Global Information Assurance Certification Paper

These 10 traces were submitted by Matthew Grimes for the practical examination following the Intrusion Detection GIAC Training and Certification Track in San Jose, May 2000

Detect #1

172.145.63.191 > 192.168.1.1
06:08:33.404945 AC913FBF.ipt.aol.com.4526 > 192.168.1.2.1243: S 3498837:3498837(0) win 4288 (DF)
06:08:33.433326 AC913FBF.ipt.aol.com.4527 > 192.168.1.3.1243: S 3498839:3498839(0) win 4288 (DF)
06:08:33.445406 AC913FBF.ipt.aol.com.4528 > 192.168.1.4.1243: S 3498846:3498846(0) win 4288 (DF)
06:08:33.445609 AC913FBF.ipt.aol.com.4529 > 192.168.1.5.1243: S 3498848:3498848(0) win 4288 (DF)
06:08:33.456381 AC913FBF.ipt.aol.com.4530 > 192.168.1.6.1243: S 3498851:3498851(0) win 4288 (DF)
06:08:33.469652 AC913FBF.ipt.aol.com.4531 > 192.168.1.7.1243: S 3498858:3498858(0) win 4288 (DF)
06:08:33.483583 AC913FBF.ipt.aol.com.4532 > 192.168.1.8.1243: S 3498860:3498860(0) win 4288 (DF)
06:08:33.488659 AC913FBF.ipt.aol.com.4533 > 192.168.1.9.1243: S 3498868:3498868(0) win 4288 (DF)
<SNIP>
06:13:23.662810 AC913FBF.ipt.aol.com.4275 > 192.168.15.169.1243: S 3788743:3788743(0) win 4288 (DF)
06:13:23.673787 AC913FBF.ipt.aol.com.4276 > 192.168.15.170.1243: S 3788748:3788748(0) win 4288 (DF)
06:13:23.675754 AC913FBF.ipt.aol.com.4277 > 192.168.15.171.1243: S 3788754:3788754(0) win 4288 (DF)
06:13:23.733655 AC913FBF.ipt.aol.com.4278 > 192.168.15.172.1243: S 3788757:3788757(0) win 4288 (DF)

AND

13:34:55.362217 AC83E030.ipt.aol.com.1608 > 192.168.5.1.27374: S 75489040:75489040(0) win 8192 (DF)
13:34:55.372245 AC83E030.ipt.aol.com.1609 > 192.168.5.2.27374: S 75489041:75489041(0) win 8192 (DF)
13:34:55.425561 AC83E030.ipt.aol.com.1610 > 192.168.5.3.27374: S 75489044:75489044(0) win 8192 (DF)
13:34:55.427418 AC83E030.ipt.aol.com.1611 > 192.168.5.4.27374: S 75489045:75489045(0) win 8192 (DF)
13:34:55.442324 AC83E030.ipt.aol.com.1614 > 192.168.5.7.27374: S 75489051:75489051(0) win 8192 (DF)
13:34:55.442653 AC83E030.ipt.aol.com.1613 > 192.168.5.6.27374: S 75489049:75489049(0) win 8192 (DF)
13:34:55.460897 AC83E030.ipt.aol.com.1612 > 192.168.5.5.27374: S 75489047:75489047(0) win 8192 (DF)
13:34:55.477062 AC83E030.ipt.aol.com.1615 > 192.168.5.8.27374: S 75489052:75489052(0) win 8192 (DF)

1. Source of Trace
    a. My network
2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

[source ip] [dest ip] [direction of traffic] [TCP flags] [bytes]
172.145.63.191 > 192.168.1.1 | | |
06:08:33.535229 AC913FBF.ipt.aol.com.4536 > 192.168.1.12.1243: S 3498878:3498878(0) win 4288 (DF)
[timestamp] [source host] | [dest host] | [begin : end] [options]
[port] [port] sequence #

3. Probability the source address was spoofed
    a. Low – Since the ip address is assigned to America OnLine it is likely a dial-up account.

4. Description of Attack
    a. Attacker is scanning a large number of addresses looking for hosts that have been infected with a specific trojan [SubSeven].
    b. This is a reconnaissance attack.
    c. This attack is very noisy; coming very fast and stepping sequentially through the addresses.

