrival Time: May 26, 2000 21:34:07.1610
Time delta from previous packet: 0.669001 seconds
Frame Number: 1496
Packet Length: 42 bytes
Capture Length: 42 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 28
Identification: 0x0455
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: ICMP (0x01)
Header checksum: 0x45f9 (correct)
Source: 237.141.191.16 (237.141.191.16)
Destination: 63.23.136.221 (63.23.136.221)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7ff
Identifier: 0x0000
Sequence number: 0

Frame 1497 (42 on wire, 42 captured)
Arrival Time: May 26, 2000 21:34:07.8220
Time delta from previous packet: 0.661000 seconds
Frame Number: 1497
Packet Length: 42 bytes
Capture Length: 42 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0

```
   Total Length: 28
   Identification: 0x0455
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: ICMP (0x01)
   Header checksum: 0x45f9 (correct)
   Source: 237.141.191.16 (237.141.191.16)
   Destination: 63.23.136.221 (63.23.136.221)
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xf7ff
   Identifier: 0x0000
   Sequence number: 0

Frame 1498 (42 on wire, 42 captured)
   Arrival Time: May 26, 2000 21:34:08.5060
   Time delta from previous packet: 0.684000 seconds
   Frame Number: 1498
   Packet Length: 42 bytes
   Capture Length: 42 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 28
   Identification: 0x0455
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: ICMP (0x01)
   Header checksum: 0x45f9 (correct)
   Source: 237.141.191.16 (237.141.191.16)
   Destination: 63.23.136.221 (63.23.136.221)
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xf7ff
   Identifier: 0x0000
   Sequence number: 0
```

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - High probability the source address was spoofed

4. Description of attack:

   - Denial of service attack (two possibilities)
     a. Smurf attack
     b. Ping flood

5. Attack mechanism:

   - A ping flood works by simply flooding the target with echo requests causing a denial of service
   - The smurf attack works by sending ICMP broadcast echo requests with a spoofed IP address to a number of various hosts. These hosts respond to the echo requests causing a denial of service at the spoofed address. If the attack is large enough the intermediary hosts may also be affected.

6. Correlations:

   - These are both common well known attacks
   - More information can be found at http://www.cert.org/advisories/CA-98.01.smurf.html

7. Evidence of active targeting:

   - There is evidence of active targeting since both attacks would require a specific target

8. Severity:

   - (Critical + Lethal) – (System + Countermeasures)
   - (3 + 4) – (4 + 5) = -2

9. Defensive recommendations:

   - Defenses are fine; blocked by firewall
   - Block incoming ICMP echo requests on your firewall
   - Configure your IDS to look for ICMP broadcasts
   - Disable the translation of directed broadcasts to physical broadcasts on your Cisco router (no ip directed-broadcast)
   - Explicitly deny traffic to broadcast addresses behind the router

10. Test question:

    The severity level in this case is low. Which of the following would cause it to rise?

    a) Poor firewall configuration
    b) Using Windows NT for your DNS server
    c) Failure to enforce a strong password policy
    d) None of the above

Answer: a)

Detect #5: SYN Flood

Frame 249 (62 on wire, 62 captured)
Arrival Time: Jun 16, 2000 10:07:58.0645
Time delta from previous packet: 0.000000 seconds
Frame Number: 249
Packet Length: 62 bytes
Capture Length: 62 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4

Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 48
Identification: 0xf01c
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 115
Protocol: TCP (0x06)
Header checksum: 0x8b9c (correct)
Source: 64.20.134.86 (64.20.134.86)
Destination: 63.23.134.141 (63.23.134.141)
Transmission Control Protocol, Src Port: 1619 (1619), Dst Port: 24 (24), Seq: 5077511, Ack: 0
Source port: 1619 (1619)
Destination port: 24 (24)
Sequence number: 5077511
Header length: 28 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x59ed
Options: (8 bytes)
Maximum segment size: 536 bytes
NOP
NOP
SACK permitted

