Stephen Thomas GIAC Practical

Detect 1:

```
00:38:12.843874 bftoemail2.bigfoot.com.4657 > destMachine.net.25: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
00:38:16.116315 bftoemail2.bigfoot.com.4657 > destMachine.net.25: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
00:38:22.678569 bftoemail2.bigfoot.com.4657 > destMachine.net.25: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
00:38:34.192352 sys-216.89.174.43.primary.net.3900 > destMachine.net.80: S
81445974:81445974(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:35.807035 bftoemail2.bigfoot.com.4657 > destMachine.net.25: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
00:38:37.095833 sys-216.89.174.43.primary.net.3900 > destMachine.net.80: S
81445974:81445974(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:43.138722 sys-216.89.174.43.primary.net.3900 > destMachine.net.80: S
81445974:81445974(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:53.210921 ppp-208-15-96-147.dialup.ltrkar.swbell.net.1468 > destMachine.net.80: S
7938988:7938988(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:55.188914 sys-216.89.174.43.primary.net.3900 > destMachine.net.80: S
81445974:81445974(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:56.190984 ppp-208-15-96-147.dialup.ltrkar.swbell.net.1468 > destMachine.net.80: S
7938988:7938988(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
00:38:56.724175 mta116.mail.yahoo.com.14941 > destMachine.net.25: S
2211145006:2211145006(0) win 16384 <mss 1460> (DF)
00:38:59.578929 mta116.mail.yahoo.com.14941 > destMachine.net.25: S
2211145006:2211145006(0) win 16384 <mss 1460> (DF)
00:39:02.172491 ppp-208-15-96-147.dialup.ltrkar.swbell.net.1468 > destMachine.net.80: S
7938988:7938988(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   A) The probability the source addresses were spoofed is low. In the case of this attack technique, the attacker would want to make it difficult to determine which of the scanning IP addresses is initiating the scan.
   B) I tested this theory on my internal network with the use of nmap and tcpdump. The following is from that test:

```
                    *******Scan******
09:42:56.575176 scanner.net.47214 > target.net.telnet: S 2009299799:2009299799(0) win 1024
(DF)
09:42:56.575304 10.1.2.3.47214 > target.net.telnet: S 2009299799:2009299799(0) win 1024
(DF)
09:42:56.575428 10.1.2.4.47214 > target.net.telnet: S 2009299799:2009299799(0) win 1024
(DF)
                    ****** Response******
```

```
09:42:56.576492 scanner.net.47214 > target.net.telnet: R 2009299800:2009299800(0) win 0
(DF)
09:42:56.577903 10.1.2.3.47214 > target.net.telnet: R 2009299800:2009299800(0) win 0
09:42:56.579243 10.1.2.4.47214 > target.net.telnet: R 2009299800:2009299800(0) win 0
```

In this detect you can't tell which machine actually initiated the nmap scan. The scanner.net machine is where the nmap scan was ran from. Howerver, with this detect you can see that all three machines responded with RESETs.

4. Description of Attack:
   A) The attacker is performing a port scan for well known services (Mail[smtp(25)]/Web Server[http(80)) possibly available on destMachine.net.
   B) The technique used is the decoy method.

5. Attack Mechanism:
   The decoy method initiates SYN packets on be half of an existing or non-existing host. However, in this case existing host. These packets are destined for particular ports (Services) on a targeted machine. If the targeted machine responds with a SYN-ACK, the attacker knows the attacked port is open. With this, known weaknesses for the services on open ports can be launched. The NMAP tool offers this type of scanning.

6. Correlations:
   This attack was described in SANS2000 supplied text "Intrusion Detection and Packet Filtering: How It Really Works" by Vicki Irwin, Psionic Software & Hal Pomeranz, Deer Run Associates. This attack is depicted on page 149 of the manual. I also found reference of this attack at the Whitehats Networks Security website at the following link:
   http://www.whitehats.com/nmap.

7. Evidence of active targeting:
   This activity was directed against the specific ports on the targeted machine (destMachine.net).

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (5 + 3) – (3 + 4) = 1

9. Defensive recommendations:
   The defense of the attacked machine is good. Use of a personal firewall with the highest security settings is in place.

10. Multiple choice question:
    What type of scanning technique is depicted by the trace?
    A) Reverse ident scanning
    B) Stealthy Host Discovery
    C) Decoy scanning
    D) None of the above
    ANSWER: D

Detect 2:

```
13:51:26.146443 24.94.23.13 > 204.210.227.34: icmp: echo request (frag 60476:1480@0+)
13:51:26.207030 24.94.23.13 > 204.210.227.34: (frag 60476:1480@1480+)
13:51:26.242469 24.94.23.13 > 204.210.227.34: (frag 60476:1480@2960+)
13:51:26.260830 24.94.23.13 > 204.210.227.34: (frag 60476:1480@4440+)
.
.
.
13:51:27.679779 24.94.23.13 > 204.210.227.34: (frag 60476:1480@47360+)
13:51:27.704113 24.94.23.13 > 204.210.227.34: (frag 60476:1480@48840+)
13:51:27.748244 24.94.23.13 > 204.210.227.34: (frag 60476:1480@50320+)
13:51:27.773712 24.94.23.13 > 204.210.227.34: (frag 60476:1480@51800+)
13:51:27.827848 24.94.23.13 > 204.210.227.34: (frag 60476:1480@53280+)
13:51:27.888127 24.94.23.13 > 204.210.227.34: (frag 60476:1480@54760+)
13:51:30.145635 24.94.23.13 > 204.210.227.34: icmp: echo request (frag 60732:1480@0+)
13:51:30.173316 24.94.23.13 > 204.210.227.34: (frag 60732:1480@1480+)
13:51:30.194334 24.94.23.13 > 204.210.227.34: (frag 60732:1480@2960+)
13:51:30.228503 24.94.23.13 > 204.210.227.34: (frag 60732:1480@4440+)
.
.
.
13:51:31.125115 24.94.23.13 > 204.210.227.34: (frag 60732:1480@32560+)
13:51:31.175807 24.94.23.13 > 204.210.227.34: (frag 60732:1480@34040+)
13:51:31.213556 24.94.23.13 > 204.210.227.34: (frag 60732:1480@35520+)
13:51:31.265879 24.94.23.13 > 204.210.227.34: (frag 60732:1480@37000+)
13:51:31.311834 24.94.23.13 > 204.210.227.34: (frag 60732:1480@38480+)
13:51:31.364825 24.94.23.13 > 204.210.227.34: (frag 60732:1480@39960+)
13:51:31.423310 arp who-has 204.210.227.1 tell 204.210.227.34
13:51:31.439004 24.94.23.13 > 204.210.227.34: (frag 60732:1480@41440+)
13:51:31.440690 arp reply 204.210.227.1 is-at 8:0:3e:7:d9:22
13:51:31.440905 204.210.227.34 > 24.94.23.13: icmp: ip reassembly time exceeded
```

***** Condensed to save space *****

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   There is a low probability that the source address was spoofed. The address is from an ISP (RoadRunner).

4. Description of Attack:
   The attacker is performing a Denial of Service (DOS) attack on 204.210.227.34.

5. Attack Mechanism:
   A) The attacker first initiates an ICMP echo request signifying that it is the first packet of a fragmented datagram.
   B) The attacker next fabricates fragmented packets that will always have the more fragments bit set. This would cause the attacked machine to wait for the last packet for

some set time dictated by the machines underlying Operating System (OS). Hence, the "icmp: ip reassembly time exceeded" message in the trace. However, the multiple generation of these fragmented datagrams could cause a machine to lockup or behave abnormally. The targeted machine's OS was susceptible to this attack.

6. Correlations:
   The usage of DOS attacks was discussed multiple times in the SANS2000 Intrusion Detection Analysis Class. Yet, I found some more information about various Denial of Service attacks on the following link:
   http://www.winplanet.com/winplanet/reports/561/1/

7. Evidence of active targeting:
   With this trace I suspect that the attacker may have first completed some reconnaissance for live machines prior to this attack.

8. Severity:
   (Criticality + Lethality)-(System + Net Countermeasures) = Severity
   (5 + 4) – (3 + 4) = 2

9. Defensive recommendations:
   A) Make sure the OS of attacked machine is patched with the latest bug and upgrade releases.
   B) Contact ISP about activity of the originating source of attack.
   C) Install packet-filtering router so ICMP echo requests are blocked.

10. Multiple choice question:
    What appears to be the goal of the attacker in this trace?
    A) Mapping of possible attack candidates
    B) Initiate a covert channel attack
    C) Perform a Denial of Service attack
    D) Initiate a Teardrop Attack
    ANSWER: C

Detect 3:

