Global Information Assurance Certification Paper

SANS GIAC Intrusion Detection Practical

Chip Kelly
June 8, 2000

Detect #1

May 12 06:52:33 cc1014244-a kernel: securityalert: udp if=ef0 from 24.64.228.161:137 to 24.3.21.199 on unserved port 137
May 12 09:02:48 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.28.212:137 to 24.3.21.199 on unserved port 137
May 12 16:03:25 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.3.112.18:3589 to 24.3.21.199 on unserved port 1243
May 12 19:11:52 cc1014244-a kernel: securityalert: udp if=ef0 from 24.20.34.151:137 to 24.3.21.199 on unserved port 137
May 12 20:34:18 cc1014244-a kernel: securityalert: udp if=ef0 from 169.254.3.125:137 to 24.3.21.199 on unserved port 137

1. Source of Trace
   May 17, 2000 GIAC web collection - http://www.sans.org/y2k/051700.htm
2. Detect was generated by:
   Don't know, same as listed on page 30, Day 4 of SANS Network Intrusion Detection Course notes.
   Explanation of key fields:
   May 12 06:52:33 [TIMESTAMP] cc1014244-a kernel: securityalert: udp if=ef0 from 24.64.228.161:137 [SOURCE ADDRESS and PORT] to 24.3.21.199 [DESTINATION ADDRESS] on unserved [PORT IS BLOCKED] port 137 [DESTINATION PORT]
3. Probability the source address was spoofed.
   Low - multiple source addresses all directed at a single destination, useful information needs to be returned to attacker so spoofing not usually an option for this type of attack.
4. Description of Attack
   Attacker is scanning for NetBios information.
   This activity could be used to gather reconnaissance data for future orchestrated attacks.
   It does not follow the "textbook" information gathering attack, since all attempts are focused on a single IP address.
5. Attack Mechanism
   Attacker tries to find a friendly IP address that can elicit a response to a UDP packet sent to a target machine.
6. Correlations:
   James J. Lippard reports a similar detect at http://www.sans.org/y2k/053100.htm. Daniel B. Holzman documented numerous netbios scans at http://www.sans.org/y2k/052600-1130.htm. Additional information about this type of scan is located at http://www.sans.org/y2k/051300.htm. This type of attack is also covered in the text for Day 4 of the Network Based Intrusion Detection Analysis course books, pages 292-295.
7. Evidence of active targeting
   Singular focal point for attack indicates active targeting.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (3+2) – (4+5) = -4
9. Defensive recommendations
   Monitor for unsolicited packets targeting port 137, sooner or later we will develop a signature to better identify the attack.
10. Multiple choice question:
    NetBios can be polled to return information on:
    a) userids
    b) MAC address
    c) Workgroups
    d) All of the above
    Answer is d)

Detect #2

May 11 15:30:58 194.159.255.250:53 -> z.y.w.66:53 UDP

```
May 11 15:30:58 194.159.255.250:30969 -> z.y.w.66:32824 UDP
May 11 15:30:58 194.159.255.250:30972 -> z.y.w.66:16440 UDP
May 11 15:30:58 194.159.255.250:30971 -> z.y.w.66:49208 UDP
```

1. Source of Trace
   May 19, 2000 GIAC web collection - http://www.sans.org/y2k/051900.htm
2. Detect was generated by:
   Don't know. Could be TCPDUMP
   Explanation of key fields:
   May 11 15:30:58 [TIMESTAMP] 194.159.255.250:53 [SOURCE ADDRESS and PORT] -> z.y.w.66:53 [DESTINATION ADDRESS and PORT] UDP [PROTOCOL]
3. Probability the source address was spoofed.
   Low – information from the scan is processed by the attacker, so packets need to return to the attacker.
4. Description of Attack
   UDP port scan
5. Attack Mechanism
   Attacker locates a receptive IP address using a well known port, in this case port 53 to establish communications. Once IP has responded, attacker probes seemingly random ports, mapping the available ones for future use.
6. Correlations:
   Johnston Andy reported a very similar scan at http://www.sans.org/y2k/052800-1100.htm. This is very similar to the NMAP signature, except UDP is the target protocol.
7. Evidence of active targeting
   A single IP address is targeted from a single source IP, source port usage is sequential, target ports are randomized.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (4+3)-(4+5)=-2
9. Defensive recommendations
   Close as many ports as you can get away with at the firewall. Only allow ports of known utility to remain open. This may not be a realistic measure at some shops.
10. Multiple choice question:
    Sequences of which ports indicates port scanning activity?
    a) Source
    b) Destination
    c) Both
    d) Neither