Frame 250 (62 on wire, 62 captured)
Arrival Time: Jun 16, 2000 10:07:58.0705
Time delta from previous packet: 0.006000 seconds
Frame Number: 250
Packet Length: 62 bytes
Capture Length: 62 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 48
Identification: 0xf21c
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 115
Protocol: TCP (0x06)
Header checksum: 0x899c (correct)
Source: 64.20.134.86 (64.20.134.86)
Destination: 63.23.134.141 (63.23.134.141)
Transmission Control Protocol, Src Port: 1621 (1621), Dst Port: 26 (26), Seq: 5077512, Ack: 0
Source port: 1621 (1621)
Destination port: 26 (26)
Sequence number: 5077512
Header length: 28 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x59e8
Options: (8 bytes)

```
      Maximum segment size: 536 bytes
      NOP
      NOP
      SACK permitted

Frame 251 (62 on wire, 62 captured)
   Arrival Time: Jun 16, 2000 10:07:58.0705
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 251
   Packet Length: 62 bytes
   Capture Length: 62 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 48
   Identification: 0xf31c
   Flags: 0x04
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 115
   Protocol: TCP (0x06)
   Header checksum: 0x889c (correct)
   Source: 64.20.134.86 (64.20.134.86)
   Destination: 63.23.134.141 (63.23.134.141)
Transmission Control Protocol, Src Port: 1622 (1622), Dst Port: 27 (27), Seq: 5077512, Ack: 0
   Source port: 1622 (1622)
   Destination port: 27 (27)
   Sequence number: 5077512
   Header length: 28 bytes
   Flags: 0x0002 (SYN)
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
   Window size: 8192
   Checksum: 0x59e6
   Options: (8 bytes)
      Maximum segment size: 536 bytes
      NOP
      NOP
      SACK permitted

Frame 252 (62 on wire, 62 captured)
   Arrival Time: Jun 16, 2000 10:07:58.0705
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 252
   Packet Length: 62 bytes
   Capture Length: 62 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 48
   Identification: 0xf41c
   Flags: 0x04
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 115
   Protocol: TCP (0x06)
   Header checksum: 0x879c (correct)
```

Source: 64.20.134.86 (64.20.134.86)
Destination: 63.23.134.141 (63.23.134.141)
Transmission Control Protocol, Src Port: 1623 (1623), Dst Port: 28 (28), Seq: 5077512, Ack: 0
Source port: 1623 (1623)
Destination port: 28 (28)
Sequence number: 5077512
Header length: 28 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x59e4
Options: (8 bytes)
Maximum segment size: 536 bytes
NOP
NOP
SACK permitted

Frame 253 (62 on wire, 62 captured)
Arrival Time: Jun 16, 2000 10:07:58.0705
Time delta from previous packet: 0.000000 seconds
Frame Number: 253
Packet Length: 62 bytes
Capture Length: 62 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 48
Identification: 0xf51c
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 115
Protocol: TCP (0x06)
Header checksum: 0x869c (correct)
Source: 64.20.134.86 (64.20.134.86)
Destination: 63.23.134.141 (63.23.134.141)
Transmission Control Protocol, Src Port: 1624 (1624), Dst Port: 29 (29), Seq: 5077513, Ack: 0
Source port: 1624 (1624)
Destination port: 29 (29)
Sequence number: 5077513
Header length: 28 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0x59e1
Options: (8 bytes)
Maximum segment size: 536 bytes
NOP
NOP
SACK permitted

1. Source of trace:

   - My network

2. Detect was generated by:

- Black Ice Defender

3. Probability the source address was spoofed:

   - Highly likely
   - Anomalous sequence numbers

4. Description of attack:

   - Denial of service attack which floods the target with SYN packets

5. Attack mechanism:

   - The attacker sends a large number of SYN packets to the target with no intention of completing the three-way handshake. The receiving computer can only take in a certain amount of packets at once; eventually the receiving computer's buffer fills up and legitimate traffic cannot get through.

6. Correlations:

   - This is one of the oldest denial of service attacks
   - Many computers have been affected
   - More information can be found on page 150 of **Intrusion Detection and Packet Filtering: How It Really Works** *by: Vicki Irwin & Hal Pomeranz*

7. Evidence of active targeting:

   - This attack goes after one specific host, so there is active targeting

8. Severity

   - (Critical + Lethal) – (System + Countermeasures) = Severity
   - (3 + 4) – (4 + 5) = -2

9. Defensive recommendations:

   - Defenses are fine; blocked by firewall
   - Some stateful firewalls can be configured to recognize this attack
   - Some intrusion detection systems can be configured to write a rule on the firewall (blocking the attacker) once this attack is recognized