5. Attack Mechanism
    a. Attacker is looking for pre-installed trojans that are listening on port 1243 or 27374. By sending a SYN request to the port the attacker can determine whether the trojan has been installed by analyzing

the response. If the target host responds with a SYN-ACK then the target host does have that port open and likely has the trojan installed. Else if the target host responds with a RST nothing is listening on that port.

6. Correlations
   a. This attack is described on the SANS web site http://www.sans.org/y2k/subseven.htm

7. Evidence of Active Targeting
   a. Most likely a general scan against a large block of addresses.

8. Severity
   a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
   b. (1 + 1) – (5 + 2) = -5
   c. We are primarily an NT based operation, SubSeven does not affect NT machines and all machines have current anti-virus definitions.

9. Defensive Recommendations
   a. Defenses could be improved by implementing ACLs on the router and/or blocking ports 1243 and 27374 on the firewall. Maintain up to date virus definitions on virus scanners.

10. Multiple Choice Test Question
    This trace is best described as:
    a) Low and Slow
    b) Port Scan
    c) IMAP Scan
    d) Host Scan

    Answer is d)

Detect 2

```
May 30, 2000
=============================================================================
20:21:15.734908 28.158.36.101.36980 > 192.168.175.80.60427: S 1855299323:1855299323(0) win 1024
21:02:31.830183 129.150.139.91.39642 > 192.168.1.121.3897: S 900778576:900778576(0) win 1024
21:06:48.696048 212.178.83.17.24240 > 192.168.84.59.56775: S 300547308:300547308(0) win 1024
21:09:43.213848 176.237.193.108.15598 > 192.168.67.13.25566: S 1315714181:1315714181(0) win 1024
21:28:20.091305 79.122.231.41.23473 > 192.168.18.12.40497: S 336148752:336148752(0) win 1024
21:31:14.782236 84.84.157.110.22142 > 192.168.112.81.14714: S 199821754:199821754(0) win 1024
21:39:16.098549 152.184.1.43.30380 > 192.168.255.80.22647: S 1851392067:1851392067(0) win 1024
21:43:41.081582 42.244.164.53.13433 > 192.168.197.40.34757: S 1798327192:1798327192(0) win 1024
22:09:55.021328 15.163.118.34.47993 > 192.168.41.80.3509: S 2034613870:2034613870(0) win 1024
22:13:00.353077 60.1.72.50.51930 > 192.168.20.73.41558: S 113988274:113988274(0) win 1024
22:13:38.049367 108.169.43.52.63488 > 192.168.243.87.60683: S 1416845821:1416845821(0) win 1024
22:15:08.134633 207.48.20.124.46109 > 192.168.47.68.50067: S 1587858227:1587858227(0) win 1024
22:25:20.659902 255.160.173.79.35781 > 192.168.235.126.59340: S 1242434928:1242434928(0) win 1024
22:33:04.456862 244.151.64.92.11302 > 192.168.111.27.58430: S 785259966:785259966(0) win 1024
22:42:05.008021 107.49.235.6.29454 > 192.168.214.36.23952: S 499790768:499790768(0) win 1024
22:43:33.143462 50.99.162.84.55266 > 192.168.74.44.48326: S 1875757353:1875757353(0) win1024
22:43:52.423915 40.166.59.62.38820 > 192.168.215.112.15996: S 455712905:455712905(0) win 1024
23:00:51.053111 57.239.224.36.18029 > 192.168.95.72.50754: S 40386787:40386787(0) win 1024
23:13:04.167620 174.151.140.125.56313 > 192.168.106.124.36414: S 1905698965:1905698965(0) win1024
23:25:28.133578 160.156.86.17.64124 > 192.168.181.65.39563: S 241882045:241882045(0) win 1024
23:25:50.369233 199.195.240.41.23338 > 192.168.201.88.63704: S 2006354198:2006354198(0) win 1024
23:33:40.948465 56.190.212.76.16180 > 192.168.182.94.60199: S 1874076025:1874076025(0) win 1024
23:33:52.990533 101.10.74.102.45205 > 192.168.209.116.26613: S 220523692:220523692(0) win 1024
23:40:32.888434 136.65.39.104.12393 > 192.168.93.22.12517: S 353976342:353976342(0) win 1024
23:43:02.062715 109.156.155.102.28547 > 192.168.154.80.52473: S 763909761:763909761(0) win 1024
23:44:19.857064 6.154.5.34.25639 > 192.168.128.44.65246: S 1033065038:1033065038(0) win 1024
```