    Correct answer a)

Detect #3

```
21:12:27.732981 ip.domain.com.1198 > rdu162-225-066.nc.rr.com.107: S 1543759455:1543759455(0) win 32768 <mss 1460> (DF)
21:12:27.733033 rdu162-225-066.nc.rr.com.107 > ip.domain.com.1198: R 0:0(0) ack 1543759456 win 0
21:12:27.759476 ip.domain.com.1199 > rdu162-225-066.nc.rr.com.485: S 2785107116:2785107116(0) win 32768 <mss 1460> (DF)
21:12:27.759568 rdu162-225-066.nc.rr.com.485 > ip.domain.com.1199: R 0:0(0) ack 2785107117 win 0
21:12:27.760302 ip.domain.com.1200 > rdu162-225-066.nc.rr.com.899: S 2623162229:2623162229(0) win 32768 <mss 1460> (DF)
21:12:27.760355 rdu162-225-066.nc.rr.com.899 > ip.domain.com.1200: R 0:0(0) ack 2623162230 win 0
21:12:27.761197 ip.domain.com.1201 > rdu162-225-066.nc.rr.com.403: S 2409628938:2409628938(0) win 32768 <mss 1460> (DF)
21:12:27.761249 rdu162-225-066.nc.rr.com.403 > ip.domain.com.1201: R 0:0(0) ack 2409628939 win 0
21:12:27.761980 ip.domain.com.1202 > rdu162-225-066.nc.rr.com.131: S 834513787:834513787(0) win 32768 <mss 1460> (DF)
21:12:27.762037 rdu162-225-066.nc.rr.com.131 > ip.domain.com.1202: R 0:0(0) ack 834513788 win 0
21:12:27.869454 ip.domain.com.1208 > rdu162-225-066.nc.rr.com.909: S 787906914:787906914(0) win 32768 <mss 1460> (DF)
21:12:27.869556 rdu162-225-066.nc.rr.com.909 > ip.domain.com.1208: R 0:0(0) ack 787906915 win 0
21:12:27.870289 ip.domain.com.1209 > rdu162-225-066.nc.rr.com.895: S 1265444083:1265444083(0) win 32768 <mss 1460> (DF)
21:12:27.870342 rdu162-225-066.nc.rr.com.895 > ip.domain.com.1209: R 0:0(0) ack 1265444084 win 0
21:12:27.870523 ip.domain.com.1211 > rdu162-225-066.nc.rr.com.1475: S 1583235113:1583235113(0) win 32768 <mss 1460> (DF)
21:12:27.870576 rdu162-225-066.nc.rr.com.1475 > ip.domain.com.1211: R 0:0(0) ack 1583235114 win 0
```

```
21:12:27.870764 ip.domain.com.1212 > rdu162-225-066.nc.rr.com.509: S 836999598:836999598(0) win 32768 <mss 1460> (DF)
21:12:27.870816 rdu162-225-066.nc.rr.com.509 > ip.domain.com.1212: R 0:0(0) ack 836999599 win 0
21:12:27.871001 ip.domain.com.1214 > rdu162-225-066.nc.rr.com.1486: S 1529212636:1529212636(0) win 32768 <mss 1460> (DF)
21:12:27.871052 rdu162-225-066.nc.rr.com.1486 > ip.domain.com.1214: R 0:0(0) ack 1529212637 win 0
21:12:27.871240 ip.domain.com.1215 > rdu162-225-066.nc.rr.com.7: S 1104485861:1104485861(0) win 32768 <mss 1460> (DF)
21:12:27.871321 rdu162-225-066.nc.rr.com.7 > ip.domain.com.1215: S 2757881:2757881(0) ack 1104485862 win 9520 <mss 1360> (DF)
```