10. Test Question:

    SYN flooding can be characterized as which of the following?

    a) Denial of service
    b) Host scanning
    c) Password sniffing
    d) None of the above

    Answer: a)

Detect #6: SYN/FIN

Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0xa19b (correct)
Source: 210.84.130.219 (210.84.130.219)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 47584 (47584), Dst Port: 21 (21), Seq: 2366111744, Ack: 0
Source port: 47584 (47584)
Destination port: 21 (21)
Sequence number: 2366111744
Header length: 20 bytes
Flags: 0x0003 (FIN, SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 28460
Checksum: 0xdc92

Frame 2059 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:06:17.6339
Time delta from previous packet: 0.000999 seconds
Frame Number: 2059
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0xd667 (correct)
Source: 43.187.244.168 (43.187.244.168)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 13620 (13620), Dst Port: 21 (21), Seq: 3819765760, Ack: 0
Source port: 13620 (13620)
Destination port: 21 (21)
Sequence number: 3819765760
Header length: 20 bytes
Flags: 0x0003 (FIN, SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 53687
Checksum: 0xdcda

Frame 2060 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:06:17.6360
Time delta from previous packet: 0.002001 seconds
Frame Number: 2060
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0x3081 (correct)
Source: 152.23.46.51 (152.23.46.51)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 30166 (30166), Dst Port: 21 (21), Seq: 2249588736, Ack: 0
Source port: 30166 (30166)
Destination port: 21 (21)
Sequence number: 2249588736
Header length: 20 bytes
Flags: 0x0003 (FIN, SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 11204
Checksum: 0xf9dc

Frame 2061 (54 on wire, 54 captured)
Arrival Time: May 26, 2000 22:06:17.6369
Time delta from previous packet: 0.000999 seconds
Frame Number: 2061
Packet Length: 54 bytes
Capture Length: 54 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 40
Identification: 0x0010
Flags: 0x00
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 252
Protocol: TCP (0x06)
Header checksum: 0x2645 (correct)
Source: 51.253.156.137 (51.253.156.137)
Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 5599 (5599), Dst Port: 21 (21), Seq: 80150528, Ack: 0
Source port: 5599 (5599)
Destination port: 21 (21)
Sequence number: 80150528
Header length: 20 bytes
Flags: 0x0003 (FIN, SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set

.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....1 = Fin: Set
Window size: 48047
Checksum: 0x40fc

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed

   - The address was spoofed
   - These packets were crafted with an impossible flag combination

4. Description of attack:

   - Network scanning

5. Attack mechanism

   - Certain operating systems might respond to a combination like this on with a reset, telling the attacker that the host is alive
   - The Linux operating system responds with a SYN-FIN-ACK. In cases like this the attacker can get lucky and be able to determine the operating system

6. Correlations:

   - This is a well known scanning method
   - More information can be found at http://geek-girl.com/bugtraq/1998_3/0104.html

7. Evidence of active targeting

   - There would not be active targeting since the attacker is probably scanning more than one host

8. Severity:

   - (Critical + Lethal) – (System + Countermeasures) = Severity
   - (3 + 1) – (4 + 5) = -5

9. Defensive recommendations:

   - Defenses are fine; packets dropped by firewall
   - Apply filters which look for this flag combination on your IDS
   - Hide hosts using network address translation

10. Test question:

This trace is an example of IP spoofing:

a) True
b) False

Answer – true

Detect #7: Nestea

Frame 6107 (70 on wire, 70 captured)
Arrival Time: May 30, 2000 20:52:59.1339
Time delta from previous packet: 0.119000 seconds
Frame Number: 6107
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x5ed3 (correct)
Source: 107.39.31.161 (107.39.31.161)
Destination: 63.23.122.173 (63.23.122.173)
User Datagram Protocol
Source port: 1029 (1029)
Destination port: 1029 (1029)
Length: 36
Checksum: 0x0000
Data (28 bytes)

0 0000 0000 0000 0000 0000 0000 0000 0000 ....
10 0000 0000 0000 0000 0000 0000 ....

