Detect 1

```
23:41:43.627936 scanner.com.4793 > 131.x.x.14.23: S
2797519430:2797519430(0) win 16060 <mss 1460,sackOK,timestamp
1915100[|tcp]> (DF) (ttl 55, id 55658)
23:41:43.637459 scanner.com.4799 > 131.x.x.20.23: S
2802462124:2802462124(0) win 16060 <mss 1460,sackOK,timestamp
1915100[|tcp]> (DF) (ttl 55, id 55664)
23:41:43.647481 scanner.com.4815 > 131.x.x.36.23: S
2788968898:2788968898(0) win 16060 <mss 1460,sackOK,timestamp
1915101[|tcp]> (DF) (ttl 55, id 55680)
23:41:43.801627 scanner.com.4837 > 131.x.x.58.23: S
2801771736:2801771736(0) win 16060 <mss 1460,sackOK,timestamp
1915120[|tcp]> (DF) (ttl 55, id 55718)
23:41:43.904159 scanner.com.4852 > 131.x.x.73.23: S
2792789447:2792789447(0) win 16060 <mss 1460,sackOK,timestamp
1915130[|tcp]> (DF) (ttl 55, id 55738)
23:41:44.630652 scanner.com.4865 > 131.x.x.86.23: S
2805664397:2805664397(0) win 16060 <mss 1460,sackOK,timestamp
1915200[|tcp]> (DF) (ttl 55, id 55798)
```

1.1 Source of trace

My network.

1.2 Detect was generated by:

Windump filter.

1.3 Probability the source address was spoofed

It is unlikely this source address was spoofed, as the attacker here appears to be searching for hosts listening on port 23. In order to learn this, the attacker needs to be able to receive the responses from the hosts being scanned. The source itself may be a compromised host, however.

1.4 Description of attack:

Scan of hosts on a network, looking to map out which hosts accept incoming tcp connections to port 23, telnet.

1.5 Attack mechanism:

This is reconnaissance in preparation for a future attack. It's an attempt to map out which hosts allow incoming telnet connections. The intention is probably to attempt to compromise one or more of these hosts via a telnetd vulnerability exploit. Nonexistent hosts will generate no reply or "host not found", and existing hosts will generate either reset packets (not listening on port 23) or SYN/ACK packets (open port 23). If the host is listening on port 23, and the three-way TCP handshake is completed, the attacker will receive a login banner that probably will reveal some useful information about this host: operating system and version, as well as possibly other information about that system. Based on this information, the attacker will be able to focus on a specific system, using exploits tailored to the telnet daemon under that system's operating system.

1.6 Correlations:

This type of detect has been seen many times, both at our site and elsewhere. The scanning tool is similar to the tool described by CERT at http://www.cert.org/incident_notes/IN-98.02.html. The attacker may be hoping to exploit a telnet vulnerability such as the one discussed by CERT in http://www.cert.org/advisories/CA-95.14.Telnetd_Environment_Vulnerability.html.

1.7 Evidence of active targeting:

No. This is likely a general scan of the entire campus network, given that a sniffer on this subnet shows a large number of addresses on that subnet being tried, and logs on other subnets show similar activity from the same source address. Many of the hosts being scanned are either nonexistent or do not support telnet.

1.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 2 [scan itself is not lethal, but could lead to more serious attack]

System Countermeasures = 2 [many systems scanned, only some have any countermeasures in place against telnet scans; some systems running telnetd may not be fully patched or observed]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+2) - (2+2)] = 0

1.9 Defensive recommendation:

Blocking replies to this host address at the border routers is a reasonable course of action. However, a more proactive stance is advisable. This particular host address was blocked after individual sysadmins observed the scanning behavior by examining logfiles such as those generated by tcpwrappers. Network-based intrusion detection software would allow attempts such as this one to be detected more quickly and blocked more rapidly.