1. Source of Trace
   May 31, 2000 windump detect from VPN tunnel into our network.
2. Detect was generated by:
   WinDump
   Explanation of key fields:
   21:12:27.732981 [TIMESTAMP] ip.domain.com.1198 [SOURCE IP AND PORT] > rdu162-225-066.nc.rr.com.107: [DESTINATION IP AND PORT]
   S [TCP FLAG SET] 1543759455:1543759455(0) [ID] win 32768 [WINDOW SIZE] <mss 1460> [MAXIMUM SEGMENT SIZE] (DF) [DO NOT FRAG]
3. Probability the source address was spoofed.
   Low – information from the scan is processed by the attacker, so packets need to return to the attacker.
4. Description of Attack
   Attacker locates receptive IP address and sends SYN packets to a range of ports, or all ports at the address.
5. Attack Mechanism
   Closed ports will return a RESET packet, open ports will return a SYN-ACK packet.
6. Correlations:
   Arrigo reports an nmap probe at http://www.sans.org/y2k/052300-0800.htm, except his is very orderly and sequential. This detect is actually a probe used by our network admin to detect open ports on nodes that are connected to our network via VPN tunnel. The last packet exchange shows that port 7 is open – bad.
7. Evidence of active targeting
   Increasing sequential ordering of the source ports indicate active targeting.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (4+3)-(5+0)=+2
9. Defensive recommendations
   Make sure remote VPN nodes are behind a local firewall as a pre-requisite for connecting to your network.
10. Multiple choice question:
    An open port responds to a SYN packet with
    a) RESET
    b) SYN-FIN
    c) SYN-ACK
    d) ACK

    Correct answer is c)

Detect #4

```
May 12 04:43:18 64.27.91.190:1135 -> a.b.e.13:53 UDP
May 12 04:43:19 64.27.91.190:3352 -> a.b.e.63:53 UDP
May 12 04:43:19 64.27.91.190:4234 -> a.b.e.79:53 UDP
May 12 04:43:19 64.27.91.190:4998 -> a.b.e.91:53 UDP
May 12 04:43:19 64.27.91.190:1227 -> a.b.e.101:53 UDP
May 12 04:43:19 64.27.91.190:1360 -> a.b.e.99:53 UDP
May 12 04:43:19 64.27.91.190:4090 -> a.b.e.128:53 UDP
May 12 04:43:20 64.27.91.190:3143 -> a.b.e.171:53 UDP
May 12 04:43:20 64.27.91.190:4029 -> a.b.e.182:53 UDP
May 12 04:43:20 64.27.91.190:4531 -> a.b.e.195:53 UDP
May 12 04:43:20 64.27.91.190:1202 -> a.b.e.201:53 UDP
May 12 04:43:20 64.27.91.190:1269 -> a.b.e.200:53 UDP
May 12 04:43:20 64.27.91.190:1586 -> a.b.e.208:53 UDP
May 12 04:43:20 64.27.91.190:2236 -> a.b.e.216:53 UDP
May 12 04:43:20 64.27.91.190:2282 -> a.b.e.217:53 UDP
```

1. Source of Trace
   May 19, 2000 GIAC web collection - http://www.sans.org/y2k/051900.htm
2. Detect was generated by:
   Unknown, could be TCPDUMP
   Explanation of key fields:
   May 12 04:43:18 [TIMESTAMP] 64.27.91.190:1135 [SOURCE IP AND PORT] -> a.b.e.13:53 [DESTINATION IP AND PORT] UDP [PROTOCOL]
3. Probability the source address was spoofed.
   Low – information from the scan is processed by the attacker, so packets need to return to the attacker.
4. Description of Attack
   Port scan, using UDP DNS port 53
5. Attack Mechanism
   Attacker locates receptive IP address and sends DNS requests to a range of hosts, in an attempt to find a vulnerable host.
6. Correlations:
   Laurie at .edu and Sean Brown both reported UDP port 53 scans at http://www.sans.org/y2k/051200.htm. Similar to other port scanning exploits except this one is only interested in one port on multiple hosts. Also similar to a network scan, except for the use of a single port on each host.
7. Evidence of active targeting
   Ascending sequential ordering of destination IP addresses indicates active targeting of this network.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+3)-(4+4)=0
9. Defensive recommendations
   DNS is a critical network function, make sure it's principal hosts are protected behind firewalls.
10. Multiple choice question:
    Zone transfers use
    a) port 53 UDP
    b) port 119 UDP
    c) port 53 TCP
    d) port 119 TCP

    correct answer is c)