Frame 6108 (70 on wire, 70 captured)
Arrival Time: May 30, 2000 20:52:59.2289
Time delta from previous packet: 0.095000 seconds
Frame Number: 6108
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x5ed3 (correct)
Source: 107.39.31.161 (107.39.31.161)
Destination: 63.23.122.173 (63.23.122.173)
User Datagram Protocol
Source port: 1029 (1029)
Destination port: 1029 (1029)

Length: 36
Checksum: 0x0000
Data (28 bytes)

0 0000 0000 0000 0000 0000 0000 0000 0000 ....
10 0000 0000 0000 0000 0000 0000 ....

Frame 6109 (70 on wire, 70 captured)
Arrival Time: May 30, 2000 20:52:59.3539
Time delta from previous packet: 0.125000 seconds
Frame Number: 6109
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x5ed3 (correct)
Source: 107.39.31.161 (107.39.31.161)
Destination: 63.23.122.173 (63.23.122.173)
User Datagram Protocol
Source port: 1029 (1029)
Destination port: 1029 (1029)
Length: 36
Checksum: 0x0000
Data (28 bytes)

0 0000 0000 0000 0000 0000 0000 0000 0000 ....
10 0000 0000 0000 0000 0000 0000 ....

Frame 6110 (70 on wire, 70 captured)
Arrival Time: May 30, 2000 20:52:59.5299
Time delta from previous packet: 0.176000 seconds
Frame Number: 6110
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0x5ed3 (correct)
Source: 107.39.31.161 (107.39.31.161)
Destination: 63.23.122.173 (63.23.122.173)
User Datagram Protocol
Source port: 1029 (1029)
Destination port: 1029 (1029)
Length: 36
Checksum: 0x0000
Data (28 bytes)

```
  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ..........
```

```
Frame 6111 (70 on wire, 70 captured)
   Arrival Time: May 30, 2000 20:52:59.6490
   Time delta from previous packet: 0.119001 seconds
   Frame Number: 6111
   Packet Length: 70 bytes
   Capture Length: 70 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 56
   Identification: 0x0455
   Flags: 0x02
      .0.. = Don't fragment: Not set
      ..1. = More fragments: Set
   Fragment offset: 0
   Time to live: 243
   Protocol: UDP (0x11)
   Header checksum: 0x5ed3 (correct)
   Source: 107.39.31.161 (107.39.31.161)
   Destination: 63.23.122.173 (63.23.122.173)
User Datagram Protocol
   Source port: 1029 (1029)
   Destination port: 1029 (1029)
   Length: 36
   Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ..........
```

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - Good chance the source was spoofed

4. Description of attack:

   - The Nestea attack is a denial of service attack mostly targeted towards Linux 2.0 and 2.1 machines

5. Attack mechanism:

   - IP fragmentation attack (similar to teardrop)
   - The attack works by exploiting the “off by one IP header” bug
   - Causes Linux 2.0, 2.1, and some Windows machines to hang or crash

6. Correlations:

- More information can be found at http://packetstorm.securify.com/Exploit_Code_Archive/nestea.c
- This is a well known attack which has been reported many times

7. Evidence of active targeting:

- There is evidence of active targeting
- This denial of service attack is made to crash one target

8. Severity:

- (Critical + Lethal) – (System + Countermeasures) = Severity
- (3 + 4) – (5 + 5) = -3

9. Defensive recommendations:

- Defenses are fine, blocked by firewall
- Maintain patches
- Apply a filter to your IDS to look for this traffic

10. Test question:

This attack shows an example of:

a) Fragmentation
b) SYN flood
c) Port scanning
d) None of the above

Answer is a)

Detect #8: Port Probe

```
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 44
   Identification: 0x8c00
   Flags: 0x04
      .1.. = Don't fragment: Set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 29
   Protocol: TCP (0x06)
   Header checksum: 0x51b3 (correct)
   Source: 63.23.135.61 (63.23.135.61)
   Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1052 (1052), Dst Port: 139 (139), Seq: 2838273, Ack: 0
   Source port: 1052 (1052)
   Destination port: 139 (139)
   Sequence number: 2838273
   Header length: 24 bytes
   Flags: 0x0002 (SYN)
```