1.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) IP spoofing
b) Scan for hosts running telnetd
c) Port scan
d) SYN flooding
Answer: b

**

Detect 2

```
07:02:21.487822 210.x.8.50.0 > 131.x.x.226.109: SF
1598685184:1598685184(0) win 512 (ttl 230, id 26883)
07:02:21.546751 210.x.8.50.0 > 131.x.x.26.109: SF
1598685184:1598685184(0) win 512 (ttl 230, id 28930)
```

```
07:02:21.590098 210.x.8.50.0 > 131.x.x.14.109: SF
1598685184:1598685184(0) win 512 (ttl 230, id 64001)
```

2.1 Source of trace

My network.

2.2. Detect was generated by:

Windump filter.

2.3 Probability the source address was spoofed

Unlikely; the attacker here appears to be searching for hosts listening on port 109. In order to learn this, the attacker needs to be able to receive the responses from the hosts being scanned. The source itself may be a compromised host, however.

2.4 Description of attack:

Attempt to map out which hosts accept incoming tcp connections to port 109, POP2.

2.5 Attack mechanism:

This is an attempt at reconnaissance for a future attack. Packets are sent with TCP flags SYN and FIN both set, and with source port 0. This combination may slip past some IDS's, and can also provide information about the OS in use on targeted systems, as different operating systems respond differently to illegal TCP flag combinations, and to packets with source port 0. Based on the reply from a given host to these packets, the attacker will be able to focus on a specific system, using known exploits tailored to a particular operating system. It's not clear which is the primary intent here: finding an open POP2 port might be a side benefit to the main intent of OS fingerprinting using SYN/FIN and source port 0. POP2, being an older and now little-used protocol, would likely be running on an older machine with unpatched vulnerabilities, a machine possibly also not very closely watched. The attacker is less likely to find any open POP2 ports, but if one is found, it might be a promising avenue for attempting a known exploit, such as the POP2d Buffer Overflow Vulnerability. The source port 0 and SYN/FIN flags give the added benefit of providing information about the operating system in use on each host scanned.

2.6 Correlations:

This exact attack pattern – packets with source port 0 and SYN and FIN flags set, sent to port 109, is discussed on p. 168 of the GIAC text for section 2.4, *Network-Based Intrusion Analysis* by Stephen Northcutt, at SANS SNAP 2000 in San Jose, May 2000.

2.7 Evidence of active targeting:

No; this is likely a general scan of the entire campus network, given that a sniffer on this subnet shows a large number of addresses on that subnet being tried, and logs on other subnets show similar activity from the same source address.

2.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 1 [scan itself is not lethal, and we aren't running POP2]

System Countermeasures = 2 [many systems scanned, some may not be well-patched or closely monitored]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(1+2) – (2+2)] = -1

2.9 Defensive recommendation:

Blocking replies to this host address at the border routers is a reasonable course of action. However, a more proactive stance is advisable. This particular host address was blocked after individual sysadmins observed the scanning behavior by examining logfiles such as those generated by tcpwrappers and other host-based IDS's. Network-based intrusion detection software would allow attacks such as this one to be detected more quickly and blocked more rapidly. In addition, simply denying all packets with SYN and FIN set in combination, and all packets with source port 0, would block this particular type of scan from the outset.

2.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) DOS attack
b) Normal POP session
c) Scan for trojans
d) illegal flag combination
Answer: d

**

Detect 3:

```
Src IP address    date/time              tzone  filename
209.x.205.21      09/Jun/2000:15:04:36    700   T
viewsource/template.html?nuyhtgmEoez65qDkyfeBBvqe0j7hyfs8Ccsegrq2E6lkvm
20yz6020x05jbhcv66ng15ABaffvlr20oBhvt6z89drimiazBvD0Dw3t6unpbguBptgf
209.x.205.21      09/Jun/2000:15:21:34    700   T
viewsource/template.html?nuyhtgmEoez65qDkyfeBBvqe0j7hyfs8Ccsegrq2E6lkvm
20yz6020x05jbhcv66ng15ABaffvlr20oBhvt6nEwhr4qwo5nirwlB3f6unpbguBptgf
```

3.1 Source of trace

My network.