Detect #5

```
03:58:15.235672 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:15.239141 phwww.netcast.nl.2356 > 204.x.x.0.echo: udp 1024
03:58:15.368527 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:15.371826 phwww.netcast.nl.41056 > 204.17.222.255.echo: udp 1024
03:58:17.902494 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:17.906341 phwww.netcast.nl.3471 > 204.x.x.0.echo: udp 1024
03:58:18.035617 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:18.039447 phwww.netcast.nl.2933 > 204.17.222.255.echo: udp 1024
03:58:19.870268 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:19.874172 phwww.netcast.nl.42557 > 204.x.x.0.echo: udp 1024
03:58:20.003372 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:20.007210 phwww.netcast.nl.21668 > 204.17.222.255.echo: udp 1024
03:58:21.896327 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:22.028786 phwww.netcast.nl.11873 > 204.x.x.0.echo: udp 1024
03:58:22.030896 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:22.162075 phwww.netcast.nl.54301 > 204.17.222.255.echo: udp 1024
03:58:23.432190 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:23.435480 phwww.netcast.nl.23701 > 204.x.x.0.echo: udp 1024
03:58:23.608424 phwww.netcast.nl > 204.17.222.255: icmp: echo request
03:58:23.611678 phwww.netcast.nl.11568 > 204.17.222.255.echo: udp 1024
03:58:24.833797 phwww.netcast.nl > 204.x.x.0: icmp: echo request
03:58:24.837642 phwww.netcast.nl.7792 > 204.x.x.0.echo: udp 1024
03:58:24.966905 phwww.netcast.nl > 204.x.x.255: icmp: echo request
03:58:24.970744 phwww.netcast.nl.9306 > 204.x.x.255.echo: udp 1024
```

1. Source of Trace
   May 20, 2000 GIAC web collection - http://www.sans.org/y2k/052000.htm
2. Detect was generated by:
   TCPDUMP
   Explanation of key fields:
   03:58:18.035617 [TIMESTAMP] phwww.netcast.nl [SOURCE IP] > 204.17.222.255 [TARGET IP]: icmp [PROTOCOL] : echo request[MESSAGE TYPE]
3. Probability the source address was spoofed.
   High - single source address, but sequence numbers would help make a better judgement. Attacker does not process information from this attack, so spoofing to conceal identity seems appropriate.
4. Description of Attack
   Denial of service using ICMP echo/echo request to broadcast addresses.
5. Attack Mechanism
   Attacker locates receptive subnet and pings to the broadcast addresses 255 and 0, in an attempt to flood the network with traffic, effectively denying service for the network.
6. Correlations:
   Bryce Alexander, while taking the SANS course in San Jose with me, reported a similar ping detect at http://www.sans.org/y2k/051200.htm. Similar to a SYN flood, this could be called a PING flood. The stealthy ping map is documented on page 301 of Day 4, SANS Network Intrusion Detection Analysis course.
7. Evidence of active targeting
   Ascending sequential ordering of destination IP addresses indicates active targeting of this network.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+4)-(5+3)=+1
9. Defensive recommendations
   Tough one to defend against. Filter out the broadcast addresses making them unresponsive to this type of attack.
10. Multiple choice question:
    Echo Request is ICMP message type
    a) 0
    b) 8
    c) 9
    d) 10

    correct answer is b)