```
18:45:18.698646 204.210.227.34.2781 > 204.210.252.249.110: S 424275049:424275049(0) win
8192 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) [tos 0x5c]
18:45:18.753488 204.210.252.249.110 > 204.210.227.34.2781: S 1829302751:1829302751(0)
ack 424275050 win 34752 <nop,nop,timestamp 410565795 0,nop,wscale 0,mss 1460> (DF)
18:45:18.753806 204.210.227.34.2781 > 204.210.252.249.110: . ack 1 win 8760
<nop,nop,timestamp 4080123 410565795> (DF) [tos 0x5c]
18:45:18.860682 204.210.252.249.110 > 204.210.227.34.2781: P 1:166(165) ack 1 win 34752
<nop,nop,timestamp 410565806 4080123> (DF)
18:45:18.861779 204.210.227.34.2781 > 204.210.252.249.110: P 1:16(15) ack 166 win 8595
<nop,nop,timestamp 4080124 410565806> (DF) [tos 0x5c]
18:45:18.873997 204.210.252.249.110 > 204.210.227.34.2781: . ack 16 win 34752
<nop,nop,timestamp 410565807 4080124> (DF)
18:45:18.880607 204.210.252.249.110 > 204.210.227.34.2781: P 166:202(36) ack 16 win 34752
<nop,nop,timestamp 410565808 4080124> (DF)
18:45:18.881637 204.210.227.34.2781 > 204.210.252.249.110: P 16:34(18) ack 202 win 8559
<nop,nop,timestamp 4080124 410565808> (DF) [tos 0x5c]
18:45:18.955268 204.210.252.249.110 > 204.210.227.34.2781: P 202:246(44) ack 34 win 34752
<nop,nop,timestamp 410565815 4080124> (DF)
18:45:18.956270 204.210.227.34.2781 > 204.210.252.249.110: P 34:40(6) ack 246 win 8515
<nop,nop,timestamp 4080124 410565815> (DF) [tos 0x5c]
18:45:19.020992 204.210.252.249.110 > 204.210.227.34.2781: P 246:259(13) ack 40 win 34752
<nop,nop,timestamp 410565822 4080124> (DF)
18:45:19.021956 204.210.227.34.2781 > 204.210.252.249.110: P 40:46(6) ack 259 win 8502
<nop,nop,timestamp 4080125 410565822> (DF) [tos 0x5c]
18:45:19.059561 204.210.252.249.110 > 204.210.227.34.2781: P 259:321(62) ack 46 win 34752
<nop,nop,timestamp 410565826 4080125> (DF)
18:45:19.060738 204.210.227.34.2781 > 204.210.252.249.110: P 46:52(6) ack 321 win 8440
<nop,nop,timestamp 4080126 410565826> (DF) [tos 0x5c]
18:45:19.110326 204.210.252.249.110 > 204.210.227.34.2781: P 321:697(376) ack 52 win
34752 <nop,nop,timestamp 410565831 4080126> (DF)
18:45:19.111434 204.210.227.34.2781 > 204.210.252.249.110: P 52:58(6) ack 697 win 8064
<nop,nop,timestamp 4080126 410565831> (DF) [tos 0x5c]
18:45:19.184046 204.210.252.249.110 > 204.210.227.34.2781: P 697:759(62) ack 58 win 34752
<nop,nop,timestamp 410565838 4080126> (DF)
18:45:19.184250 204.210.252.249.110 > 204.210.227.34.2781: F 759:759(0) ack 58 win 34752
<nop,nop,timestamp 410565838 4080126> (DF)
18:45:19.184478 204.210.227.34.2781 > 204.210.252.249.110: . ack 760 win 8002
<nop,nop,timestamp 4080127 410565838> (DF) [tos 0x5c]
18:45:19.185495 204.210.227.34.2781 > 204.210.252.249.110: F 58:58(0) ack 760 win 8002
<nop,nop,timestamp 4080127 410565838> (DF) [tos 0x5c]
18:45:19.215096 204.210.252.249.110 > 204.210.227.34.2781: . ack 59 win
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   A) There is a low probability that the source address was spoofed.

B) The source machine is initiating communication with the local mail server.

4. Description of Attack:
   The probability of an attack is low. The initiating source machine (204.210.227.34) and destination mail server machine (pop3, port 110, address 204.210.252.249) both exist within the same confounds of a mutual ISPs network address space.

5. Attack Mechanism:
   The source machine has a user mail client process that is conversing with the mail server to download mail. The client application opens up an ephemeral port to communicate with the destination host on port 110. If the source machine supplies the correct user access information it should be allowed to accomplish the task. If not communication should be halted. The process follows the TCP three-way handshake scenario. It evens closes the connection with a FYN/ACK by both the source and destination.

6. Correlations:
   I conducted further investigation on a controlled connection in which I forced the mail server to request a password from the connecting client mail process. The supplied password was incorrectly keyed twice. The trace of both of these connections resembled the aforementioned one above. However, the connections were closed immediately after the invalid passwords were supplied, whereas in the case of a successful connection sever PUSH packets were negotiated by both involved parties.

7. Evidence of active targeting:
   The nature of the connection would indicate that the client was non-maliciously targeting the mail server. Yet, be wary of multiple closely timed connections to the mail server in which successful opened and closed portals have minimal PUSH packets during the TCP client/server communiqué process.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (4 + 5) - (5 + 5) = -1

9. Defensive recommendations:
   A) Make sure operating system and underlying pop3 mail server software is patched to latest versions.
   B) Make sure firewall is in place with filters to watch for brute force attacks to the mail server.

10. Multiple choice question:
    The trace signifies what type of protocol connection?
    A) UDP connection to a RPC NFS server
    B) ICMP request-reply of a known host
    C) TCP connection to a pop3 mail server
    D) FAILED TCP three-way handshake between a source and destination machine
    ANWSER: C

Detect 4:

```
12:36:56.298779 188.200.104.2.4020 > 188.200.104.40.telnet: S 13347083:13347083(0) win
8192 <mss 1460> (DF)
12:36:56.298826 188.200.104.40.telnet > 188.200.104.2.4020: S 242791709:242791709(0) ack
13347084 win 8760 <mss 1460> (DF)
12:36:56.299373 188.200.104.2.4020 > 188.200.104.40.telnet: . ack 1 win 8760 (DF)
12:36:56.328674 188.200.104.2.4021 > 188.200.104.40.telnet: S 13347120:13347120(0) win
8192 <mss 1460> (DF)
12:36:56.328737 188.200.104.40.telnet > 188.200.104.2.4021: S 242877168:242877168(0) ack
13347121 win 8760 <mss 1460> (DF)
12:36:56.329307 188.200.104.2.4021 > 188.200.104.40.telnet: . ack 1 win 8760 (DF)
.
.
.
12:36:56.336872 188.200.104.2.4020 > 188.200.104.40.telnet: P 1:16(15) ack 1 win 8760 (DF)
12:36:56.337013 188.200.104.40.telnet > 188.200.104.2.4020: . ack 16 win 8760 (DF)
12:36:56.338079 188.200.104.2.4021 > 188.200.104.40.telnet: P 1:16(15) ack 1 win 8760 (DF)
12:36:56.338164 188.200.104.40.telnet > 188.200.104.2.4021: . ack 16 win 8760 (DF)
.
.
.
12:47:06.607326 188.200.104.2.4020 > 188.200.104.40.telnet: F 16:16(0) ack 25 win 8736 (DF)
12:47:06.607386 188.200.104.40.telnet > 188.200.104.2.4020: . ack 17 win 8760 (DF)
12:47:06.607529 188.200.104.2.4059 > 188.200.104.40.telnet: F 79:79(0) ack 99 win 8662 (DF)
12:47:06.607622 188.200.104.40.telnet > 188.200.104.2.4059: . ack 80 win 8760 (DF)
12:47:06.607798 188.200.104.2.4022 > 188.200.104.40.telnet: F 16:16(0) ack 25 win 8736 (DF)
12:47:06.607826 188.200.104.40.telnet > 188.200.104.2.4022: . ack 17 win 8760 (DF)
12:47:06.608137 188.200.104.2.4052 > 188.200.104.40.telnet: F 132:132(0)
```

***** Condensed to save space *****

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using tcpdump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   A) Low probability address was spoofed.
   B) Both machines are on the same intranet segment.
   C) Utilization of an telnet attack would dictate that the attacking source machine is under control of the attacker.

4. Description of Attack:
   A) Attempted connection to the telnet server process on destination machine (destMachine).
   B) Source machine initiates multiple connections (SYN) from incrementing ephemeral ports with closely time-stamped packets to the telnet server process on destination machine (destMachine).

5. Attack Mechanism:

The closely time-stamped packets would signify an application aided brute force attack against the telnet process. This is backed up with the following section of the /etc/messages file of the attacked machine:

```
May 18 12:37:17 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/19
FROM 188.200.104.2
May 18 12:37:17 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/22
FROM 188.200.104.2
May 18 12:37:58 188.200.104.40 last message repeated 1 time
May 18 12:37:58 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/19
FROM 188.200.104.2
May 18 12:38:39 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/22
FROM 188.200.104.2
May 18 12:38:39 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/19
FROM 188.200.104.2
May 18 12:39:20 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/22
FROM 188.200.104.2
May 18 12:40:02 188.200.104.40 last message repeated 1 time
May 18 12:40:44 188.200.104.40 login: REPEATED LOGIN FAILURES ON /dev/pts/22
FROM 188.200.104.2
```

6. Correlations:
   I found reference of this type of an attack at the following web links:
   http://advice.networkice.com/advice/Intrusions/2001608/default.htm
   http://grc.com/su-danger.htm

7. Evidence of active targeting:
   The evidence of active targeting is high. By attacking the telnet process, the hacker shows he/she had acquired prior knowledge that the recipient of the assault was indeed a UNIX machine.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (2 + 5) – (3 + 2) = 2

9. Defensive recommendations:
   A) Make sure users employ strong passwords consisting of the following:
      - Length greater than 7 characters
      - Mix of upper case and lower case
      - Use of numbers and punctuation
   B) Install latest OS and patches to latest level.
   C) Dictate good use policy to users of machines resident within the Intranet in question.

10. Multiple choice question
    Which of the following is true of the destination host shown in the trace?
    A) Telnet port is open
    B) Communicates with the source machine on unique ephemeral ports
    C) The telnet service running on the destination machine responds with an SYN/ACK
    D) All of the above
    ANSWER: D

Detect 5:

```
16:08:53.489875 212.161.41.70.3169 > destMachine.net.53: S 3327978309:3327978309(0) win
32120 <mss 1460,sackOK,timestamp 12544598 0,nop,wscale 0> (DF)
16:08:56.483360 212.161.41.70.3169 > destMachine.net.53: S 3327978309:3327978309(0) win
32120 <mss 1460,sackOK,timestamp 12544898 0,nop,wscale 0> (DF)
16:09:02.637578 212.161.41.70.3169 > destMachine.net.53: S 3327978309:3327978309(0) win
32120 <mss 1460,sackOK,timestamp 12545498 0,nop,wscale 0> (DF)
16:09:14.481878 212.161.41.70.3169 > destMachine.net.53: S 3327978309:3327978309(0) win
32120 <mss 1460,sackOK,timestamp 12546698 0,nop,wscale 0> (DF)
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   Low probability the source address was spoofed. There was a live host at the source.

4. Description of Attack:
   This trace denotes an attacker(212.161.41.70) is tying to query the destination host (destMachine.net) for a Domain Name Server(port 53). This could have been a network scan. The attacker may have been using random addresses. The destination host may have been the only attacked machine on its particular subnet.

5. Attack Mechanism:
   The attacker is looking for a particular service to be available on the targeted system. This is done by rapidly sending SYN packets to the port of the besieged machine(s). If a targeted host responds to the probe with a RESET, then the attacker knows that the targeted service is not available. However, if the targeted machine responds to the SYN with a SYN-ACK combination, then the attacker knows the service is available.

6. Correlations:
   This attack was described in SANS2000 supplied text "Intrusion Detection and Packet Filtering: How It Really Works" by Vicki Irwin, Psionic Software & Hal Pomeranz, Deer Run Associates. This attack is depicted on page 111 of the manual.

7. Evidence of active targeting:
   This is a random generated attack since the destination host has a DHCP address. However, this scan is reconnaissance to target machines for possible later intrusion.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (2 + 1) – (3 + 4) = -4

9. Defensive recommendations:
   A) This scan was not successful. The DNS service is unavailable on the attacked machine.
   B) Inventory of running servers and their accompany ports should be done.

10. Multiple choice question:
    The attacker was looking for which of the following services?

A) SMT
B) SNMP
C) POP3
D) DNS
ANSWER: D

Detect 6:

```
17:58:18.798839 sourceMach.43001 > destMach.111: S 1332016810:1332016810(0) win 8192
<mss 1460> (DF) (ttl 128, id 41148)
17:58:18.798900 destMach.111 > sourceMach.43001: S 863642613:863642613(0) ack
1332016811 win 8760 <mss 1460> (DF) (ttl 255, id 28159)
17:58:18.799431 sourceMach.43001 > destMach.111: . ack 1 win 8760 (DF) (ttl 128, id 41404)
17:58:18.799690 sourceMach.43001 > destMach.111: P 1:45(44) ack 1 win 8760 (DF) (ttl 128, id
41660)
17:58:18.799747 destMach.111 > sourceMach.43001: . ack 45 win 8716 (DF) (ttl 255, id 28160)
17:58:18.801780 destMach.111 > sourceMach.43001: P 1:1313(1312) ack 45 win 8760 (DF) (ttl
255, id 28161)
17:58:18.883381 sourceMach.43001 > destMach.111: R 1332016855:1332016855(0) win 0 (DF)
(ttl 128, id 41916)
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using tcpdump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**][**urgent**][**options**]

3. Probability the source address was spoofed:
   The probability the source address was spoofed is low. The source of the scan is a active known windows NT machine.

4. Description of Attack:
   A) This is not an attack. However, the machine has successfully established a connection with the Remote Procedure Communication (RPC) service running on port 111 of machine at destMach. If you notice that the machine running the service actually only pushes one large packet of data to the source machine (sourceMach). The source seems to be attempting reconnaissance.
   B) The minimum exchange of data would lower probability of some type of buffer overflow attack.

5. Attack Mechanism:
   The source machine first initiates a legitimate TCP three-way handshake with the portmapper service on the destination machine. The source machine upon successful communication pushes bytes to the portmapper process. This would be some type of request. The portmapper service responds as denoted in the trace with the pushing of 1312 bytes. The source machine sends a reset to close the connection instead of a FYN/ACK.

6. Correlations:
   A) I later ran a rpcinfo –p on a resident UNIX machine while I was tracing the connection with tcpdump. The output looked similar to the above detect.
   B) This type of query was described in SANS2000 supplied text “Intrusion Detection Workshop” by Stephen Northcutt. The referring text starts on page 173.

7. Evidence of active targeting:
   It appears the source of the scan had prior knowledge that the targeted machine housed a UNIX OS. Thus, he/she may have already done prior OS directed mapping scans of subnet.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (2 + 1) – (3 + 2) = -2

9. Defensive recommendations:
   A) Turn off any unnecessary rpc based services.
   B) Install rpc(portmapper) wrapper scripts.

10. Multiple choice question:
    What can be gained by an attacker in respects to the supplied detect?
    A) Attacker can gain access to all available server processes
    B) Attacker could query the portmapper to find out what rpc services are available
    C) Initiate a UDP port scan
    D) Map of all active TCP and UDP protocol oriented services
    ANSWER: B

Detect 7:

```
17:28:19.566622 host62-7-95-161.btinternet.com.1596 > destMach.31337: udp 18
17:28:19.566969 destMach > host62-7-95-161.btinternet.com: icmp: destMach udp port 31337
unreachable
17:32:50.885337 host62-7-95-161.btinternet.com.1596 > destMach.31337: udp 18
17:32:50.885663 destMach > host62-7-95-161.btinternet.com: icmp: destMach udp port 31337
unreachable
17:34:48.008320 host62-7-95-161.btinternet.com.1596 > destMach.139: udp 18
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   The probability the address was spoofed is low. Upon further research address was found to belong to a British ISP.

4. Description of Attack:
   The attacker was conducting a Trojan Horse ping for the remote administrative program Back Orifice.

5. Attack Mechanism:
   A) The attacker is utilizing the Back Orifice client to query the destination machine for it's server component which uses UDP as the transport protocol.
   B) The attacker seems to be a script kiddie. Please note the bold text in the following hex dump portion of the detect:

```
17:34:48.008320 host62-7-95-161.btinternet.com.1596 > destMach.139: udp 18
                                  4500 002e 5d56 0000 3011 dfcb 3e07 5fa1
                                  ccd2 e322 063c 008b 001a 58fb ce63 d1d2
                                  16e7 13cf 39a5 a586 b275 4b99 aa32
```

   The default string "**ce63 d1d2 16e7 13cf"** is contained in each packet that originates from the attacker. This is reminiscent of the old version of Back Orifice.

6. Correlations:
   This attack was described in SANS2000 supplied text "Intrusion Detection and Packet Filtering: How It Really Works" by Vicki Irwin, Psionic Software & Hal Pomeranz, Deer Run Associates. The Back Orifice trojan attack depiction starts on page 101 of the manual.

7. Evidence of active targeting:
   I think the possibility of targeting is low in this case. The origination of the attack is from an address that belongs to the address space of an ISP. The attacker is inexperienced and is probably randomly picking a subnet and trying various addresses within that address space.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (2 + 5) – (3 + 4) = 0

9. Defensive recommendations:
   A) Make sure latest anti-virus software and updates are installed on targeted machine.

B) Make sure firewall is set to filter any scans and or communication trying to reference this trojan.

10. Multiple choice question:
    The detect shows a scan for what type of an attack method?
    A) Buffer Overflow
    B) Trojan Horse
    C) Teardrop
    D) Man in the middle
    ANSWER: B

Detect 8:

```
17:59:36.640146 192.100.201.12.746 > 175.24.104.4.59820: udp 96 (DF)
17:59:36.641498 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.644905 192.100.201.12.746 > 175.24.104.4.59820: udp 96 (DF)
17:59:36.645288 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.647572 192.100.201.12.746 > 175.24.104.4.59820: udp 92 (DF)
17:59:36.647859 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.650209 192.100.201.12.746 > 175.24.104.4.59820: udp 88 (DF)
17:59:36.650508 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.653421 192.100.201.12.746 > 175.24.104.4.59820: udp 60 (DF)
17:59:36.653699 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.656694 192.100.201.12.746 > 175.24.104.4.59820: udp 92 (DF)
17:59:36.656984 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.660490 192.100.201.12.746 > 175.24.104.4.59820: udp 88 (DF)
17:59:36.660780 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.663696 192.100.201.12.746 > 175.24.104.4.59820: udp 92 (DF)
17:59:36.663990 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.667072 192.100.201.12.746 > 175.24.104.4.59820: udp 68 (DF)
17:59:36.667360 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
17:59:36.669814 192.100.201.12.746 > 175.24.104.4.59820: udp 60 (DF)
17:59:36.670087 175.24.104.4.59820 > 165.77.15.88.746: udp 88 (DF)
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using tcpdump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   A) There is a high probability both addresses were spoofed. The address 192.100.201.12 belongs to an application server. Yet, the 175.24.104.4 belongs to a UNIX desktop.
   B) The same port numbers are being used for each successive connection between the two machines.

4. Description of Attack:
   This is an UDP Flood attack.

5. Attack Mechanism:
   A) The attacker spoofs the addresses of the target machines.
   B) The targeted machines establish a connection between two UDP services that both produce output.
   C) With these two services on either machines responding to each other, a very high number of packets can be generated that can lead to a denial of service on the machine(s) where the services are offered. Yet, in this case the two port numbers used are not of known services. Moreover, this could also cause bandwidth issues if enough machines are attacked on the same network at the same time.

6. Correlations:
   A) This attack was described in SANS2000 supplied text “Intrusion Detection and Packet Filtering: How It Really Works” by Vicki Irwin, Psionic Software & Hal Pomeranz, Deer Run Associates. The attack in question is on page 87.

B) The other reference to this type of attack can be seen at the cert.org web site at the following advisory:

CA-96.01.UDP_service_denial

7. Evidence of active targeting:
   The evidence of active targeting is high. Due to the nature of this attack these machine could have been part of a more distributed attack.

8. Severity:
   (Critical + Lethal)-(System + Net Countermeasures) = Severity
   (4 + 4) + (3 + 2) = 3

9. Defensive recommendations:
   A) Disable all unused UDP services on hosts.
   B) Block all UDP ports outgoing and incoming with the exception of specific services that are required at firewalls.

10. Multiple choice question:
    The UDP flooding in this detect is also know as what type of an attack?
    A) Network Mapping
    B) Fragmented IGMP Attack
    C) UDP Denial of Service Attack
    D) Teardrop Attack
    ANSWER: C

Detect 9:

```
23:38:13.341697 dppp23.cura.net.3433 > destMach.net.12345: S 10326433:10326433(0) win
8192 <mss 1460> (DF)
23:38:13.355687 destMach.net.12345 > dppp23.cura.net.3433: R 0:0(0) ack 10326434 win 0
23:38:16.559964 dppp23.cura.net.3433 > destMach.net.12345: S 10326433:10326433(0) win
8192 <mss 1460> (DF)
23:38:16.560329 destMach.net.12345 > dppp23.cura.net.3433: R 0:0(0) ack 1 win 0
23:38:17.079546 dppp23.cura.net.3433 > destMach.net.12345: S 10326433:10326433(0) win
8192 <mss 1460> (DF)
23:38:17.079900 destMach.net.12345 > dppp23.cura.net.3433: R 0:0(0) ack 1 win 0
23:38:17.901637 dppp23.cura.net.3433 > destMach.net.12345: S 10326433:10326433(0) win
8192 <mss 1460> (DF)
23:38:17.901991 destMach.net.12345 > dppp23.cura.net.3433: R 0:0(0) ack 1 win 0
```

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using windump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   There is a low probability that the address was spoofed. The address belongs to an ISP. Either the attacker is using his/her machine or the source address is from a commandeered machine. I tried to ping the machine and of course it was not responsive. Seeing that this addressed is from an ISP the attacker could have released the attacking machines IP address and gotten a new lease; thus, retaining a new address.

4. Description of Attack:
   This is not an attack. However, this is a scan for the Netbus trojan(server) process on the targeted machine.

5. Attack Mechanism:
   A) The attacker sends the target server on the Netbus port (12345) a SYN. If the targeted machine responds back with a SYN/ACK then the service is listening on that port. However, if the service were not available a RESET/ACK would be the response.
   B) Once it is determined that the Netbus server is available, the attacker could initiate the client portion of this tool on their own or hijacked machine directed at the server running on the targeted machine.

6. Correlations:
   A) I found reference of this at the CERT Coordination Center under the following CERT Summary:
      CS-99-01
   B) I also found info on this at the xforce.iss.net website at the following link:
      http://xforce.iss.net/alerts/advise8.php#list

7. Evidence of active targeting:
   This scan itself could be considered active targeting. The attacker is gearing up for an attack on positive Netbus server responses.

8. Severity:

(Criticality + Lethality)-(System + Net Countermeasures) = Severity
(4 + 1) – (3 + 4) = -2

9. Defensive recommendations:
   A) Make sure virus software is at the latest level along with any current patches and signature updates.
   B) Set firewall to filter any incoming communication to TCP port 12345 or 12346.

10. Multiple choice question:
    The attacker is scanning for what Trojan Horse server process?
    A) Back Orifice
    B) Wintrinoo
    C) Netbus
    D) TFN2K
    ANSWER: C

Detect 10:

```
17:27:54.883628 188.30.104.2.1576 > 188.30.104.4.23: S 16405497:16405497(0) win 8192
<mss 1460> (DF)
17:27:54.883676 188.30.104.4.23 > 188.30.104.2.1576: S 628766864:628766864(0) ack
16405498 win 8760 <mss 1460> (DF)
17:27:54.884217 188.30.104.2.1576 > 188.30.104.4.23: . ack 1 win 8760 (DF)
17:27:54.937010 188.30.104.4.23 > 188.30.104.2.1576: P 1:16(15) ack 1 win 8760 (DF)
17:27:54.937754 188.30.104.2.1576 > 188.30.104.4.23: P 1:4(3) ack 16 win 8745 (DF)
.
.
.
17:27:55.883275 188.30.104.4.23 > 188.30.104.2.1576: . ack 36 win 8760 (DF)
17:27:55.935555 188.30.104.2.1576 > 188.30.104.4.23: P 36:39(3) ack 28 win 8733 (DF)
17:27:55.983281 188.30.104.4.23 > 188.30.104.2.1576: . ack 39 win 8760 (DF)
17:27:56.036156 188.30.104.2.1576 > 188.30.104.4.23: R 16405536:16405536(0) win 0 (DF)
17:27:56.042193 188.30.104.2.1577 > 188.30.104.4.23: S 16406701:16406701(0) win 8192
<mss 1460> (DF)
17:27:56.042270 188.30.104.4.23 > 188.30.104.2.1577: S 629025467:629025467(0) ack
16406702 win 8760 <mss 1460> (DF)
17:27:56.042827 188.30.104.2.1577 > 188.30.104.4.23: . ack 1 win 8760 (DF)
17:27:57.074965 188.30.104.4.23 > 188.30.104.2.1577: P 1:16(15) ack 1 win 8760 (DF)
17:27:57.075735 188.30.104.2.1577 > 188.30.104.4.23: P 1:4(3) ack 16 win 8745 (DF)
.
.
.
17:27:57.075778 188.30.104.4.23 > 188.30.104.2.1577: . ack 4 win 8760 (DF)
17:27:58.068670 188.30.104.2.1577 > 188.30.104.4.23: P 36:39(3) ack 28 win 8733 (DF)
17:27:58.113336 188.30.104.4.23 > 188.30.104.2.1577: . ack 39 win 8760 (DF)
17:27:58.169213 188.30.104.2.1577 > 188.30.104.4.23: R 16406740:16406740(0) win 0 (DF)
17:27:58.175396 188.30.104.2.1578 > 188.30.104.4.23: S 16408785:16408785(0) win 8192
<mss 1460> (DF)
17:27:58.175463 188.30.104.4.23 > 188.30.104.2.1578: S 629321938:629321938(0) ack
16408786 win 8760 <mss 1460> (DF)
17:27:58.176031 188.30.104.2.1578 > 188.30.104.4.23: . ack 1 win 8760 (DF)
17:27:59.215147 188.30.104.4.23 > 188.30.104.2.1578: P 1:16(15) ack 1 win 8760 (DF)
17:27:59.215906 188.30.104.2.1578 > 188.30.104.4.23: P 1:4(3) ack 16 win 8745 (DF)
.
.
.
17:28:00.153385 188.30.104.4.23 > 188.30.104.2.1578: . ack 36 win 8760 (DF)
17:28:00.211783 188.30.104.2.1578 > 188.30.104.4.23: P 36:39(3) ack 28 win 8733 (DF)
17:28:00.253367 188.30.104.4.23 > 188.30.104.2.1578: . ack 39 win 8760 (DF)
17:28:00.312353 188.30.104.2.1578 > 188.30.104.4.23: R 16408824:16408824(0) win 0 (DF)
```

***** Condensed to save space *****

1. Source of trace:
   The trace originated from my network.

2. Detect was generated by:
   A) This detect was generated from raw data using tcpdump.
   B) The fields are as follows:
   [**Timestamp**][**src**]>[**dst**]:[**flags**][**data-sequence number**][**ack**][**window**]
   [**urgent**][**options**]

3. Probability the source address was spoofed:
   The probability the source the address was spoofed was low. This is a live machine resident on the same subnet as the attacked machine.

4. Description of Attack:
   This is a Denial of Service (DOS) attack. The source machine is bombarding the destination machine's telnet service (23).

5. Attack Mechanism:
   A) The source machine first initiates a legitimate TCP three-way handshake with the telnet service on the destination machine.
   B) Upon successful negotiation of the connection the attacking machines pushes data consisting of small amounts of data in this case 3 bytes.
   C) The source machine later sends the targeted machine a RESET. Which will end the session.

   The above steps are repeated within small time frames during each new connection. Also notice the sequential numbering of the source port of each new connection. This fact with the minute time expenditure and above facets would signify automation of some type.

6. Correlations:
   Information on what a normal telnet session should look like can be seen on page 214 of the SANS2000 supplied text “Intrusion Detection Analysis – Shadow Style” by Judy Novak, The SANS Institute

7. Evidence of active targeting:
   Since both machine exist within the same intranet the attacker would have access to host maps with legitimate machines. However, earlier detects did not denote any active targeting.

8. Severity:
   (Criticality + Lethality)-(System + Net Countermeasures) = Severity
   (2 + 4) – (3 + 2) = 1

9. Defensive recommendations:
   A) Upgrade machine to latest OS and Patches.
   B) Notify system administrators of source of attack.

10. Multiple choice question:
    The initial process conducted by the source machine in this detect successfully completed what phase of a TCP connection?
    A) Two-way session termination
    B) Data transfer
    C) Ephemeral port initiation
    D) Three-way handshake
    ANSWER: D

Stephen Thomas
GIAC Extra Work Assignment

Day One Questions
Perimeter Defense:

1. What is the largest integer an octet can hold?
   A) 32
   B) 64
   C) 256
   D) None of the above
   ANSWER: D

2. Which of the following represents a Class B IP network address?
   A) 2206.19.25.4
   B) 127.206.65.7
   C) 185.77.8.9
   D) 192.10.3.4
   ANSWER: C

3. Which IP protocol utilizes a three-way handshake to establish a connection?
   A) UDP
   B) ICMP
   C) TCP
   D) IGMP
   ANSWER: C

4. Which of the following IP protocols are considered connectionless?
   A) TCP
   B) ICMP
   C) UDP
   D) ARP
   ANSWER: C

5. What is the communicating port number of the destination host in the following tcpdump output?
   12:24:38.286245 aa.net.1169 > bb.net.23: S 6987673:6987673(0) win
   8192 <mss 1460> (DF)
   A) 1169
   B) 6987673
   C) 286245
   D) 23
   ANSWER: D

6. Given a common fragment identification number, what other information must a packet fragment carry so the destination host can reassemble them back to the original unfragmented state?
   A) Its offset in the original unfragmented packet
   B) Length of data payload
   C) Tell whether or not if another fragment will follow
   D) All of the above
   ANSWER: D

7. Which of the following is true about ephemeral ports?
   A) Historically numbered below 1023

B) Port remains the same on each TCP connection
C) Reused after a connection is freed
D) A ephemeral port number originates from the Server on a TCP connection
ANSWER: C

8. In a DNS Domain, the secondary name server offers which of the following?
   A) DNS information maintained in flat text files
   B) Load balancing of response to queries
   C) Downloads of specific record changes
   D) Reliable zone transfers via UDP.

9. What is the maximum allowable size of data contained in a DNS datagram response?
   A) 256 bytes
   B) 512 bytes
   C) 484 bytes
   D) 680 bytes
   ANSWER: C

10. What is being communicated to a sending host when it receives an ICMP “Redirect” message?
    A) Destination host is responding with the optimum router to use for any preceding traffic to its location
    B) That a non-optimum router forwarded its traffic to the requested destination; however, a more optimum route is returned
    C) Responding router failed to forwarded traffic due to the fact the destination host is unreachable on its subnet
    D) None of the above

    ANSWER: C

Day Two Questions
Perimeter Defense:

11. What is not true of encapsulation in respects to the Internet Protocol model?
    A) It is the process of building a datagram with a previous layer data within the data portion of the datagram format on the preceding layer below it.
    B) Makes sure the frame, IP, and protocol headers are all adjacent.
    C) Help make IP be more hardware independent.
    D) Enhance the speed of datagrams across the network.
    ANSWER: D

12. Components of an ICMP datagram include which of the following?
    A) Acknowledgement number
    B) Source and destination port numbers
    C) Message type
    D) All of the above
    ANSWER: C

13. What Protocol is best served by an application that must have a guarantee of packet delivery and order?
    A) UDP
    B) TCP
    C) ICMP
    D) IGMP
    ANSWER: TCP

14. Which of the following tcpdump commands would detect all SMTP traffic originating from a machine with the IP address of 172.155.72.3?
    A) windump tcp[2:2]=25 and src host 172.155.73.3
    B) windump ip[9:2]=6 and src host 172.155.73.3
    C) windump tcp[0:2]=25 and src host 172.155.73.3
    D) None of the above
    ANSWER: A

15. Why would one choose to use a packet filtering router over a firewall?
    A) Inexpensive way to provide firewall security
    B) Less administrative cost
    C) If performance is an issue
    D) All of the above
    ANSWER: D

16. What is not true in the deployment of an Access Control List (ACL) on a router?
    A) ACLs can be applied to an interface of a router for incoming and out going packets
    B) An ACL may be used by multiple interfaces.
    C) A Interface can only have one inbound and one outbound access list a any given time
    D) ACLs are made up of individual rules.
    ANSWER: A

17. Why is the order of ACL rules important?
    A) Router reads ACL in its entirety
    B) Out of order rules of an ACL could allow traffic that was thought to be denied into your network
    C) ACL list follow a last match and exit behavior
    D) None of the above

ANSWER: B

18. Which of the following are good practices to follow when designing filters to identify specific attack signatures?
    A) Rarely trigger on non-attack traffic
    B) Find slight variations of the attack
    C) Are not overly complex
    D) All of the above
    ANSWER: D
19. Blocking ICMP echo-request and echo-reply is a good way to stop which of the following attacks?
    A) Teardrop Attacks
    B) Smurf Attacks
    C) Network Mapping
    D) ICMP Timestamp Attack
    ANSWER: B

20. Enabled small services on a machine could be used for what kind of action by an attacker?
    A) Map out a network
    B) Back Orifice scan
    C) Sesquipedalian DOS
    D) SOCKS port scan
    ANSWER: A

Day Three Questions
Perimeter Defense:

21. Which of the following is not a benefit of shadow?
    A) Tunable
    B) Provision for an audit trail of activity to and from network
    C) Uses snort as its collection software
    D) Will give an intimate view of network activity
    ANSER: C

22. What would be the correct tcpdump mask to determine if the don't fragment (DF) flag is set in an IP datagram?
    A) ip[06:2]&0x40
    B) ip[06:2]&0x20
    C) tcp[06:2]&0x40
    D) tcp[06:2]&0x20
    ANSWER: A

23. Which of the following instances of tcpdump would increase the tcpdump packet snapshot length to 90 and save the raw packet data to a file?
    A) tcpdump –s /tmp/outfile.out –I 90
    B) tcpdump –s 90 –x /tmp/outfile.out
    C) tcpdump –s 90 –F /tmp/outfile.out
    D) tcpdump –s 90 >/tmp/outfile.out
    ANSWER: B

24. Which of the following Shadow sensor filters would capture a packet if the IP protocol is UDP and the destination port was 31337 originating from net 204.14.16?
    A) (udp and (udp[2:2]=31337) and src net 204.14.16)
    B) (udp and (udp[2:0]=31337) and src net 204.14.16)
    C) (udp and (udp[0:2]=31337) and src net 204.14.16)
    D) None of the above
    ANSWER: A

25. Why would you want to incorporate exclusions in Shadow analysis filters to aid in the elimination of noise?
    A) Known traffic of non-malicious nature may be recurrent and voluminous
    B) Source traffic is trivial and originates from a known source
    C) Traffic source is from a mutual subnet and is of reoccurring nature
    D) Traffic is malicious and is not being blocked
    ANSWER: A

26. Which of the following do the Shadow hourly filters not provide?
    A) Extraction of the previous hour's tcpdump filter data records
    B) The retrieval of any anomalous records from anomalous condition
    C) The examination of the various protocols, core infrastructure hosts, and one-to-many relationships
    D) Tally count at bottom web wrap-up html document
    ANSWER: D

27. The Time To Live (TTL) value in the header of a source IP can be used to determine the validity of which of the following?
    A) Three machines having identical TTL values
    B) Multiple machines having decreasing TTL values
    C) Using traceroute and getting conflicting TTL counts
    D) All of above

ANSWER: D

28. In regards to the Shadow analysis filters, which of the following should not be a response of hostile fire traffic?
    A) Investigation and conformation of the activity
    B) Report of the activity to management
    C) Vulnerability assessment of scanned or accessed hosts and or ports
    D) Recording of activity for later reference
    ANSWER: D