3.2. Detect was generated by:

RealServer log.

3.3 Probability the source address was spoofed

Possible. It's not clear that the attacker here needs to see replies from the victim site, since the goal appears to be denial of service.

3.4 Description of attack:

Attempt to exploit a known vulnerability on the Real Networks brand Real Server media server.

3.5 Attack mechanism:

This is an attempt to exploit the "ViewSource" vulnerability, a known security hole on RealServer systems that allows a remote attacker to send a malformed request using the command "viewsource/template.html" and thereby cause the RealServer software to hang until rebooted, shutting down all streaming media broadcasts in the interim.

3.6 Correlations:

This vulnerability has been discussed on Bugtraq at
http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-05-28&thread=4.1.20000601210348.00d6eca0@mail.real.com
And at
http://www.securityfocus.com/templates/archive.pike?list=1&date=2000-05-28&thread=4.3.1.0.20000602150841.00aeeac0@pop.schulte.org

3.7 Evidence of active targeting:

Yes. This is a publicly accessible media server and the attacker targeted it specifically. The timing of the attack coincided with an event that involved high visibility of this server to the public.

3.8 Severity:

Criticality = 4 [attack was well-targeted, however, temporary loss of this server would be embarrassing and inconvenient, but have no impact on core operations]

Lethality = 4 [known to cause denial of service]

System Countermeasures = 5 [Hole was previously closed and the system is fully patched and up to date]

Network Countermeasures = 2 [This IP blocked at border, but only after attempt was observed]

Severity = [(4+4) - (5+2)] = 1

3.9 Defensive recommendation:

Blocking replies to this host address at the border routers and notifying the system managers for the source site is a reasonable course of action, although there is a risk that this will result in an unintentional denial of access to a legitimate site whose address was being spoofed here. However, the most useful defense had already been performed: the manager of this system keeps up with security bulletins regarding this type of server, and had already taken steps to close this security hole, as well as scanning the logfiles for just such an attempt.

3.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Security vulnerability exploit
b) Normal HTTP session
c) Reconnaissance
d) Scan for trojans

Answer: a

**

Detect 4:

```
15:23:40.187107 208.x.x.200.44342 > 131.x.x.192.1722: R 0:0(0) ack
674719802 win 0 (ttl 243, id 64989)
17:01:12.922296 208.x.x.200.58799 > 131.x.x.238.1881: R 0:0(0) ack
674719802 win 0 (ttl 243, id 2347)
07:36:27.450135 208.x.x.200.58799 > 131.x.x.238.2021: R 0:0(0) ack
674719802 win 0 (ttl 243, id 33573)
08:57:29.659977 208.x.x.200.58799 > 131.x.x.238.1121: R 0:0(0) ack
674719802 win 0 (ttl 243, id 23637)
```

4.1 Source of trace

My network.

4.2. Detect was generated by:

Windump filter.

4.3 Probability the source address was spoofed

Unlikely. In order for this attack to succeed, responses need to be received by the source address.

4.4 Description of attack:

Unsolicited reset packets to various hosts on our network, all from the same source IP.

4.5 Attack mechanism:

Originally I thought this was a second-order effect caused by the source IP (a security website, in this case) being subjected to a denial of service attack from multiple spoofed IP addresses, some of which happen to correspond to real hosts on our network. These are various types of hosts receiving these packets: a printer, a random workstation, a router, etc. On further consideration, however, this is far more likely to be a slow inverse scan of the network using reset packets. The intent is to map the network by receiving no response in the case of existing hosts, and receiving "host unreachable" ICMP messages from a router in the case of nonexistent hosts. Inadequate monitoring tools for a switched network, and the lack of correlation from other subnets served at first to obfuscate the true nature of this scan attack. In retrospect, the particular sequence number used on these packets is a dead giveaway – it was even mentioned in class at the SNAP workshop.