1. Source of Trace
    a. My network
2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

[source ip] [dest ip] [direction of traffic] [TCP flags] [bytes]
172.145.63.191 > 192.168.1.1 | | |
06:08:33.535229 AC913FBF.ipt.aol.com.4536 > 192.168.1.12.1243: S 3498878:3498878(0) win 4288 (DF)
[timestamp] [source host] | [dest host] | [begin : end] [options]
[port] [port] sequence #

3. Probability the source address was spoofed
    a. Very High – they seem to be completely random. At least one (`42.244.164.53) is` reserved by the Internet Assigned Numbers Authority.

4. Description of Attack
    a. Attacker is coming in low and slow with a high degree of randomness. Only 8 or 9 packets per hour. What brought this to my attention was the fact that only one packet at a time was showing up and the source IP's seemed to have an unusually high number of class A addresses.
    b. This is a reconnaissance attack attempting to map our network.

5. Attack Mechanism
    a. Attacker is looking for a response from the target machine. Any response will validate that a machine exists at that address.

6. Correlations
    a. None

7. Evidence of Active Targeting
    a. The attack is targeting a specific network address space..

8. Severity
    a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    b. (2 + 3) – (2 + 1) = 2

9. Defensive Recommendations
    a. Defenses could be improved by implementing a restrictive firewall that allowed incoming traffic on known ports only.

10. Multiple Choice Test Question
    This trace is best described as:
    a) Low and Slow
    b) Port Scan
    c) IMAP Scan
    d) Host Scan

    Answer is a)

Detect #3

01:59:16.652064 198.161.199.2 > 10.5.71.0: icmp: host 208.246.224.20 unreachable - admin prohibited filter
02:43:44.557379 198.161.199.2 > 10.12.92.0: icmp: host 204.210.42.11 unreachable - admin prohibited filter
09:40:12.562199 198.161.199.2 > 10.5.255.0: icmp: host 204.210.42.11 unreachable - admin prohibited filter
09:46:25.613212 198.161.199.2 > 192.168.158.0: icmp: host 208.246.224.20 unreachable - admin prohibited filter
13:33:42.773649 198.161.199.2 > 10.5.7.0: icmp: host 204.210.42.11 unreachable - admin prohibited filter
14:13:25.011878 198.161.199.2 > 192.168.79.0: icmp: host 208.246.224.20 unreachable - admin prohibited filter
19:28:10.400791 198.161.199.2 > 192.168.239.0: icmp: host 24.5.244.74 unreachable - admin prohibited filter
22:49:57.989057 198.161.199.2 > 10.5.167.0: icmp: host 208.246.224.20 unreachable - admin prohibited filter

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

22:49:57.989057 198.161.199.2 > 10.5.167.0: icmp: host 208.246.224.20 unreachable - admin prohibited filter
[timestamp] [source host] [dest host] | [error message] [protocol]

3. Probability the source address was spoofed
    a. High – The source address would appear to be the intended victim.

4. Description of Attack
    a. Broadcast ICMP - Attacker may be attempting to generate a ping flood denial of service attack against a 3rd party victim by using our networks, or it could be a reconnaissance probe.

5. Attack Mechanism
    a. Attacker seems to be operating from several compromised hosts (208.246.224.20, 24.5.244.74, and 204.210.42.11) and is sending icmp packets (probably echo requests) to broadcast addresses on several of our networks. The intent could be a basic smurf type denial of service by making every host on our networks respond with echo replies directed at the victim thus overwhelming his host. But, given the large time gaps between packets this seems misleading. It could also be a coordinated inverse mapping attempt looking for unreachable hosts messages from the router.