29. What is an attacker attempting when they are causing the degradation of a network or host by sending multiple connections in a short time span?
    A) Buffer overflow
    B) Denial of service
    C) Network mapping
    D) Packet sniffing

30. The UDP datagram's error correcting checksum could provide insight on which of the following?
    A) UDP length field has been crafted
    B) Sequence number out of order
    C) Options variables are invalid
    D) None of the above
    ANSWER: D

Day Four and Five Questions
Network-Based Intrusion Detection Analysis and
Intrusion Detection Workshop:

31. Which of the following is a good rule to follow on the initial configuration of a firewall?
    A) Allow all traffic and then deny what is deemed dangerous
    B) Deny all traffic and then add back what is explicitly allowed
    C) Allow UDP traffic and deny dangerous TCP traffic
    D) Deny all TCP, ARP, and UDP traffic and deny what is latter found to be dangerous
    ANSWER: B

32. If a firewall is needed why would the filtering of a router not suffice?
    A) They are not stateful
    B) They stop unwanted traffic
    C) Tend not to detect attacks that pass through them
    D) Will detect and report on attacks which violate their policy
    ANSWER: A

33. Which of the following is not true of intrusion detection system signatures?
    A) Can be traffic or header based
    B) Can be content based
    C) A representation of known attacks
    D) Incorporates site policy
    ANSWER: D

34. What type of analysis would be utilized to catch the following SYN/FIN packet:
    17:58:18.798839 sourceA.com.43001 > destB.com.111: SF
    1332016810:1332016810(0) win 8192 <mss 1460> (DF) (ttl 128, id
    41148)
    A) Traffic or header Analysis
    B) Content analysis
    C) Mapping analysis
    D) Alarm analysis
    ANSWER: A

35. Which of the following SYN packets is considered a legitimate conversation starter?
    A) 12:36:56.331845 sourceA.net.4023 > destB.com.23: S 13347137:13347137(5) win 8192 <mss 1460> (DF)
    B) 12:36:56.331845 sourceA.net.4023 > destB.com.23: S 13347137:13347137(0) win 8192 <mss 1460> (DF)
    C) 12:36:56.331845 sourceA.net.4023 > destB.com.23: S 13347137:13347137(10) win 8192 <mss 1460> (DF)
    D) 12:36:56.331845 sourceA.net.4023 > destB.com.23: S 13347137:13347137(12) win 8192 <mss 1460> (DF)
    ANSWER: B

36. The spoofed machine in a SYN flood attack must exhibit which of the following attributes?
    A) Routable to and live
    B) Routable to and unreachable
    C) Not routable to and live
    D) Not routable and unreachable
    ANSWER: B

37. In hijacking a connection, which of the following steps do not belong?
    A) Silence one party in the TCP connection
    B) Fake the silenced party's IP address

C) Send an echo-request to the second party of the hijacked connection
D) Calculate the expected sequence number of the next packet destined for receiving machine
ANSWER: C

38. Which of the following would constitute an Event of Interest (EOI)?
A) Nightly batch flow ran at midnight that uses remote copy(rcp) to update files
B) Telnet connections to a login server
C) FTP connections on a anonymous ftp server
D) Notice of multiple failed login request of the root ID on mail relay system at a remote site
ANSWER: D

39. A buffer overflow problem in Microsoft Outlook would be lethal to which of the following systems?
A) Macintosh
B) Solaris Sparc5(UNIX)
C) Windows95/98/NT
D) IBM AS400
ANSWER: C

40. Assuming that your headend router (connection to Internet) is filtering, where should the placement of your network based IDS be located?
A) Behind the firewall(s) connected to the headend router
B) Between the firewall(s) and the headend router
C) Between the internet and headend router
D) None of the above
ANSWER: C

41. What is the last line of defense if an attacker was able to penetrate network protection schemes?
A) Firewall
B) Filters on network routers
C) System countermeasures
D) Intrusion Detection System
ANSWER: C

42. Dictionary based intrusion detection systems should incorporate which of the following?
A) List of dangerous ports
B) Strings in content that might signal an attack
C) Bad hosts list
D) All of the above
ANSWER: D

43. What scanning technique is being exhibited on a targeted machine when the attacker attempts to detect it's running services and any other information it may yield?
A) Stealthy scan
B) YA mulitscan
C) Vulnerability scan
D) SNMP scan
ANSWER: C

44. With the I&W style of analysis, why would the following detect constitute evidence of active targeting?

```
00:38:12.843874 sourceMachine.net.4657 > 192.88.10.200.110: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
```

```
00:38:16.116315 sourceMachine.net.4657 > 192.88.10.200.111.net.110: S
3006384960:3006384960(0) win 8192 <mss 1460> (DF)
00:38:22.678569 sourceMachine.net.4657 > 192.88.10.200.112.110: S
```

A) The attacker is tying to initiate a connection to the POP3 server
B) The attacker if probing the network to see which machines are POP3 servers
C) The attacker is sending malformed TCP packets
D) The attacker is initiating a DOS attack on all POP3 server machines
ANSWER: B

45. The success of analysis through sensor usage within intrusion detection systems requires which of the following techniques?
A) Meshing of observations from multiple types of sensors
B) Correlation of various observations from like sensors
C) Construction of the solution a piece at a time
D) All of the above
ANSWER: D

46. The overall benefits of manual correlation can be seen as which of the following?
A) Can be used as a primary key to maintain situational awareness
B) The administration of system log files and an alert system can enhance a site's overall detection effectiveness
C) Correlation of log files from multiple sources enable the correct scope of how widespread and serious an attack may be
D) All of the above
ANSWER: D

47. In regards to traffic analysis, which of the following points is not true about a link?
A) Entities joined by links are nodes
B) Links can be weighted by the number of connections
C) Links exist amongst all machine within a common network
D) A link is created when a connection from a source machine and destination machine is made
ANSWER: C

48. Which of the following is true about services running at ports below 1024?
A) Usually used by Malicious server processes(trojans)
B) Usually Utilized by known system services
C) Are attached to static services and can't be changed
D) Good to use for newly developed application software
ANSWER: B

49. What is an attacker attempting if they are sending ICMP:echo request to the following addresses:
192.188.10.255
192.188.10.0
A) Probing for services on all listening ports
B) Network Mapping
C) Probing for candidates of buffer overflows
D) Looking for available routers
ANSWER: B

50. Why do stealthy attacks evade most intrusion detection systems?
A) They are noisy in nature
B) They are embedded within a larger volume of identical traffic
C) Incorporates high-speed scanning techniques

D) They duration of connections are too long to be caught by intrusion detection systems
ANSWER: B