4.6 Correlations:

Reset scans were mentioned at several points during the SANS SNAP 2000 Intrusion Detection workshop in San Jose, and an example of this exact technique, including the same crafted sequence numbers (probably generated by the same tool) is given on p. 304 of 2.4, *Network-Based Intrusion Analysis* by Stephen Northcutt.

4.7 Evidence of active targeting:

No. This is probably a scan to map the network in preparation for future targeted attacks.

4.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 2 [scan itself is not lethal, but could lead to more serious attack]

System Countermeasures = 2 [many systems scanned, apparently few have countermeasures to detect this type of scan]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+2) – (2+2)] = 0

4.9 Defensive recommendation:

Better network monitoring and coordination of information would be useful. Use of a stateful monitoring device or IDS, without which the two suspicious factors about these packets (unsolicited resets, and identical sequence numbers) would probably go unnoticed.

4.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Denial of service attack
b) inverse network mapping
c) Syn flooding
d) illegal flag combination

Answer: b

**

Detect 5:

```
01:59:01.220478 216.x.24.123 > 131.x.x.224: icmp: echo request
01:59:01.389937 216.x.24.123 > 131.x.x.228: icmp: echo request
01:59:01.846833 216.x.24.123 > 131.x.x.236: icmp: echo request
01:59:01.860851 216.x.24.123 > 131.x.x.237: icmp: echo request
01:59:01.941971 216.x.24.123 > 131.x.x.238: icmp: echo request
01:59:01.961574 216.x.24.123 > 131.x.x.239: icmp: echo request
01:59:02.263647 216.x.24.123 > 131.x.x.246: icmp: echo request
02:01:10.171905 216.x.24.123.2233 > 131.x.x.215.12345: S
4901255:4901255(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
02:01:10.172692 131.x.x.215.12345 > 216.x.24.123.2233: R 0:0(0) ack
4901256 win 0
02:01:10.205224 216.x.24.123.2234 > 131.x.x.215.27374: S
4901319:4901319(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
02:01:10.205308 131.x.x.215.27374 > 216.x.24.123.2234: R 0:0(0) ack
4901320 win 0
```

5.1 Source of trace

My network.

5.2. Detect was generated by:

Windump filter.

5.3 Probability the source address was spoofed

Highly unlikely. The attacker needs to be able to see replies to these packets.

5.4 Description of attack:

A ping sweep, followed by SYN packets sent to known trojan ports on any hosts that replied to the pings.

5.5 Attack mechanism:

According to lists of well-known trojan ports such as the one posted at http://www.simovits.com/nyheter9902.html, port 12345 is used by a number of trojans, including GabanBus, My Pics, NetBus, Pie Bill Gates, Whack Job, and X-bill; and port 27374 is used by the SubSeven trojan.

5.6 Correlations:

The SubSeven trojan is discussed at http://www.datafellows.com/v-descs/subseven.htm**, and Netbus is discussed at** http://www.europe.f-secure.com/v-descs/netbus.htm.
The use of a ping sweep prior to a more targeted attack is discussed in many places, including the glossary at http://www.3dg.com/cybercop/resources/glossary.html.

5.7 Evidence of active targeting:

Yes, to some degree. First a non-targeted ping sweep of the network is made, and then followed with SYN packets targeted directly to the machines that replied to the pings.

5.8 Severity:

Criticality = 2 [attack not well-targeted, various systems scanned, none of which actually housed the trojans sought]

Lethality = 2 [scan itself relies on trojans having been previously installed, which they weren't on these systems]

System Countermeasures = 2 [many systems scanned, apparently few have countermeasures to detect this type of scan]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+2) - (2+2)] = 0

5.9 Defensive recommendation:

Blocking this IP address at the border routers once the attack pattern was discovered was a reasonable course of action. We might also consider blocking SYN packets sent to some of these specific ports. A network-based intrusion detection system might have alerted us to the ping sweep before the followup trojan scan occurred.

