Practical Exam

Mark Freeman

Detect 1

```
Jun 4 16:41:47 fwall 11 deny: icmp from 38.27.213.54
  to xxx.xxx.xxx.255 type Echo Request
Jun 4 16:41:47 fwall 12 deny: icmp from 38.27.213.54
  to xxx.xxx.xxx.0 type Echo Request
Jun 4 16:41:48 fwall 11 deny: icmp from 38.27.213.54
  to xxx.xxx.xxx.255 type Echo Request
Jun 4 16:41:48 fwall 12 deny: icmp from 38.27.213.54
  to xxx.xxx.xxx.0 type Echo Request
```

1. Source of trace

http://www.sans.org/y2k/060600.htm

2. Detect was generated by:

Detect is generated by Firewall log files.

3. Probability the source address was spoofed

The IP was probably spoofed

4. Description of attack:

This has the characteristics of two attack signatures. This is either a DoS attack against a spoofed IP or a network mapping effort using ICMP broadcast echo requests.

5. Attack mechanism:

If the source IP, is in fact spoofed, this is a DoS attack against the spoofed IP. The DoS is accomplished by sending broadcast echo requests using the spoofed IP as the source/requesting IP. Responses to the broadcast request will flood the source/spoofed IP. This attack was executed using two types of broadcasts, i.e., x.0 and x.255. The same type of echo broadcast requests can also be used to execute a network mapping attack, wherein, hosts responding to the requests will be identified.

6. Correlations:

This detect is attributed to Drew Brunson. It is an often used technique that has been reported on several occasions.

7. Evidence of active targeting:

Both scenarios indicate active targeting. In, the one instance if the source IP is spoofed and being victimized by the DoS attack. In the other, the entire network is being mapped.

8. Severity:

3 +3 – (3 + 4) = 1

9. Defensive recommendation:

Defenses are adequate ICMP was denied by the Firewall.

10. x.x.x.0 is what style of broadcasting:

a) Roman new style
b) Old style ATT
c) Old style BSD
d) New style Unix

Answer: c

Detect 2

```
Jun 3 22:45:28 dns1 snort[248951]: spp_portscan:
  PORTSCAN DETECTED from 207.174.228.81
Jun 3 22:45:28 dns1 snort[248951]: SCAN-SYN FIN:
  207.174.228.81:111 -> z.y.w.34:111
Jun 3 22:45:34 dns1 snort[248951]: spp_portscan: portscan status
  from 207.174.228.81: 2 connections across 1 hosts:
  TCP(1), UDP(1) STEALTH
Jun 3 22:45:40 dns1 snort[248951]: spp_portscan:
  End of portscan from 207.174.228.81
--------
[**] SCAN-SYN FIN [**]
06/03-22:45:28.174384 207.174.228.81:111 -> z.y.w.34:111 TCP
  TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0x5EE0C4BE Ack:
  0x2A65F72E Win: 0x404 00 00 00 00 00 00 ......
Jun 3 22:45:28 dns2 snort[8668]: spp_portscan:
  PORTSCAN DETECTED from 207.174.228.81
Jun 3 22:45:28 dns2 snort[8668]: SCAN-SYN FIN:
  207.174.228.81:111 -> z.y.w.66:111
Jun 3 22:45:29 dns2 snort[8668]: RPC Info Query:
  207.174.228.81:880 -> z.y.w.66:111
Jun 3 22:45:34 dns2 snort[8668]: spp_portscan: portscan status
  rom 207.174.228.81: 3 connections across 1 hosts:
  TCP(2), UDP(1) STEALTH
Jun 3 22:45:40 dns2 snort[8668]: spp_portscan:
  End of portscan from 207.174.228.81
--------
[**] SCAN-SYN FIN [**]
06/03-22:45:28.821565 207.174.228.81:111 -> z.y.w.66:111 TCP
  TTL:27 TOS:0x0 ID:39426 **SF**** Seq: 0xC8A3EA5 Ack:
  0x5F4322AB Win: 0x404 00 01 00 00 00 00 ......

[**] RPC Info Query [**]
06/03-22:45:29.160691 207.174.228.81:880 -> z.y.w.66:111 TCP
  TTL:49 TOS:0x0 ID:30945 DF *****PA* Seq: 0x1ED9A545 Ack:
  0xE4D93173 Win: 0x7D78
TCP Options => NOP NOP TS: 70043372 688047587 80 00 00 28 54 36
```

```
  FE 57 00 00 00 00 00 00 00 02 ...(T6.W........ 00 01 86 A0 00
  00 00 02 00 00 00 04 00 00 00 00 ................ 00 00 00 00
  00 00 00 00 00 00 00 00 ............

Jun 3 22:45:29 dns3 snort[9890]: spp_portscan:
  PORTSCAN DETECTED from 207.174.228.81
Jun 3 22:45:29 dns3 snort[9890]: SCAN-SYN FIN:
  207.174.228.81:111 -> z.y.w.98:111
Jun 3 22:45:29 dns3 snort[9890]: RPC Info Query:
  207.174.228.81:881 -> z.y.w.98:111
Jun 3 22:45:35 dns3 snort[9890]: spp_portscan:
  portscan status from 207.174.228.81: 3 connections across 1 hosts:
  TCP(2), UDP(1) STEALTH
Jun 3 22:45:41 dns3 snort[9890]: spp_portscan:
  End of portscan from 207.174.228.81
```