6. Correlation
    a. Network Intrusion Detection an Analyst's Handbook by Stephen Northcutt, pg. 125,

7. Evidence of Active Targeting
    a. The attack is targeting a specific network address space..

8. Severity
    a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    b. (3 + 3) – (2 + 5) = -1

9. Defensive Recommendations
    a. Defenses are adequate. Router is blocking directed broadcast traffic.

10. Multiple Choice Test Question
    This attack will most likely be:
    a) Completely successful
    b) Blocked by a router acl
    c) Partially successful
    d) Blocked by a router service

Answer is d)

Detect #4

212.30.95.119 > 10.5.147.60
00:10:01.051443 user.775f1ed4.cable.link.si.46327 > 10.5.147.60.33116: SR 2090168564:2090168564(0) win 15572 (DF)
00:17:28.305571 user.775f1ed4.cable.link.si.38685 > 192.168.110.59.28391: SR 970408953:970408953(0) win 29625 (DF)
00:24:09.340606 user.775f1ed4.cable.link.si.46326 > 10.5.31.78.37563: SR 295501936:295501936(0) win 37872 (DF)
00:25:44.944138 user.775f1ed4.cable.link.si.39108 > 10.5.47.242.43050: SR 921969448:921969448(0) win 6632 (DF)

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

        see Detect #1

3. Probability the source address was spoofed
    a. Low – The source address would appear to be the attacker on a cable modem or dialup.

4. Description of Attack
    a. Unusual TCP flag combination – Possibly OS fingerprinting

5. Attack Mechanism
    a. Attacker is constructing packets with odd TCP flag combinations. Probably in an attempt to fingerprint the operating systems in conjunctions with a host scan.

6. Correlation
    a. None that I could find. I have not seen this before.

7. Evidence of Active Targeting
    a. The attack is targeting specific hosts..

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

9. Defensive Recommendations
    a. Defenses could be improved by having router drop malformed packets.

10. Multiple Choice Test Question
    This trace best describes:
    a) Host Scan
    b) Port Scan
    c) OS fingerprinting
    d) Stealth scanning

Answer is c)

Detect #5

01:12:00.181374 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:12:00.181678 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:12:00.181852 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:12:00.182128 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:12:00.182225 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:12:00.182496 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
<snip>
01:26:40.997530 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.997868 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.997970 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.998237 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.998339 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.998687 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.998789 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
01:26:40.999056 isea.ru > 10.12.0.0: icmp: time stamp reply [tos 0x60]
<snip>
01:30:22.744856 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.745240 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.745342 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.745607 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.745792 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.746058 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.746160 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]
01:30:22.746428 isea.ru > 10.5.0.0: icmp: time stamp reply [tos 0x60]

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

22:49:57.989057 198.161.199.2 > 10.5.167.0: icmp: time stamp reply [tos 0x60]
[timestamp] [source host] [dest host] | [optional data]
[protocol]

3. Probability the source address was spoofed
    a. Low – The source address would appear to be reasonable for an attacker.

4. Description of Attack
    a. Broadcast ICMP - Attacker is trying to map the network by pushing through icmp packets to a broadcast address hoping that we only have echo requests blocked.

5. Attack Mechanism
    b. The attacker is crafting packets that will appear to the router/firewall as responses to requests originated inside our network. If the router/firewall passes them through then each host on the network would respond with a RST since no host actually requested an icmp time stamp. This would allow the attacker to map out hosts on the network.

6. Correlations
    b. SANS IDS Course, Book 2.1 Chapter 5

7. Evidence of Active Targeting
    b. The attack is targeting a specific network address space..

8. Severity
    c. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    d. (3 + 3) – (2 + 5) = -1

9. Defensive Recommendations
    b. Defenses are adequate. Router is blocking directed broadcast traffic.

10. Multiple Choice Test Question
    This attack is most likely:
    a) Mapping the network
    b) Fingerprinting OS's
    c) Scanning for trojans
    d) Attempting denial of service

Answer is a)