5.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Ping o' Death
b) Smurf attack
c) Trojan scan
d) Land attack

Answer: c

**

Detect 6 is

```
6/9/00      9:54:59 PM  Security    Failure Audit     Logon/Logoff
      529   NT AUTHORITY\SYSTEM     MOYA  Logon Failure:
      Reason:           Unknown user name or bad password
      User Name:  SERVICE
      Domain:           FIELDSAUTO
      Logon Type: 3
      Logon Process:    KSecDD
      Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
      Workstation Name: \\SERVICE1
20:54:55.643887 38.x.105.200.11768 > 131.x.x.215.139: S
235543338:235543338(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:54:55.644004 131.x.x.215.139 > 38.x.105.200.11768: S
1719199:1719199(0) ack 235543339 win 8244 <mss 1374> (DF)
20:54:55.821847 38.x.105.200.11768 > 131.x.x.215.139: . ack 1 win 8244
(DF)
20:54:55.829058 38.x.105.200.11768 > 131.x.x.215.139: P 1:73(72) ack 1
win 8244 (DF)
20:54:55.829197 131.x.x.215.139 > 38.x.105.200.11768: P 1:5(4) ack 73
win 8172 (DF)
20:54:56.024737 38.x.105.200.11768 > 131.x.x.215.139: P 73:231(158) ack
5 win 8240 (DF)
20:54:56.036517 131.x.x.215.139 > 38.x.105.200.11768: P 5:102(97) ack
231 win 8014 (DF)
20:54:56.243938 38.x.105.200.11768 > 131.x.x.215.139: P 231:387(156)
ack 102 win 8143 (DF)
20:54:56.366554 131.x.x.215.139 > 38.x.105.200.11768: . ack 387 win
7858 (DF)
20:54:59.344783 131.x.x.215.139 > 38.x.105.200.11768: P 102:141(39) ack
387 win 7858 (DF)
20:54:59.531785 38.x.105.200.11768 > 131.x.x.215.139: F 387:387(0) ack
141 win 8104 (DF)
20:54:59.531943 131.x.x.215.139 > 38.x.105.200.11768: F 141:141(0) ack
388 win 7858 (DF)
20:54:59.705787 38.x.105.200.11768 > 131.x.x.215.139: . ack 142 win
8104 (DF)
```

6.1 Source of trace

My network.

6.2 Detect was generated by:

Windump log correlated with Windows Event Viewer with auditing policy for login success/failure.

6.3 Probability the source address was spoofed

Highly unlikely. The attacker needs to be able to see replies to these packets.

6.4 Description of attack:

An attempt to successfully guess the Administrator password for this computer and log in remotely via Windows Networking.

6.5 Attack mechanism:

This machine has an open NetBIOS port. An attacker attempted to exploit this by trying to guess the password for the Administrator account, so as to gain control of this host.

6.6 Correlations:

The pages at www.grc.com discuss in detail the ways in which Microsoft Networking is insecure, and predict attacks just like this one.

6.7 Evidence of active targeting:

Yes. Only this machine was targeted. This could have been the next step after a reconnaissance probe for machines listening on port 139.

6.8 Severity:

Criticality = 2 [non-critical desktop machine targeted]

Lethality = 3 [administrator privileges over a desktop system were sought]

System Countermeasures = 4 [this type of attack was anticipated and effective countermeasures were taken]

Network Countermeasures = 2 [This IP blocked at border, but only after attack was observed]

Severity = [(2+3) – (4+2)] = -1

6.9 Defensive recommendation:

Blocking this IP address at the border routers once the attack pattern was discovered was a reasonable course of action. If a Windows machine must allow remote access, as this one does, appropriate steps include severely restricting which accounts have remote access privileges, renaming the Administrator account, and making share names hidden. All of these steps were taken. Since without the Windows Event Log correlation, this simply looks like a normal transaction, it is not immediately clear how to set up an IDS rule to detect such attacks. Logging connections to port 139 from outside the local network might be advisable. For Windows systems that have no need to allow remote filesharing, following the instructions on http://grc.com/faq-shieldsup.htm#139 for closing port 139 is an excellent course of action. Failing that, see http://www.cert.org/security-improvement/implementations/i041.04.html for some instructions about creating auditing policies in NT.