..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xa43a
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 6357 (58 on wire, 58 captured)
Arrival Time: May 30, 2000 21:07:14.2829
Time delta from previous packet: 0.000000 seconds
Frame Number: 6357
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x8d00
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x50b3 (correct)
Source: 63.23.135.61 (63.23.135.61)
Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1052 (1052), Dst Port: 139 (139), Seq: 2838273, Ack: 0
Source port: 1052 (1052)
Destination port: 139 (139)
Sequence number: 2838273
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xa43a
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 6358 (58 on wire, 58 captured)
Arrival Time: May 30, 2000 21:07:20.5800
Time delta from previous packet: 6.297001 seconds
Frame Number: 6358
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x8e00
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0

Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x4fb3 (correct)
Source: 63.23.135.61 (63.23.135.61)
Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1052 (1052), Dst Port: 139 (139), Seq: 2838273, Ack: 0
Source port: 1052 (1052)
Destination port: 139 (139)
Sequence number: 2838273
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xa43a
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 6359 (58 on wire, 58 captured)
Arrival Time: May 30, 2000 21:07:33.2400
Time delta from previous packet: 12.660000 seconds
Frame Number: 6359
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x8f00
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x4eb3 (correct)
Source: 63.23.135.61 (63.23.135.61)
Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1052 (1052), Dst Port: 139 (139), Seq: 2838273, Ack: 0
Source port: 1052 (1052)
Destination port: 139 (139)
Sequence number: 2838273
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xa43a
Options: (4 bytes)
Maximum segment size: 1460 bytesFrame 6360 (58 on wire, 58 captured)
Arrival Time: May 30, 2000 21:07:58.4739
Time delta from previous packet: 25.233999 seconds
Frame Number: 6360
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x9100
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x4cb3 (correct)
Source: 63.23.135.61 (63.23.135.61)
Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1053 (1053), Dst Port: 21 (21), Seq: 2885556, Ack: 0
Source port: 1053 (1053)
Destination port: 21 (21)
Sequence number: 2885556
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xebfb
Options: (4 bytes)
Maximum segment size: 1460 bytes

Frame 6361 (58 on wire, 58 captured)
Arrival Time: May 30, 2000 21:08:01.5650
Time delta from previous packet: 3.091001 seconds
Frame Number: 6361
Packet Length: 58 bytes
Capture Length: 58 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 44
Identification: 0x9200
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 29
Protocol: TCP (0x06)
Header checksum: 0x4bb3 (correct)
Source: 63.23.135.61 (63.23.135.61)
Destination: 63.23.122.173 (63.23.122.173)
Transmission Control Protocol, Src Port: 1053 (1053), Dst Port: 21 (21), Seq: 2885556, Ack: 0
Source port: 1053 (1053)
Destination port: 21 (21)
Sequence number: 2885556
Header length: 24 bytes
Flags: 0x0002 (SYN)
..0. .... = Urgent: Not set
...0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..1. = Syn: Set
....0 = Fin: Not set
Window size: 8192
Checksum: 0xebfb
Options: (4 bytes)
Maximum segment size: 1460 bytes

1. Source of trace:

- My network

2. Detect was generated by:

- Black Ice Defender

3. Probability the source address was spoofed:

- The source address was spoofed
- Anomalous sequence numbers

4. Description of attack:

- TCP port probe

5. Attack mechanism

- By sending SYN packets to certain ports on this host; the attacker is hoping to find a listening port (which could be a possible entry point into the system)

6. Correlations:

- Port scanning is a very common technique used by hackers hoping to find a vulnerable system
- More information can be found on page 110 of **Intrusion Detection and Packet Filtering: How It Really Works** *by: Vicki Irwin & Hal Pomeranz*

7. Evidence of active targeting:

- It appears the attacker is looking for an open port on this host

8. Severity:

- (Critical + Lethal) – (System + Countermeasures) = Severity
- (3 + 2) – (4 + 5) = -4

9. Defensive recommendation:

- Defenses are fine; blocked by firewall
- Turn of any unneeded services on every host to cut down on listening ports
- Block access to common ports through your firewall

10. Test question:

Port scanning is an example of:

a) Reconnaissance
b) Denial of service
c) Fragmentation
d) None of the above

Answer is a)

Detect #9: UDP Flood

Frame 5407 (70 on wire, 70 captured)
Arrival Time: May 27, 2000 00:21:41.7849
Time delta from previous packet: 0.000000 seconds
Frame Number: 5407
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0xd1d8 (correct)
Source: 192.168.72.234 (192.168.72.234)
Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
Source port: 80 (80)
Destination port: 80 (80)
Length: 36
Checksum: 0x0000
Data (28 bytes)

```
  0  0000 0000 0000 0000 0000 0000 0000 0000  ................
 10  0000 0000 0000 0000 0000 0000            ............
```

Frame 5408 (70 on wire, 70 captured)
Arrival Time: May 27, 2000 00:21:41.7849
Time delta from previous packet: 0.000000 seconds
Frame Number: 5408
Packet Length: 70 bytes
Capture Length: 70 bytes
Ethernet II
Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..00 = Currently Unused: 0
Total Length: 56
Identification: 0x0455
Flags: 0x02
.0.. = Don't fragment: Not set
..1. = More fragments: Set
Fragment offset: 0
Time to live: 243
Protocol: UDP (0x11)
Header checksum: 0xd1d8 (correct)
Source: 192.168.72.234 (192.168.72.234)
Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
Source port: 80 (80)
Destination port: 80 (80)
Length: 36
Checksum: 0x0000
Data (28 bytes)

```
  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ..............

Frame 5409 (70 on wire, 70 captured)
    Arrival Time: May 27, 2000 00:21:41.7849
    Time delta from previous packet: 0.000000 seconds
    Frame Number: 5409
    Packet Length: 70 bytes
    Capture Length: 70 bytes
Ethernet II
    Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
    Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Currently Unused: 0
    Total Length: 56
    Identification: 0x0455
    Flags: 0x02
        .0.. = Don't fragment: Not set
        ..1. = More fragments: Set
    Fragment offset: 0
    Time to live: 243
    Protocol: UDP (0x11)
    Header checksum: 0xd1d8 (correct)
    Source: 192.168.72.234 (192.168.72.234)
    Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
    Source port: 80 (80)
    Destination port: 80 (80)
    Length: 36
    Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ..............

Frame 5410 (70 on wire, 70 captured)
    Arrival Time: May 27, 2000 00:21:41.7849
    Time delta from previous packet: 0.000000 seconds
    Frame Number: 5410
    Packet Length: 70 bytes
    Capture Length: 70 bytes
Ethernet II
    Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
    Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
    Type: IP (0x0800)
Internet Protocol
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..00 = Currently Unused: 0
    Total Length: 56
    Identification: 0x0455
    Flags: 0x02
        .0.. = Don't fragment: Not set
        ..1. = More fragments: Set
    Fragment offset: 0
    Time to live: 243
    Protocol: UDP (0x11)
    Header checksum: 0xd1d8 (correct)
    Source: 192.168.72.234 (192.168.72.234)
    Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
    Source port: 80 (80)
    Destination port: 80 (80)
    Length: 36
    Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ..............
```

```
Frame 5411 (70 on wire, 70 captured)
   Arrival Time: May 27, 2000 00:21:41.7849
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 5411
   Packet Length: 70 bytes
   Capture Length: 70 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 56
   Identification: 0x0455
   Flags: 0x02
      .0.. = Don't fragment: Not set
      ..1. = More fragments: Set
   Fragment offset: 0
   Time to live: 243
   Protocol: UDP (0x11)
   Header checksum: 0xd1d8 (correct)
   Source: 192.168.72.234 (192.168.72.234)
   Destination: 63.23.136.221 (63.23.136.221)
User Datagram Protocol
   Source port: 80 (80)
   Destination port: 80 (80)
   Length: 36
   Checksum: 0x0000
Data (28 bytes)

  0  0000 0000 0000 0000 0000 0000 0000 0000   ................
 10  0000 0000 0000 0000 0000 0000             ............
```

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - The address was spoofed
   - This is an illegal IP address

4. Description of attack:

   - UDP denial of service

5. Attack mechanism:

   - The attacker is sends more UDP datagrams than the receiving computer can handle therefore causing a denial of service

6. Correlations

   - This is a well known attack
   - More information can be found at http://www.cert.org/advisories/CA-96.01.UDP_service_denial.html

7. Evidence of active targeting:

- This attack was targeted at this specific computer

8. Severity:

- (Critical + Lethal) – (System + Countermeasures) = Severity
- (3 + 4) – (4 + 5) = -2

9. Defensive recommendations:

- Defenses are fine; blocked by firewall
- Use host based protection such as TCP Wrapper
- Block access to certain ports on your firewall

10. Test question:

UDP is a connectionless protocol

a) True
b) False

Answer is a)