Detect #6

00:00:24.703085 202.104.24.123.2034 > 192.168.1.39.53: 571+ (35)
00:00:30.137594 202.104.24.123.2034 > 192.168.1.39.53: 571+ (35)
00:03:31.651164 61.143.157.74.137 > 192.168.1.39.53: 4040+ Type0 (Class 256)? . (34)
00:03:33.089178 61.143.157.74.137 > 192.168.1.39.53: 4040+ Type0 (Class 256)? . (34)
01:23:51.648594 gnet124.szptt.net.cn.34479 > 192.168.1.39.53: 1+ (34)
01:23:54.217561 gnet124.szptt.net.cn.34514 > 192.168.1.39.53: 2+ (32)
01:23:58.673094 gnet124.szptt.net.cn.34603 > 192.168.1.39.53: 1+ (33)
01:24:00.189425 gnet124.szptt.net.cn.34603 > 192.168.1.39.53: 1+ (33)
01:24:08.301807 gnet124.szptt.net.cn.34715 > 192.168.1.39.53: 2+ (45)
01:24:09.805678 gnet124.szptt.net.cn.34715 > 192.168.1.39.53: 2+ (45)
01:24:13.368013 gnet124.szptt.net.cn.34715 > 192.168.1.39.53: 2+ (45)
04:20:56.481016 202.96.141.245.1470 > 192.168.1.39.53: 2+ (31)
04:20:57.926729 202.96.141.245.1470 > 192.168.1.39.53: 2+ (31)
05:00:19.006293 202.103.171.196.1449 > 192.168.1.39.53: 3+ (32)
05:00:19.035406 202.103.171.196.1451 > 192.168.1.39.53: 4+ (34)

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

01:24:13.368013 gnet124.szptt.net.cn.34715 > 192.168.1.39.53: 2+ (45)
[timestamp] [source host.port] [dest host.port] [optional data]

3. Probability the source address was spoofed
    a. Low – The source address would appear to be reasonable for an attacker.

4. Description of Attack
    a. DNS Exploit

5. Attack Mechanism
    a. The attacker is generating DNS queries to port 53 looking for a response. This particular host does not exist. But there are repetitive DNS query attempts by various Asian source addresses to this particular IP address on a daily basis. I suspect that the trace is not malicious but rather that at one time a DNS server did in fact exist at this address and still shows up somewhere as an authority record.

6. Correlation
    a. none

7. Evidence of Active Targeting
    a. The traffic is directed to a specific host.

8. Severity
    a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    b. (0 + 0) – (0 + 0) = 0

9. Defensive Recommendations
    a. Defenses are adequate. Destination IP is vacant.

10. Multiple Choice Test Question
    This attack is most likely:
    a) Mapping the network
    b) Fingerprinting OS's
    c) Scanning for DNS servers
    d) Attempting denial of service

Answer is c)

Detect #7

202.104.36.76 > 192.168.1.63
01:08:29.539145 202.104.36.76.61524 > 192.168.1.63.111: udp 100
01:08:29.555350 202.104.36.76.61524 > 192.168.1.63.111: udp 100
01:08:33.523181 202.104.36.76.61524 > 192.168.1.63.111: udp 100
01:08:33.543654 202.104.36.76.61524 > 192.168.1.63.111: udp 100
01:08:41.479170 202.104.36.76.61524 > 192.168.1.63.111: udp 100
01:08:41.513887 202.104.36.76.61524 > 192.168.1.63.111: udp 100

202.104.36.77 > 192.168.1.63
01:00:10.118166 202.104.36.77.61269 > 192.168.1.63.111: udp 100
01:00:10.142911 202.104.36.77.61269 > 192.168.1.63.111: udp 100
01:00:56.249891 202.104.36.77.61331 > 192.168.1.63.111: udp 100
01:00:56.259935 202.104.36.77.61331 > 192.168.1.63.111: udp 100
01:01:00.171870 202.104.36.77.61331 > 192.168.1.63.111: udp 100
01:01:00.178389 202.104.36.77.61331 > 192.168.1.63.111: udp 100

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

22:49:57.989057 198.161.199.2 > 10.5.167.0: udp 100
[timestamp] [source host] [dest host] | [optional data]
[protocol]

3. Probability the source address was spoofed
    a. Low – The source address (mainland China) would appear to be reasonable for an attacker.