1. Source of trace

http://www.sans.org/y2k/060600-1200.htm

2. Detect was generated by:

Snort intrusion detection system. The relevant fields for analysis are: date/time, target host name, attack signature, source/destination IPs & port numbers, identification number/flags and, TCP options.

3. Probability the source address was spoofed

The IP was probably not spoofed. It wouldn't be needed to accomplish the portscan.

4. Description of attack:

The attack appears to be a stealth port scan employing SF flags in an attempt to avoid IDS detection or system logging. All source ports are low numbered trusted ports. The aberration occurs on 06/03 @ 22:45:29.160691 wherein the DF PA bits are set, (TCP options is nop) indicating a buffer over flow attempt.

5. Attack mechanism:

The attack is targeting DNS servers, port 111. All target hosts are DNS with the exception of HOSTH. The attack is portscanning using SF flags with the one exception, where DF*P*A bits are set. The attack maybe targeting portmapper in an attempt to compromise this service so as to allow the attacker to assign programs to listen on specific UDP/TCP ports for future connections.

6. Correlations:

This detect was attributed to Laurie.edu. This attack has been correlated over two days worth of logs. Steve Richards reported a SYN-FIN attack against a DNS in March 2000 http://www.sans.org/y2k/032400-2000.htm and Laurie.edu http://www.sans.org/y2k/032900-2000.htm

7. Evidence of active targeting:

The attacker appears to be actively targeting DNS and port 111.

8. Severity:

5 +4 – (3 + 4) = 2

9. Defensive recommendation:

Recommend the installation of portmapper programs that invoke ACLs and logs.
Block port 111 at the Firewall.

10. This attack has the attribute(s) of:

a) DNS Load Balancing
b) DNS buffer overflow
c) DNS portscan
d) b & c

Answer: d

Detect 3

```
Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3483
  to server1/27374 flags SYN
Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-7-106011:
  Deny inbound (No xlate) tcp src outside:216.58.19.218/3487
  dst outside:global/27374
Jun 03 00:06:26 [FW1] Jun 03 2000 00:08:00: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3488
  to server2/27374 flags SYN
Jun 03 00:06:27 [FW1] Jun 03 2000 00:08:01: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3483
  to server1/27374 flags SYN
Jun 03 00:06:27 [FW1] Jun 03 2000 00:08:01: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3488
  to server2/27374 flags SYN
Jun 03 00:06:28 [FW1] Jun 03 2000 00:08:02: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3488
  to server2/27374 flags SYN
Jun 03 00:06:29 [FW1] Jun 03 2000 00:08:03: %PIX-7-106011:
  Deny inbound (No xlate) tcp src outside:216.58.19.218/3487
  dst outside:global/27374
Jun 03 00:06:29 [FW1] Jun 03 2000 00:08:03: %PIX-2-106001:
  Inbound TCP connection denied from 216.58.19.218/3491
  to server3/27374 flags SYN
```

1. Source of trace

http://www.sans.org/y2k/060600.htm

2. Detect was generated by:

Pix Firewall logs. Date/time fields can help detect coordinated attacks or attack spacing or situation awareness; Source data field may identify attacker host and location (if not spoofed); Actions taken by the system or firewall indicates response to attack; Destination host data can be used to indicate the criticality of the attack; Port number field can indicate the exploit the hacker is seeking to execute and the potential lethality of the attack; and, the flags field can indicate the hacker's attack technique/mechanism to realize an exploit.

3. Probability the source address was spoofed

The source address was probably not spoofed in an attempt to complete a 3 way handshake.

4. Description of attack:

The attack is a probe for port 27374, which is a notorious Trojan port used to execute Subseven. Jeff detected one - http://www.sans.org/y2k/033000-2300.htm

5. Attack mechanism:

The attacker is probing for a specific open port on two servers and uses SYN to establish a connection. The attack alternates probes between server 1 & 2. This represents a possible slow and go technique to avoid detection. There's a 1-2 minute delay between probes. The attack uses a static source port-to-server mapping. Specifically, server 1 is probed by source port 3483, server 2 by port3488.

6. Correlations:

This detected was attributed to Roger Lutz. This detect has been noted on several traces before and is a recent but popular attack.

7. Evidence of active targeting:

Attacker is blatantly targeting a specific port, 27374.

8. Severity:

4 + 5 – (3 + 5) = 1

9. Defensive recommendation:

Defense seems solid at the network level. Firewall denied connection. Suggest port/service be closed at the system level.

10. This attack is a:

a) Probe for a Trojan port
b) mscan
c) syn flood
d) none of the above

Answer: a

Detect 4

```
May 29 12:27:40 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.48.137
May 29 12:27:49 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.49.137
May 29 12:28:01 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.50.137
May 29 12:28:02 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.50.137
May 29 12:28:10 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.51.137
May 29 12:28:19 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.52.137
May 29 12:28:28 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.53.137
May 29 12:28:39 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.54.137
May 29 12:28:42 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.54.137
May 29 12:28:48 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.55.137
May 29 12:29:57 pyramid 28 deny: UDP from
  208.21.150.39.137 to 204.245.8.62.137
```

1. Source of trace

http://www.sans.org/y2k/053100.htm

2. Detect was generated by:

Detect appears to be generated by the systems logs. Important fields are the date/time used to determine attack timing or sequencing; Target host name to determine criticality, if the name indicates service being provided; Action taken by the host to determine current state of the attack; Protocol type can help categorized or pinpoint the exploit using traffic analysis; Source IP identifies the attack host/location; Destination IP identifies target host; and , the port number can indicate potential exploits or hacker intentions.

3. Probability the source address was spoofed

The IP was probably not spoofed to execute this attack.

4. Description of attack:

Attack appears to be a Netbios scan of a class C network to determine if a system is running services from port 137. The attack is an automated scan of successive hosts. The objective is to determine which, if any, host within the specified scan range has port 137 open. The only unusual or noticeable activity of this scan is that on every third host it executes a double scan for 137, i.e., it repeats the scan on the same host.

5. Attack mechanism:

The attack works by sending a UDP packet to probe each target host's port 137. UDP's connectionless attributes allow for fact probes. If a host responds with an open port 137, the attacker will probably note the response for future reference. This appears to be a reconnaissance activity.

6. Correlations:

This detect was attributed to James Lippard. This particular detect has been seen before, probes for netbios are plentiful. Robert Sorensen reported one www.sans.org/y2k/032400-2000.htm

7. Evidence of active targeting:

Attack is actively targeting port 137.

8. Severity:

3 + 5 – (5 + 4) = -1

9. Defensive recommendation:

Defenses are sound, access was denied. Recommend network level devices block UDP/TCP 137.

10. An objective of this attack was:

a) To flood port 137
b) Execute Trojan code
c) Scan for port 137
d) none of the above

Answer: c

Detect 5

```
Jun 3 00:34:01 cc1014244-a kernel: securityalert: tcp if=ef0
  from 24.3.6.190:4421 to 24.3.21.199 on unserved port 27374
Jun 3 00:41:57 cc1014244-a kernel: securityalert: tcp if=ef0
  from 24.3.6.190:2649 to 24.3.21.199 on unserved port 27374
Jun 3 00:57:49 cc1014244-a kernel: securityalert: tcp if=ef0
  from 24.3.6.190:2086 to 24.3.21.199 on unserved port 27374
Jun 3 01:51:17 cc1014244-a kernel: securityalert: tcp if=ef0
  from 24.3.9.15:1567 to 24.3.21.199 on unserved port 27374
Jun 3 05:39:48 cc1014244-a kernel: securityalert: udp if=ef0
  from 62.125.37.168:60000 to 24.3.21.199 on unserved port 2140
Jun 3 11:11:06 cc1014244-a kernel: securityalert: tcp if=ef0
```

```
  from 210.140.231.147:109 to 24.3.21.199 on unserved port 109
Jun 3 11:33:22 cc1014244-a kernel: securityalert: tcp if=ef0
  from 208.191.77.182:2982 to 24.3.21.199 on unserved port 8080
Jun 3 11:33:23 cc1014244-a kernel: securityalert: tcp if=ef0
  from 208.191.77.182:2982 to 24.3.21.199 on unserved port 8080
Jun 3 14:25:20 cc1014244-a kernel: securityalert: tcp if=ef0
  from 24.6.159.44:1242 to 24.3.21.199 on unserved port 27374
Jun 3 14:47:54 cc1014244-a kernel: securityalert: udp if=ef0
  from 24.15.67.242:137 to 24.3.21.199 on unserved port 137
```

1. Source of trace

http://www.sans.org/y2k/060500.htm

2. Detect was generated by:

Detect was generated by system logs. The fields for analysis are – Date/time; a kernel identifier; Protocol field and interface used; source IP/port and destination IP/port.

3. Probability the source address was spoofed

The source address was probably not spoofed. Exploit appears to be a reconnaissance effort using multiple source IP addresses.

4. Description of attack:

The attack appears to be a slow scan of a single host on a class A subnet. The attack employs a combination of UDP and TCP packets to scan for Windows-based vulnerabilities to exploit. This assessment is based on the target destination ports and correlation with other system logs for different time periods.

5. Attack mechanism:

The attack works by executing scans for specific ports with the least amount of noise. Noise reduction is accomplished by very slow scans. Time lapses in between scans range from 13 minutes to 6 hours. Multiple source IPs and Port numbers are used to scan multiple ports on a single host, 199. The targeted ports have well document exploits. A stealth scanning application like Nmap may have been used to conduct this scan. This attack has the maskings of a multi-distributed, coordinated scan.

6. Correlations:

This detect was conducted by Binette. It has been report on other occasions, December 1999 and May 2000.

7. Evidence of active targeting:

The attack is targeting a specific host (199) on this class A network.

8. Severity:

3 + 5 – (3 – 2) = 3

9. Defensive recommendation:

Need to deploy/configure Firewall to block these ports. Recommend review of host-based safeguard activity to deny access to or eliminate unused services.

10. This attack is actively targeting:

a) a specific port
b) multiple networks
c) a specific host
d) all of the above

Answer: c

Detect 6

```
Jun 4 01:37:42 solar portsentry[721]: attackalert: Unknown Type: Packet
  Flags: SYN: 1 FIN: 1 ACK: 0 PSH: 0 URG: 0 RST: 0 from host:
  PF-231-147.tokyoweb.or.jp/210.140.231.147 to TCP port: 109
Jun 4 01:37:42 solar portsentry[721]: attackalert: Host 210.140.231.147
  has been blocked via wrappers with string: "ALL: 210.140.231.147"
Jun 4 01:37:42 solar portsentry[721]: attackalert: Host 210.140.231.147
  has been blocked via dropped route using command: "/sbin/ipchains -I
  input -s 210.140.231.147 -j DENY -l"
```

1. Source of trace

http://www.sans.org/y2k/06500.htm

2. Detect was generated by:

Portsentry. Fields relevant to analysis are – date/time fields; attack type; flags set; source IP and port number; target port number; and, system response to attack.

3. Probability the source address was spoofed

The IP was probably not spoofed for this attack.

4. Description of attack:

This attack is against a port 109, maybe a mail server. This appears to be either a fingerprinting activity to identify the operating system or an attempted stealth probe for POP.

5. Attack mechanism:

The attack works by using a crafted packet with the SYN-FIN bits set. In one scenario, the response of the O/S can provide a fingerprint indicating what O/S is running and thereby scope the exploit for the identified system. In another scenario the attacker is trying to avoid detection by combining SYN-FIN flags as some intrusion detection systems will not drop a packet with this combination of flags. POP is being attacked maybe as a possible launch point for a Spam attack or information collection of mail addresses.

6. Correlations:

This detect was attributed Pierre Lamy. Syn-Fin fingerprinting exploits are a common practice and a have been detected on previous occasions. Alex Luetzow reported one, http://www.sans.org/y2k/043000.htm

7. Evidence of active targeting:

Can't conclusively determine if active targeting is taking place due to brevity of trace. However, SYN-FIN flags to port 109 would indicate such.

8. Severity:

4 + 4 - (3 + 4) = 1

9. Defensive recommendation:

Defenses seem adequate at the system level, with the presence of Portsentry and TCP wrapper. Firewall should drop packets in support of host-based policy.

10. The use of SYN-FIN flags most likely indicates what type of attack(s)?

a) Buffer overflow
b) O/S fingerprinting
c) Stealth attack
d) b or c

Answer: d

Detect 7

```
14:20:38.606496 ip 62: 1Cust136.tnt31.atl2.da.uu .net.2895 > my.box.23:
  S 21147693:21147693(0) win 8192 <mss 536,nop,nop,sack OK> (DF)
  (ttl 115, id 13097) 4500 0030 3329 4000 7306 686a 3f26 4088 1803 d483
0b4f
  0017 0142 b02d 0000 0000 7002 2000 3db1 0000 0204 0218 0101 0402
14:20:38.655185 ip 62: my.box.23 > 1Cust136. tnt31.atl2.da.uu.net.2895:
  S 2715738005:2715738005(0) ack 21147694 win 16616 <ms s
1460,nop,nop,sackOK>
  (DF) (ttl 128, id 2897)
14:20:38.998631 ip 60: 1Cust136.tnt31.atl2.da.uu .net.2895 > my.box.23:
  . ack 1 win 8576 (DF) (ttl 115, id 20009) 4500 0028 4e29 4000 7306
4d72
  3f26 4088 1803 d483 0b4f 0017 0142 b02e a1de df96 5010 2180 e3d3 0000
  0000 0001 0800
14:20:39.005475 ip 60: 1Cust136.tnt31.atl2.da.uu .net.2895 > my.box.23:
  P 1:4(3) ack 1 win 8576 (DF) (ttl 115, id 20521)
14:20:39.182122 ip 54: my.box.23 > 1Cust136. tnt31.atl2.da.uu.net.2895:
  . ack 4 win 16613 (DF) (ttl 128, id 2898) 4500 0028 0b52 4000 8006
8349
  1803 d483 3f26 4088 0017 0b4f a1de df96 0142 b031 5010 40e5 c46b 0000
```

1. Source of trace

http://www.sans.org/y2k/053000-1100.htm

2. Detect was generated by:

TCPdump. It provides the time of attack and IP ID; source IP and port number; destination IP and port number; flags & sequence numbers; window size maximum segment size; IP flags; packets TTL; packet ID, and Hex output

3. Probability the source address was spoofed

The source was probably not spoofed. There's a 3 way handshake involved.

4. Description of attack:

This particular probe is against port 23, telnet. This trace represents a portion of active, but slow, probes for exploitable ports on MY.BOX. A different probe takes place every 2-3 hours. Either the attacker is very busy conducting other attacks in between probes or attempting to avoid detection.

5. Attack mechanism:

The attacker has apparently established a 3 way handshake and pushed some data through. The attacker will inevitably tag this system (MY.BOX) and service for future reference as either a potential system to exploit or for use as an attack launch point.

6. Correlations:

Detect was contributed by Stephan Odak. This attack can be correlated with at least 2-3 days worth of traces, same URL.

7. Evidence of active targeting:

The attack is targeting a specific system for probing activities

8. Severity:

4 + 5 – (4 + 3) = 2

9. Defensive recommendation:

Defense seems marginal. There's and IDS and I assume a complementary Firewall. Suggest telnet sessions be passworded and host based safeguards be installed/activated to emulate firewall policy.

10. This attack establishes a _______ connection:

a) DNS
b) RPC
c) Telnet
d) POP

Answer: c

Detect 8

```
06/07/2000 16:56:30.224 UDP packet dropped 24.22.99.180, 1240, WAN
  206.230.232.xx, 161, LAN 0
06/07/2000 16:56:32.896 UDP packet dropped 24.22.99.180, 1251, WAN
  206.230.232.xx, 161, LAN 0
06/07/2000 16:56:35.256 UDP packet dropped 24.22.99.180, 1267, WAN
  206.230.232.xx, 161, LAN 0
06/07/2000 16:56:37.880 UDP packet dropped 24.22.99.180, 1284, WAN
  206.230.232.xx, 161, LAN 0
```

1. Source of trace

http://www.sans.org/y2k/061000.htm

2. Detect was generated by:

System logs. Fields used for analysis are – date/time; offending packet protocol; action taken; source IP and port number; network type (WAN,LAN); target IP and port number; target network type/ID.

3. Probability the source address was spoofed

The source address was probably not spoofed.

4. Description of attack:

This attack is targeting SNMP (161) on a class B subnet. This appears to be a attack using multiple high numbered (1240, 1251, 1267, 1284) ports on a single host (24.22.99.180) to probe port 161 on a target system (206.230.232.xx).

5. Attack mechanism:

The attack works by attempting to send a crafted SNMP message to the target host, port 161 from multiple high numbered ports. The use of multiple ports may be to avoid detection. Without the HEX dump can't determine what data or message content was transmitted. Port 161 may have been targeted because SNMP can be used to internally map a network structure or shut down operations. Content analysis, via Hex dump, would provide more insight into attack objectives.

6. Correlations:

This detect was contributed by Todd Kohl. Unable to locate any data to exactly correlate this attack. A similar detect was provided by David Hoelzer, http://www.sans.org/y2k/042600.htm.

7. Evidence of active targeting:

Attack on a specific subnet and port number indicates active targeting.

8. Severity:

4 + 4 – (4 + 3) = 1

9. Defensive recommendation:

Defense seems adequate packet was dropped.

10. What type of attack signature is this?

a) DoS attack
b) SNMP probe
c) SNMP buffer over flow
d) all of the above

Answer: b

Detect 9

```
Jun 7 17:52:10 hostm /kernel:
  Connection attempt to TCP z.y.x.14:8080 from 202.235.50.12:65535
Jun 7 17:59:25 dns1 snort[266909]: MISC-WinGate-8080-Attempt:
  202.235.50.12:65535 -> z.y.w.34:8080
Jun 7 17:59:26 dns2 snort[8668]: MISC-WinGate-8080-Attempt:
  202.235.50.12:65535 -> z.y.w.66:8080
Jun 7 17:59:27 dns3 snort[1813]: MISC-WinGate-8080-Attempt:
  202.235.50.12:65535 -> z.y.w.98:8080
--------
[**] MISC-WinGate-8080-Attempt [**]
  06/07-17:59:25.458320 202.235.50.12:65535 -> z.y.w.34:8080 TCP
  TTL:240 TOS:0x0 ID:15990 **S***** Seq: 0x3E760000 Ack: 0x0 Win:
  0x200 00 00 00 00 00 00 ......
[**] MISC-WinGate-8080-Attempt [**]
  06/07-17:59:26.099813 202.235.50.12:65535 -> z.y.w.66:8080 TCP
  TTL:240 TOS:0x0 ID:15990 **S***** Seq: 0x3E760000 Ack: 0x0 Win:
  0x200 16 90 49 32 1D E1 ..I2..
[**] MISC-WinGate-8080-Attempt [**]
  06/07-17:59:26.734588 202.235.50.12:65535 -> z.y.w.98:8080 TCP
  TTL:240 TOS:0x0 ID:15990 **S***** Seq: 0x3E760000 Ack: 0x0 Win:
  0x200 00 00 00 00 00 00 ......
```

1. Source of trace

http://www.sans.org/y2k/061000.htm

2. Detect was generated by:

Snort intrusion detection. For this detect the fields used were in the HEX output - date/time field; source IP and port number; destination IP and port number; protocol; TTL value; ID value; and flag fields.

3. Probability the source address was spoofed

The IP was probably spoofed.

4. Description of attack:

The attack is a scan for port 8080 which a documented hacker friendly port.

5. Attack mechanism:

The attack works by using a crafted packet to scan multiple hosts on a target network for port 8080, Ring0, a notorious port. The source port is 65535 and the ID number for each packet is static (15990), both of which are signatures of hacker activity. An attacker is targeting DNS servers probably because of their criticality to a system and the range of damage that can be inflicted from a compromised DNS.

6. Correlations:

This detect was attributed to Uonumanet Ltd, Niigata, JP. Correlations were found in contributions by Arrigo (052300 – 0800), Mou-liang Kung (61100.htm), Phillip (052500.htm)

7. Evidence of active targeting:

Attack targets a specific port on a specific network.

8. Severity:

5 + 5 - (3 + 3) = 4

9. Defensive recommendation:

Defenses do not seem adequate. There's no indication that packets were dropped at the [1]network level, nor was there a "deny" at the host. Recommend network level controls be installed to drop packets or filter traffic from/to these ports.

10. A static IP identifier for packets generated at different times indicates:

a) frugal use of Id numbers
b) a crafted packet

[1] Mark Freeman, SANS 2000, Practical Exam

c) Good programming practices
d) all of the above

Answer: b

Detect 10

```
Jun 05 2000 21:30:30: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1051
Jun 05 2000 21:32:30: Deny inbound UDP
  from 169.132.184.211/6801 to x.x.x.31/1052
Jun 05 2000 21:34:30: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1053
Jun 05 2000 21:36:31: Deny inbound UDP
  from 169.132.184.211/6801 to x.x.x.31/1054
Jun 05 2000 21:38:31: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1055
Jun 05 2000 21:40:31: Deny inbound UDP
  from 169.132.184.211/6801 to x.x.x.31/1056
Jun 05 2000 21:42:31: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1057
Jun 05 2000 21:44:31: Deny inbound UDP
  from 169.132.184.211/6801 to x.x.x.31/1058
Jun 05 2000 21:46:31: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1059
Jun 06 05:55:14: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1303
Jun 06 05:59:06: Deny inbound UDP
  from 169.132.184.211/6801 to x.x.x.31/1304
Jun 06 06:01:08: Deny inbound UDP
  from 216.53.10.1/6801 to x.x.x.31/1305
```

1. Source of trace

http://www.sans.org/y2k/060900.htm

2. Detect was generated by:

Detect appears to be generated by system logs which provided date/time; action taken; protocol type and direction; source IP and port; destination IP and port.

3. Probability the source address was spoofed

The source IP was probably spoofed.

4. Description of attack:

The attack appears to be a port scan of high numbered ports using UDP packets.

5. Attack mechanism:

The attack is executed by using, or simulating the use of, two different hosts to transmit UDP packets from the same port number (6801) to a target IP. A dual system attack against a single host. The attacking hosts are conducting a sequential (but alternating) scan of each port on the target system. One host is scanning odd numbered ports, the other is scanning even numbered ports. There's an approximately 2 minute delay between scans which indicates the offending host is either busy intermittently conducting other attacks, or trying to make as little noise as possible or both. This appears to be reconnaissance activity against a specific host.

6. Correlations:

This particular system log has captured data over a two day period.

7. Evidence of active targeting:

A specific host is being targeted.

8. Severity:

3 + 3 – (4 + 3) = -1

9. Defensive recommendation:

Defenses are adequate the UDP packet was denied.

10. This attack signature appears to be:

a.) A troll for Trojan ports
b.) A DoS attack
c.) A Port scan
d.) All of the above

Answer: c