6.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Trojan scan
b) Normal Windows Networking session
c) IP spoofing
d) Password-guessing attempt

Answer: c

**

Detect 7:

```
59     2000-06-14 04:50:05    2003105      SubSeven port probe
128.x.x.110  r42h110.res.univ.edu    131.x.x.75
port=27374&name=Sub_7_2 1
```

```
59     2000-06-14 04:50:57    2003105      SubSeven port probe
128.x.x.47   sc47.eastnet.univ.edu   131.x.x.75
port=1243&name=Sub_7    1
59     2000-06-14 04:51:14    2003103      NetBus port probe
128.x.x.28   r80h28.res.univ.edu     131.x.x.75
port=12345&name=NetBus  1
```

7.1 Source of trace

My network.

7.2. Detect was generated by:

BlackICE host-based IDS. Format is: Severity (As calculated by BlackICE), Datestamp (GMT), BlackICE IssueID, BlackICE Issue Name, source IP, source domain (if available), victim IP, "parameters" including source port, number of iterations of this specific attack.

7.3 Probability the source address was spoofed

Unlikely. Unless this scan is simply intended to make people think that univ.edu has some compromised machines, the attack won't succeed unless the source hosts are able to receive replies from the victim machine.

7.4 Description of attack:

Ports commonly used by trojans are probed with SYN packets to see if they're open. If they are open, the victim host likely has a trojan running on it awaiting remote control.

7.5 Attack mechanism:

SYN packets are sent to specific ports used by trojan horse programs. If a SYN/ACK is received in response, rather than a reset packet (as would happen if the victim existed but did not have these unusual ports open), then a connection can be completed and the trojan horse program listening on the victim computer can be activated and controlled. In all likelihood the source hosts in this case have themselves already been compromised.

7.6 Correlations:

The SubSeven trojan is discussed at http://www.datafellows.com/v-descs/subseven.htm, and http://advice.networkice.com/advice/Phauna/RATs/SubSeven/default.htm. Netbus is discussed at http://www.europe.f-secure.com/v-descs/netbus.htm.

7.7 Evidence of active targeting:

No. Initially it appeared that this host might have been targeted, however, similar probes of this port from these same source IP's were reported on other hosts on this network, many of which were not even running Windows, which is the operating system required by the SubSeven and NetBus remote control trojans. Targeting might have been active to the extent that only valid IP's appear to have been probed, indicating that a previous reconnaissance sweep might have weeded out invalid IP addresses on this network.

7.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 2 [scan itself relies on trojans having been previously installed, which they weren't on these systems]

System Countermeasures = 2 [many systems scanned, apparently few have countermeasures to detect this type of scan]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+2) - (2+2)] = 0

7.9 Defensive recommendation:

Blocking this IP address at the border routers once the attack pattern was discovered was a reasonable course of action. Alerting on SYN packets sent to these well-known trojan ports might be worth considering as well.

7.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Trojan scan
b) Normal Windows Networking session
c) IP spoofing
d) Password-guessing attempt

Answer: a

**

Detect 8:

```
01:22:47.310076 210.x.231.147.53 > 131.x.x.76.53: SF
2078088031:2078088031(0) win 1028 (ttl 28, id 39426)
01:22:47.329663 210.x.231.147.53 > 131.x.x.77.53: SF
2078088031:2078088031(0) win 1028 (ttl 28, id 39426)
01:22:47.509099 210.x.231.147.53 > 131.x.x.86.53: SF
2078088031:2078088031(0) win 1028 (ttl 28, id 39426)
01:22:47.971470 210.x.231.147.53 > 131.x.x.109.53: SF
2078088031:2078088031(0) win 1028 (ttl 28, id 39426)
01:22:48.069170 210.x.231.147.53 > 131.x.x.114.53: SF
2078088031:2078088031(0) win 1028 (ttl 28, id 39426)
01:22:49.109343 210.x.231.147.53 > 131.x.x.166.53: SF
1781538967:1781538967(0) win 1028 (ttl 28, id 39426)
```

8.1 Source of trace

My network.

8.2. Detect was generated by:

Windump filter.

8.3 Probability the source address was spoofed

Unlikely. This scan requires a response from the victim machine in order to be successful.

8.4 Description of attack:

OS fingerprinting, possibly also intending to get DNS information.

8.5 Attack mechanism:

The SYN/FIN flag combination provides operating system information for the victim machines, as specific operating systems respond in different ways to such combinations. Some OS's (for example, Windows), will respond to SYN/FIN as if to a proper SYN packet, by replying with a SYN/ACK if the port is open. In this way, the technique used here can act as both an OS fingerprinting scan as well as a standard scan of port 53, possibly resulting in DNS information about the victim network, in addition to information about which IP addresses are in use, and what operating systems are in use at these addresses. The reuse of packet ID and sequence numbers further points to packets crafted by a scanning tool of some sort. It is possible that there's no interest in DNS information here, and that the choice of port 53 (source port and destination port) is merely an additional attempt to slip this OS fingerprinting attempt past IDS's and firewalls by disguising it as a DNS request. A successful zone transfer would probably be welcomed by the attacker, but that is probably not the primary intent here.

8.6 Correlations:

Illegal flag combinations are discussed on p. 54 of the GIAC text for section 2.4, *Network-Based Intrusion Analysis* by Stephen Northcutt, at SANS SNAP 2000 in San Jose, May 2000. SYN/FIN's to port 53 are specifically mentioned at http://www.sans.org/y2k/051800.htm.

8.7 Evidence of active targeting:

No. The entire network was scanned.

8.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 2 [scan itself is not lethal, but may be preparation to a more targeted attack]

System Countermeasures = 2 [many systems scanned, apparently few have countermeasures to detect this type of scan]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+2) – (2+2)] = 0

8.9 Defensive recommendation:

Blocking this IP address at the border routers once the attack pattern was detected was a reasonable course of action. However, it would be more proactive to simply deny any packets with illegal TCP flag combinations.

8.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) normal DNS request
b) telnet scan

c) OS fingerprinting
d) Password-guessing attempt

Answer: c

**

Detect 9:

```
39     2000-06-14 03:11:10    2003102      TCP port probe
210.x.173.1        131.x.x.75        port=1524  1
```

9.1 Source of trace

My network.

9.2. Detect was generated by:

BlackICE host-based IDS. Format is: Severity (As calculated by BlackICE), Datestamp (GMT), BlackICE IssueID, BlackICE Issue Name, source IP, source domain (if available), victim IP, "parameters" including source port, number of iterations of this specific attack.

9.3 Probability the source address was spoofed

Unlikely. Unless this scan is simply intended to make people think that the source site has some compromised machines, the attack won't succeed unless the source hosts are able to receive replies from the victim machine.

9.4 Description of attack:

Attempt to locate or activate a previously-installed trojan.

9.5 Attack mechanism:

SYN packets are sent to a specific port used by a Unix-based distributed denial of service tool, Trin00. If a SYN/ACK is received in response, rather than a reset packet (as would happen if the victim existed but did not have this port open), then a connection can be completed and the trojan horse program listening on the victim computer can be activated and controlled.

9.6 Correlations:

Trin00 is discussed in many places, including Bugtraq at http://www.securityfocus.com/templates/archive.pike?list=1&date=1999-12-8&msg=Pine.GUL.4.20.9912071041410.9470-100000@red7.cac.washington.edu.

9.7 Evidence of active targeting:

Unlikely. Scans to this port from this same source IP were widespread on the rest of the network, and directed at machines running operating systems other than Unix.

9.8 Severity:

Criticality = 2 [attack not targeted, various systems scanned]

Lethality = 3 [scan itself relies on trojan having been previously installed, which it wasn't, however a distributed denial of service attack could have been launched if trojan had been found]

System Countermeasures = 2 [many systems scanned, apparently few have countermeasures to detect or block this type of scan]

Network Countermeasures = 2 [This IP blocked at border, but only after scan was observed]

Severity = [(2+3) - (2+2)] = 1

9.9 Defensive recommendation:

Blocking this IP address at the border routers once the attack pattern was discovered was a reasonable course of action. Alerting on SYN packets sent to well-known trojan ports might be worth considering as well.

9.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Windows Networking remote access
b) Mistyped destination
c) IP spoofing
d) Trojan scan

Answer: d

Detect 10:

```
Jun 14 10:32:06 [DELETED.12.103] 2033578: Jun 14 10:27:32 PDT:
%SEC-6-IPACCESSLO
GP: list 109 denied udp 212.x.119.15(953) -> 131.x.x.45(111), 1
packet
Jun 14 10:35:28 [DELETED.12.103] 2033591: Jun 14 10:30:53 PDT:
%SEC-6-IPACCESSLO
GP: list 109 denied udp 212.x.119.15(952) -> 131.x.x.45(111), 10
packets
Jun 14 10:36:01 [DELETED.12.103] 2033593: Jun 14 10:31:27 PDT:
%SEC-6-IPACCESSLO
GP: list 109 denied udp 212.x.119.15(953) -> 131.x.x.45(111), 4
Packets
```

10.1 Source of trace

My network.

10.2. Detect was generated by:

Cisco router Access Control List syslog to Unix server, fields are: timestamp, local host IP, packet number, timestamp and router ACL that logged packet, ACL filter action, protocol, source address and port, destination address and port, number of packets ACL action was taken on.

10.3 Probability the source address was spoofed

Unlikely. The source host needs to receive replies from the victim machine in order for the scan to succeed.

10.4 Description of attack:

Scan for open SUNRPC/Portmapper port, 111.

10.5 Attack mechanism:

UDP packets are sent to port 111, Portmapper. The intent is probably to discover which services are listening to which ports,

and then to attempt a known exploit of a vulnerable Remote Procedure Call service. UDP packets may have been used here in hopes that if this port was being blocked or monitored, only TCP packets were being examined.

10.6 Correlations:

The SANS "10 Most Critical Internet Security Threats" suggests simply blocking remote access to port 111, at http://www.sans.org/topten.htm under the heading "Perimeter Protection For An Added Layer of Defense In Depth".

10.7 Evidence of active targeting:

Yes. The scan was directed toward a system that was actually running Solaris and potentially vulnerable to such an exploit. This indicates prior knowledge, probably gleaned from a previous reconnaissance effort to determine the operating system in use on this host.

10.8 Severity:

Criticality = 3 [scan targeted at non-critical server]

Lethality = 2 [scan itself is non-lethal, but may be preparation for future targeted exploit]

System Countermeasures = 5 [fully patched OS, tcpwrappers in use]

Network Countermeasures = 4 [This IP previously blocked at router after a big upswing in SunRPC scans was observed]

Severity = [(3+2) – (5+4)] = -4

10.9 Defensive recommendation:

Blocking packets sent to this port at our border routers was a good choice here. Very few of our users have a legitimate reason to need to use remote procedure calls from outside our network. Those who do can be explicitly permitted on our access lists.

10.10 Multiple choice test question, write a question based on the trace and your analysis with your answer.

a) Trojan scan
b) Open relay probe
c) IP spoofing
d) RPC port scan

Answer: d