4. Description of Attack
    a. Portmapper – Attacker(s) is attempting to exploit SUNRPC (portmapper) vulnerabilities on a UNIX machine.

5. Attack Mechanism
    a. The attacker is sending UDP packets to the Remote Procedure Call port. In RPC –enabled environments, users can issue commands on the attackers machine to be executed on the server. Various UNIX applications and systems use RPC, including NFS.

6. Correlations
    a. SANS IDS Course, Book 2.1 Chapter 5
    b. CERT Advisories CA-97-26 and CA-99-05

7. Evidence of Active Targeting
    a. The attack is targeting a specific host.

8. Severity
    a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    b. (4 + 4) – (5 + 3) = 0

9. Defensive Recommendations
    a. Defenses are adequate. RPC services are turned off.

10. Multiple Choice Test Question
    This attack is most likely:
    a) Mapping the network
    b) Fingerprinting OS's
    c) Scanning for trojans
    d) Exploiting UNIX systems

Answer is d)

Detect #8

05:35:03.560109 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)
05:35:03.560430 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)
05:35:03.560549 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)
05:35:03.560921 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)
05:35:03.561041 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

05:35:03.561041 166.102.24.224.1145 > 10.5.0.0.53: 56603+ (48)
[timestamp] [source host.port] [dest host.port] [optional data]

3. Probability the source address was spoofed
    a. Low – The source address (ALLTEL ISP in Little Rock, AR) would appear to be reasonable for an attacker.

4. Description of Attack
    a. Scanning for DNS Servers – Zone Transfer

b. This is a reconnaissance attack.

5. Attack Mechanism
   a. The attacker is generating DNS queries to port 53 looking for a response. Rather than stepping through individual addressess he has elected to target network broadcast addresses hoping to get all machines to respond with only one volley. This is a less noisy approach but not very effective if the router/firewall is blocking traffic to broadcast addresses that originate outside of the network (a smart thing to do).

6. Correlations
   a. SANS Intrusion Detection Workshop 2.5 pg. 288

7. Evidence of Active Targeting
   a. The traffic is directed to a specific network.

8. Severity
   a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
   b. (5 + 4) – (5 + 5) = -1

9. Defensive Recommendations
   a. Defenses are adequate. Router blocks packets to broadcast addresses. DNS server have latest code.

10. Multiple Choice Test Question
    This attack is most likely:
    a) Scan for Zone Transfer
    b) Ping of Death
    c) Buffer Overflow
    d) Denial of service

Answer is a)

Detect #9

```
03:45:24.830015 195.127.94.7.110 > 192.168.0.1.110: SF 1666911282:1666911282(0) win 1028
03:45:24.848027 195.127.94.7.110 > 192.168.0.2.110: SF 1666911282:1666911282(0) win 1028
03:45:24.868882 195.127.94.7.110 > 192.168.0.3.110: SF 1666911282:1666911282(0) win 1028
03:45:24.883464 195.127.94.7.110 > 192.168.0.4.110: SF 1666911282:1666911282(0) win 1028
03:45:24.902757 195.127.94.7.110 > 192.168.0.5.110: SF 1666911282:1666911282(0) win 1028
03:45:24.924416 195.127.94.7.110 > 192.168.0.6.110: SF 1666911282:1666911282(0) win 1028
03:45:24.940761 195.127.94.7.110 > 192.168.0.7.110: SF 1666911282:1666911282(0) win 1028
03:45:24.964402 195.127.94.7.110 > 192.168.0.8.110: SF 1666911282:1666911282(0) win 1028
<snip>
04:07:09.732607 195.127.94.7.110 > 192.168.255.249.110: SF 1904401157:1904401157(0) win 1028
04:07:09.754324 195.127.94.7.110 > 192.168.255.250.110: SF 1904401157:1904401157(0) win 1028
04:07:09.772673 195.127.94.7.110 > 192.168.255.251.110: SF 1904401157:1904401157(0) win 1028
04:07:09.796759 195.127.94.7.110 > 192.168.255.252.110: SF 1904401157:1904401157(0) win 1028
04:07:09.816584 195.127.94.7.110 > 192.168.255.253.110: SF 1904401157:1904401157(0) win 1028
04:07:09.847282 195.127.94.7.110 > 192.168.255.254.110: SF 1904401157:1904401157(0) win 1028
04:07:09.857052 195.127.94.7.110 > 192.168.255.255.110: SF 1904401157:1904401157(0) win 1028
```