Detect #10: DNS

```
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 40
   Identification: 0x0010
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: TCP (0x06)
   Header checksum: 0x57d3 (correct)
   Source: 116.214.42.34 (116.214.42.34)
   Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 60848 (60848), Dst Port: 53 (53), Seq: 1243807744, Ack: 0
   Source port: 60848 (60848)
   Destination port: 53 (53)
   Sequence number: 1243807744
   Header length: 20 bytes
   Flags: 0x0002 (SYN)
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
   Window size: 8969
   Checksum: 0xede3

Frame 2331 (54 on wire, 54 captured)
   Arrival Time: May 26, 2000 22:42:25.7009
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 2331
```

```
   Packet Length: 54 bytes
   Capture Length: 54 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 40
   Identification: 0x0010
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: TCP (0x06)
   Header checksum: 0xefe7 (correct)
   Source: 198.154.64.73 (198.154.64.73)
   Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 5815 (5815), Dst Port: 53 (53), Seq: 1473511424, Ack: 0
   Source port: 5815 (5815)
   Destination port: 53 (53)
   Sequence number: 1473511424
   Header length: 20 bytes
   Flags: 0x0002 (SYN)
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
   Window size: 52823
   Checksum: 0xa3f2

Frame 2332 (54 on wire, 54 captured)
   Arrival Time: May 26, 2000 22:42:25.7059
   Time delta from previous packet: 0.005000 seconds
   Frame Number: 2332
   Packet Length: 54 bytes
   Capture Length: 54 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 40
   Identification: 0x0010
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: TCP (0x06)
   Header checksum: 0xa445 (correct)
   Source: 230.199.107.190 (230.199.107.190)
   Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 10058 (10058), Dst Port: 53 (53), Seq: 4078436352, Ack: 0
   Source port: 10058 (10058)
   Destination port: 53 (53)
   Sequence number: 4078436352
   Header length: 20 bytes
   Flags: 0x0002 (SYN)
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
```

```
   Window size: 53512
   Checksum: 0xa9c7

Frame 2333 (54 on wire, 54 captured)
   Arrival Time: May 26, 2000 22:42:25.7059
   Time delta from previous packet: 0.000000 seconds
   Frame Number: 2333
   Packet Length: 54 bytes
   Capture Length: 54 bytes
Ethernet II
   Destination: 44:45:53:54:00:00 (44:45:53:54:00:00)
   Source: 20:53:52:43:00:00 (20:53:52:43:00:00)
   Type: IP (0x0800)
Internet Protocol
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Currently Unused: 0
   Total Length: 40
   Identification: 0x0010
   Flags: 0x00
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 252
   Protocol: TCP (0x06)
   Header checksum: 0x0942 (correct)
   Source: 129.100.108.37 (129.100.108.37)
   Destination: 63.23.136.221 (63.23.136.221)
Transmission Control Protocol, Src Port: 63355 (63355), Dst Port: 53 (53), Seq: 190644224, Ack: 0
   Source port: 63355 (63355)
   Destination port: 53 (53)
   Sequence number: 190644224
   Header length: 20 bytes
   Flags: 0x0002 (SYN)
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
   Window size: 17659
   Checksum: 0xb25b
```

1. Source of trace:

   - My network

2. Detect was generated by:

   - Black Ice Defender

3. Probability the source address was spoofed:

   - Highly likely
   - The addresses are different, however the packets are arriving so close together that it seems like a program which is randomly generating IP addresses

4. Description of attack:

   - Denial of service of port 53 (DNS)

5. Attack mechanism:

   - Attacker is sending an enormous amount of packets to port 53; hoping to deny legitimate DNS requests

6. Correlations:

- DNS servers are frequently targeted by attackers
- More information can be found at: http://www.cert.org/advisories/CA-98-13-tcp-denial-of-service.html

7. Evidence of active targeting:

- There is evidence of active targeting

8. Severity:

- (Critical + Lethal) – (System + Countermeasures) = Severity
- (3 + 4) – (4 + 5) = -2

9. Defensive recommendations:

- Defenses are fine; attack blocked by firewall
- Apply filters to your IDS, and routers

10. Test question:

This attack is an example of:

a) SYN flood
b) Denial of service
c) Attack against DNS server
d) All of the above

Answer is d)