Detect #6

```
May 15 10:22:06.696556 63.70.24.149,111 -> 10.0.0.3,111 PR tcp len 20 40 -SF
May 15 10:22:06.698949 63.70.24.149,111 -> 10.0.0.4,111 PR tcp len 20 40 -SF
May 15 10:22:06.713726 63.70.24.149,111 -> 10.0.0.5,111 PR tcp len 20 40 -SF
May 15 10:22:06.809107 63.70.24.149,111 -> 10.0.0.8,111 PR tcp len 20 40 -SF
May 15 10:22:06.810740 63.70.24.149,111 -> 10.0.0.6,111 PR tcp len 20 40 -SF
May 15 10:22:06.811461 63.70.24.149,111 -> 10.0.0.9,111 PR tcp len 20 40 -SF
May 15 10:22:06.813503 63.70.24.149,111 -> 10.0.0.7,111 PR tcp len 20 40 -SF
May 15 10:22:06.928030 63.70.24.149,111 -> 10.0.0.13,111 PR tcp len 20 40 -SF
May 15 10:22:06.932926 63.70.24.149,111 -> 10.0.0.14,111 PR tcp len 20 40 -SF
May 15 10:22:11.768263 63.70.24.149,111 -> 10.0.0.254,111 PR tcp len 20 40 -SF
```

1. Source of Trace
   May 20, 2000 GIAC web collection - http://www.sans.org/y2k/052000.htm
2. Detect was generated by:
   ?
   Explanation of key fields:
   May 15 10:22:06.696556 [TIMESTAMP] 63.70.24.149,111 [SOURCE IP AND PORT] -> 10.0.0.3,111 [TARGET IP AND PORT] PR tcp [PROTOCOL]
   len 20 [LENGTH OF IP DATAGRAM] 40 [TOTAL LENGTH OF PACKET?] –SF [FLAGS SET]

3. Probability the source address was spoofed.
   Low – single IP/PORT used to scan multiple hosts, but information must be returned to the attacker in order to be useful.
4. Description of Attack
   Port 111 TCP mapping attack using SYN/FIN crafted packets.
5. Attack Mechanism
   Attacker locates a receptive network and emits crafted packets, attempting to map network.
6. Correlations:
   Similar detect reported by Tod Kohl on 10JUN2000, see http://www.sans.org/y2k/061000.htm. Dominic J. Eidson reported several on 06JUN2000, see Dominic J. Eidson. See page 269 of Day 4, SANS Network-based Intrusion Detection Analysis course for description and history of RPC port mapping exploits. Page 114 of Day 2, SANS Intrusion Detection and Packet Filtering: How It Really Works documents scanning with SF packets.
7. Evidence of active targeting
   Sequential ordering of target IP addresses indicate active targeting.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+4)-(5+3)=+1
9. Defensive recommendations
   Block port 111 from incoming, unsolicited packets.
10. Multiple choice question:
    What part of a TCP conversation elicits a SYN/FIN packet?
    a) Initial handshake
    b) First conversation termination packet
    c) Acknowledgement
    d) None of the above
    Correct answer is d)

Detect #7

May 15 22:35:11 Deny inbound tcp src 207.233.243.234/1677 dst x.x.x.113/23
May 15 22:35:11 Deny inbound tcp src 207.233.243.234/1688 dst x.x.x.124/23
May 15 22:35:12 Deny inbound tcp src 207.233.243.234/1689 dst x.x.x.125/23
May 15 22:35:12 Deny inbound tcp src 207.233.243.234/1690 dst x.x.x.126/23

1. Source of Trace
   May 21, 2000 GIAC web collection - http://www.sans.org/y2k/052100.htm
2. Detect was generated by:
   ?
   Explanation of key fields:
   May 15 22:35:11 [TIMESTAMP] Deny inbound tcp [RULE FOLLOWED] src 207.233.243.234/1677 [SOURCE IP/PORT] dst x.x.x.113/23 [DESTINATION IP/PORT]
3. Probability the source address was spoofed.
   Low. A single IP address, using sequentially ordered ports, but information from the scan is processed by the attacker, so packets need to return to the attacker.
4. Description of Attack
   A network scan to find telnet port vulnerabilities.
5. Attack Mechanism
   Attacker locates receptive network, then issues telnet initiation packets to multiple hosts, attempting to locate vulnerable addresses for exploit.
6. Correlations:
   Sean Brown reports a telenet port probe on 12MAY2000, http://www.sans.org/y2k/051200.htm. Sean's was paired with a SOCKS/Wingate scan of port 1080. This is similar to other network scans, this one is probing for vulnerable telnet ports.
7. Evidence of active targeting

Ascending sequential source ports, ascending sequential destination IP addresses, fixation on port 23, all indicate active targeting.

8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (4+5)-(5+4)=0
9. Defensive recommendations
   Block inbound, unsolicited telnet packets.
10. Multiple choice question:
    An indication of a network scan is a collection of:
    a) Random source IP addresses targeting random target IP addresses.
    b) Sequential source IP addresses targeting random target IP addresses.
    c) Single IP address targeting sequential target IP addresses.
    d) Single IP address targeting single target IP address.
    Correct answer is c)

Detect #8

```
May 17 21:17:53 ardvark kernel: Packet log: input DENY eth0 PROTO=6 212.54.71.59:2092 xxx.xxx.xxx.11:21 L=48 S=0x00 I=8654 F=0x4000 T=112 SYN
May 17 21:17:56 ardvark kernel: Packet log: input DENY eth0 PROTO=6 212.54.71.59:2092 xxx.xxx.xxx.11:21 L=48 S=0x00 I=13518 F=0x4000 T=112 SYN
May 17 21:18:02 ardvark kernel: Packet log: input DENY eth0 PROTO=6 212.54.71.59:2092 xxx.xxx.xxx.11:21 L=48 S=0x00 I=22222 F=0x4000 T=112 SYN
```

1. Source of Trace
   May 27, 2000 GIAC web collection - http://www.sans.org/y2k/052700.htm
2. Detect was generated by:
   ? (Aardvark)
   Explanation of key fields:
   May 17 21:17:53 [TIMESTAMP] Packet log: input DENY eth0 PROTO=6 [PROTOCOL ID] 212.54.71.59:2092 [SOURCE IP:PORT] xxx.xxx.xxx.11:21 [TARGET IP:PORT] L=48 [PACKET LENGTH] S=0x00 [] I=8654 [SEQUENCE ID] F=0x4000 [] T=112 [TIME TO LIVE] SYN [TCP FLAG SET]
3. Probability the source address was spoofed.
   Hard to tell from the log. Sequence numbers could be crafted, but the return on this investment is the information from the recon, which needs to be sent back to the attacker for analysis. I don't think this detect has spoofed source IP addresses.
4. Description of Attack
   Attacker searches for a vulnerable FTP port, either for immediate exploitation or as reconnaissance for a future exploit. This is a curious detect, though, in that both the source IP:PORT and target IP:PORT are static throughout the attack. The attacker just wouldn't take "no" for an answer. I suppose the masked octets in the target IP addresses could represent different hosts on the same network, all with the same 11 as their last octet.
5. Attack Mechanism
   FTP and TELNET are two of the richest finds for an attacker if they are found to be vulnerable. In this case, an immediate exploit could be to establish a connection and transfer either a malicious payload to the target, or retrieve confidential information from the target. This detect only shows the opportunity to perform those types of exploits, it does not indicate that that is the intent or capability of the attacker.
6. Correlations:
   Laurie from .edu reports an FTP probe originating at CyberCity Denmark Internet, Denmark. See http://www.sans.org/y2k/052300-0800.htm. Similar to other network scans, this one is probing for vulnerable FTP ports.
7. Evidence of active targeting
   Persistence of port 21, unchanging source IP:PORT.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+5)-(5+3)=+2
9. Defensive recommendations
   Protect the FTP port by placing it behind a firewall, and only allowing solicited incomin FTP packets.

10. Multiple choice question:
    The normal response to a SYN packet in a three-way handshake is:
    a) SYN/FIN
    b) SYN/ACK
    c) RESET
    d) SYN/PUSH
    Correct answer is b)

Detect #9

00:02:10.038459 ip 61: pool0004.cvx35-bradley.di alup.earthlink.net.2806 > my.box.31337: udp 19 (ttl 47, id 24930)
00:02:10.097812 ip 84: my.box.31337 > pool00 04.cvx35-bradley.dialup.earthlink.net.2806: udp 42 (ttl 128, id 19)

1. Source of Trace
   May 30, 2000 GIAC web collection - http://www.sans.org/y2k/053000-1000.htm
2. Detect was generated by:
   ?
   Explanation of key fields:
   00:02:10.038459 [TIMESTAMP] ip [PACKET TYPE?] 61 [PACKET LENGTH?] : pool0004.cvx35-bradley.di alup.earthlink.net.2806 [SOURCE IP.PORT] > my.box.31337: [TARGET IP.PORT] udp [PROTOCOL] 19 [?] (ttl 47,[TIME TO LIVE] id 24930[SEQUENCE ID])
3. Probability the source address was spoofed.
   Low – information from this event needs to be returned to the attacker for evaluation.
4. Description of Attack
   Back Orifice scan for infected hosts
5. Attack Mechanism
   Back Orifice is a client/server application that allows the server side to take control of the machine the client is installed on. A client may be transparently installed on a vulnerable host, then contacted, much like this detect illustrates, for subsequent interactions with the server.
6. Correlations:
   Binette @home reports a poke to port 31337 on 06MAY2000, see http://www.sans.org/y2k/050600.htm for an interesting detect. Also Erik Fichtner reports on some 31337 activity on 08MAY2000, see http://www.sans.org/y2k/050800.htm. See http://www.bo2k.com/ for more information about Back Orifice. This website promotes the use of BO for network monitoring, but the powerful nature of the tool makes it a natural choice for black hats with malicious intentions.
7. Evidence of active targeting
   Port 31337 is suspicious any time you see it in a log file.
8. Severity
   (Critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+5)-(5+3)=+2
9. Defensive recommendations
   Definitely block port 31337, although that is not the only port that Back Orifice can use.
10. Multiple choice question:
    31337 translates to which of the following in cracker-speak:
    a) Tribal
    b) Trinoo
    c) Eleet
    d) Foghat
    Correct answer is c)

Detect #10

May 31, 2000
21:21:50.239911 pool0659.cvx4-bradley.dialup.earthlink.net.2527 > rdu25-22-120.nc.rr.com.27374: S 4456259:4456259(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
21:21:50.240024 rdu25-22-120.nc.rr.com.27374 > pool0659.cvx4-bradley.dialup.earthlink.net.2527: R 0:0(0) ack 4456260 win 0

1. Source of Trace
   May 27, 2000 GIAC web collection - http://www.sans.org/y2k/052700.htm
2. Detect was generated by:
   Explanation of key fields:
   May 24 21:45:11 dns1 portsentry[278053]: attackalert: Connect from host: 208.201.208.71/208.201.208.71 to TCP port: 143
3. Probability the source address was spoofed.
   Low – any useful information must be fed back to the attacker, so spoofing the source IP would defeat the purpose of the attack.
4. Description of Attack
   Trolling for Trojans, probably SubSeven.
5. Attack Mechanism
   Trojan horse attacks work in two steps, the first to infect a vulnerable host with the Trojan horse, the second to locate and activate the Trojan horse(s) as part of a singular or orchestrated multiple host attack. This detect looks like the second step, attempting to locate an installed Trojan horse.
6. Correlations:
   Binette @home reports similar trolling on 09MAY2000 and 12MAY2000, see http://www.sans.org/y2k/050900.htm and http://www.sans.org/y2k/051200.htm for detect listings. See http://www.sans.org/y2k/ports.htm for a list of ports known for exploitation – 27374 is listed as a SubSeven 2.1 port.
7. Evidence of active targeting
   The use of port 27374 is a giveaway.
8. Severity
   (critical + Lethal) – (System + Net Countermeasures) = Severity
   (5+4)-(5+3)=+1
9. Defensive recommendations
   This was the only detect I had from many days of scanning Windump files. I was going to discard it until I saw the previous detect on the GIAC website and recognized the IP address of the perp. Two days before I detected a probe for SubSeven, someone from the same Earthlink account was caught checking for Back Orifice. My recommendation for protecting against these types of probes is to block to known ports in the firewall, and remain vigilant in case other ports are used for similar malicious actions.
10. Multiple choice question:
    A Trojan Horse attack requires which two steps for completion:
    a) Infection with a payload and activation of the payload
    b) Scanning for vulnerable hosts and infecting them
    c) Infecting a host and scanning for results
    d) Creating the payload and activating the payload.
    Correct answer is a)