1. Source of Trace
   a. My network
2. Detect was generated by:
   a. Shadow IDS (tcpdump)

b. Explanation of fields:

[source ip] [dest ip] [direction of traffic] [TCP flags] [bytes]
172.145.63.191 > 192.168.1.1 | | |
06:08:33.535229 AC913FBF.ipt.aol.com.4536 > 192.168.1.12.1243: S 3498878:3498878(0) win 4288 (DF)
[timestamp] [source host] | [dest host] | [begin : end] [options]
[port] [port] sequence #

3. Probability the source address was spoofed
   a. Low –the ip address is part of a class c block assigned to a German computer consulting firm.

4. Description of Attack
   a. Attacker is scanning a large number of addresses looking for hosts that have the POP3 service running.
   b. This is a reconnaissance attack.
   c. This attack is very noisy; coming very fast and stepping sequentially through the addresses.

5. Attack Mechanism
   a. Attacker is looking for email servers running the POP3 protocol. Earlier versions of POP3 had known vulnerabilities. By sending a SYN request to the port the attacker can determine whether the service is running by analyzing the response. The attacker also has the FIN flag set. This can help get past logging systems and evade filtering devices. .

6. Correlations
   a. Stephen Northcutt describes this attack in Network Intrusion Detection, an Analyst's Handbook on pg. 104.

7. Evidence of Active Targeting
   a. Most likely a general scan against a large block of addresses.

8. Severity
   a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
   b. (4 + 4) – (5 + 2) = 1
   c. POP3 servers are up to date.

9. Defensive Recommendations
   a. Defenses are adequate. Update POP3 programs as they become available.

10. Multiple Choice Test Question
    This trace is best described as:
    a) Low and Slow
    b) POP3 Scan
    c) IMAP Scan
    d) Host Scan

    Answer is b)

Detect #10

202.182.85.31 > 10.12.224.0
04:02:32.346967 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]
04:02:32.347310 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]
04:02:32.347393 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]
04:02:32.347638 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]
04:02:32.347721 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]
04:02:32.348007 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]

04:02:32.348089 just.got.stormed.org.46853 > 10.12.224.0.10199: R 0:0(0) ack 187494437 win 0 [tos 0x8]

1. Source of Trace
    a. My network

2. Detect was generated by:
    a. Shadow IDS (tcpdump)
    b. Explanation of fields:

    See Detect #1

3. Probability the source address was spoofed
    a. Low – The source address would appear to be reasonable for an attacker. ; -)

4. Description of Attack
    b. RESET Scan - Attacker is trying to map the network by pushing through packets to a broadcast address.

5. Attack Mechanism
    c. The attacker is crafting packets that will appear to the router/firewall as responses to requests originated inside our network. The idea is to fool the router . If the router/firewall passes them through then each host on the network would respond with a RST since no host actually initiated the original SYN packet. This would allow the attacker to map out hosts on the network.

6. Correlations
    a. Stephen Northcutt describes this attack in Network Intrusion Detection, an Analyst's Handbook on pg. 138.

7. Evidence of Active Targeting
    a. The attack is targeting a specific network address space..

8. Severity
    a. (Criticality + Lethality) – (System + Net Countermeasures) = Severity
    b. (2 + 1) – (1 + 5) = -3

9. Defensive Recommendations
    a. Defenses are adequate. Router is blocking traffic to broadcast addresses from sources outside the network.

10. Multiple Choice Test Question
    This attack is most likely:
    a) Mapping the network
    b) Fingerprinting OS's
    c) Scanning for trojans
    d) Attempting denial of service

Answer is a)

Last Updated: October 23rd, 2017

Upcoming Training

SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 07, 2018	vLive
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced