Intrusion Detection: 10 detects + analysis

Kimberly Engle

Detect 1

```
(snip)
May 17 01:24:24 Router_addr 114837: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3702) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.60(143), 1 packet
May 17 01:24:25 Router_addr 114838: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3219) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.57(139), 1 packet
May 17 01:24:26 Router_addr 114839: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3809) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.60(23), 1 packet
May 17 01:24:28 Router_addr 114840: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3823) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.60(53), 1 packet
May 17 01:24:30 Router_addr 114841: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3898) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.60(23), 1 packet
May 17 01:24:33 Router_addr 114843: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3507) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.59(53), 1 packet
May 17 01:24:34 Router_addr 114844: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4059) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(23), 1 packet
May 17 01:24:36 Router_addr 114845: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4067) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(53), 1 packet
May 17 01:24:38 Router_addr 114846: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4135) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(23), 1 packet
May 17 01:24:40 Router_addr 114847: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4218) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.62(143), 1 packet
May 17 01:24:42 Router_addr 114848: %SEC-6-IPACCESSLOGP: list 150 permitted tcp
200.42.24.154(4227) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.62(109), 1 packet
May 17 01:24:43 Router_addr 114849: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4317) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.62(143), 1 packet
May 17 01:24:45 Router_addr 114850: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4343) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.62(139), 1 packet
May 17 01:24:46 Router_addr 114851: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(3961) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(23), 1 packet
May 17 01:24:48 Router_addr 114852: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4007) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(53), 1 packet
May 17 01:24:51 Router_addr 114853: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4059) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(23), 1 packet
May 17 01:24:55 Router_addr 114854: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4595) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.62(53), 1 packet
May 17 01:24:56 Router_addr 114855: %SEC-6-IPACCESSLOGP: list 150 denied tcp
200.42.24.154(4067) (Vlan1000 xxxx.yyyy.zzzz) -> my.net.work.61(53), 1 packet
(snip)
```

Multiple ftp and telnet connection attempts appeared in the system logs also. Here's a small chunk of the relevant detect:

```
May 17 01:06:06 my.host.1 ftpd[2053]: connect from host024154.prima.com.ar
May 17 01:06:06 my.host.1 telnetd[3440]: connect from host024154.prima.com.ar
May 17 01:06:20 my.host.2 in.ftpd[16347]: connect from host024154.prima.com.ar
May 17 01:06:20 my.host.2 in.telnetd[16349]: connect from host024154.prima.com.ar
May 17 01:06:32 my.host.2 in.ftpd[16374]: connect from host024154.prima.com.ar
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL logs + system logs

Explanation of Fields:

Cisco ACL logs:

```
May 17 01:24:24 [timestamp] Router_addr 114837: %SEC-6-IPACCESSLOGP: list 150
[pattern matching ACL list specified was detected] denied [action taken]
tcp [transport protocol] 200.42.24.154(3702) [source IP and port]
(Vlan1000 xxxx.yyyy.zzzz) [Network] -> my.net.work.60(143) [destination IP and port],
1 packet
```

System log:

```
May 17 01:06:06 [timestamp] my.host.1 [destination host] ftpd[2053]: [service
and PID] connect from host024154.prima.com.ar [source host]
```

3. Probability address was spoofed: Very low, since the hacker would need the host to collect the information gleaned from the scan. This address was most like a "throw-away" machine, since the overt nature of the scan would likely tip off anyone (or everyone) that the host is compromised.

4. Description of Attack: Mscan-type attack (described in the SANS book 2.2 pg 261, but missing cgi-bin probes)- probably a script kiddie with a new toy. This is an obvious scan for services on well-known ports 21/tcp (ftp), 23/tcp (telnet), 53/tcp (DNS), 80/tcp (http), 109/tcp (POP2), 139/tcp (NETBIOS), 143/tcp (IMAP), 6000/tcp (Xwindows uses this among others), and 6667/tcp (popular IRC choice).

5. Attack mechanism: Looks like the attacker has a script that systematically (and overtly) probes specified popular services (with known exploits!) on a specified network, host by host. This is a reconnaissance attack. The hacker will review information obtained from this scan to (probably) attack specific services on specific hosts in this network at a later date, and from a different source machine (unless the hacker is really dumb).

6. Correlations: The IP address corresponds to prima.com.ar (with very limited information in the whois database), but is most likely an ISP in Argentina. A user at this site used the account to send spam. (From http://easyweb.easynet.co.uk/~gcaselton/spam/kills.html:
"Dear Sir: We have received you complaint regarding unsolicited E-mail from someone using our services. Be assured that the appropriate actions (Warning, suspension or deletion) have been taken to resolve this issue. We apologized for any inconvenience that this may have caused you or your company. Best Regards - Facundo Maldonado Supervisor General.")

NASA's Incident Response Center (NASIRC) reported increases in scans from Argentina, so this may have been part of the same group. (NASIRC Bulletin B-00-40 (May 11, 2000):
"There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.")

7. Evidence of active targeting: This is a scan of specific services on all live hosts in my network.

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 3 (mix of machine types and functions)
lethality = 3 (recon scan)
system CM = 5 (OSs patched and up-to-date)
network CM = 3 (some packets got through for running services, but most are blocked)

severity = -2

***9. Defensive recommendations**:* Defines are good. The router blocked connections to most tcp ports listed, and the permitted ones are tcp wrapped and/or logged. Also, host patches are up-to-date.

10. Multiple choice question:

The intent of this attack is

a. denial-of-service
b. to scan for DNS zone transfer
c. reconnaissance
d. a direct attempt to gain root access

Detect 2

```
Mar 25 18:01:28 Router_addr 73423: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(26658) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.16.2(5232), 1 packet
Mar 25 18:01:30 Router_addr 73424: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(26769) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.17.1(5232), 1 packet
Mar 25 18:01:31 Router_addr 73425: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(27006) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.17.238(5232), 1 packet
Mar 25 18:01:32 Router_addr 73426: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(27025) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.18.2(5232), 1 packet
Mar 25 18:01:34 Router_addr 73427: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(27142) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.19.1(5232), 1 packet
Mar 25 18:08:45 Router_addr  39024: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(6069) (Fddi1/0 aa00.0400.fb3f) -> 128.183.240.2(5232), 1 packet
Mar 26 03:14:11 Router_addr 73543: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17276) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.16.2(5232), 1 packet
Mar 26 03:14:13 Router_addr 73544: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17403) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.17.1(5232), 1 packet
Mar 26 03:14:14 Router_addr 73545: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17651) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.17.249(5232), 1 packet
Mar 26 03:14:15 Router_addr 73546: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17659) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.18.2(5232), 1 packet
Mar 26 03:14:17 Router_addr 73547: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17788) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.19.1(5232), 1 packet
Mar 26 03:14:18 Router_addr 73548: %SEC-6-IPACCESSLOGP: list 100 denied tcp
171.64.100.16(17975) (Vlan1000 xxxx.yyyy.zzzz) -> 128.183.19.204(5232), 1 packet
```

1. Source of trace: My network

2. Detect was generated by: Cisco ACL log output

```
Mar 25 18:01:28 [timestamp] Router_addr 73423: %SEC-6-IPACCESSLOGP: list 100
 [pattern matching ACL list specified was detected] denied [action taken]
tcp [transport protocol] 171.64.100.16(26658)  [source IP and port]
(Vlan1000 xxxx.yyyy.zzzz)-> my.network.a.2(5232) [destination IP and port], 1 packet
```

3. Probability address was spoofed: Low, since the information obtained from the attack must be collected later by the hacker. I'd be willing to bet the host 171.64.100.16 (mahler.Stanford.EDU) is a compromised university computer.

4. Description of attack: This is most likely a probe for SGIs, since port 5232/tcp is used for distributed graphics by SGI.

5. Attack mechanism: The hacker is looking for SGI computers by checking for a specifically SGI service listening on port 5232, probably so he/she/they can return at a later date (from a different host probably) and try to exploit some IRIX vulnerability. For example, once the hacker obtains a list of possible SGIs, they might begin scanning port 1/tcp to check for tcpmux, which is enabled by default by IRIX. Then they can begin telneting to the machines to check for unpassworded accounts (like "guest", "lp", etc.), which also are included by default by the IRIX OS. (The ones and twos in the final octet of many destination IP addresses may indicate they are looking for network equipment (by probing perhaps for some unregistered vendor-specific port), which is often given low numbers in the final octet.)

6. Correlations: The "Hunting SGIs" probe was described at SANS2000 (San Jose) and is in book 2.4 page 267. The warning concerning the scan of port 1/tcp and unpassworded IRIX accounts can be found in the CERT Incident Note IN-98.01.

7. Evidence of active targeting: This was a scan of specific hosts, looking for SGI systems in particular.

8. Severity: (Criticality + Lethality) - (System + Network Countermeasures)

criticality = 2 (Unix desktops)
lethality = 2 (recon)
system CM = 5 (SGIs patched and up-to-date)
network CM = 4 (blocked packets at the router)

severity = -5

***9. Defensive recommendation:*:** Defenses are fine. None of the machines targeted are SGIs (so the hacker does not seem to have previous knowledge of our network), and all packets to port 5232/tcp were denied at the router. To be on the safe side though, I'd have all our SGI systems double-checked for unpassworded accounts, and keep a close eye out for probes to port 1/tcp, and/or be sure port 1/tcp is blocked at the router and/or firewall. It would also be a good to make sure all the latest IRIX patches have been installed, just in case...

10. Multiple choice question:

This trace is an example of a

a. search for SGI systems
b. search for trojan software
c. Land Attack
d. Denial of Service attack

Detect 3

```
May 22 05:48:34 Router_addr 122890: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1317) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:49:58 Router_addr 122891: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1458) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:05 Router_addr 122893: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1476) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:45 Router_addr 122896: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1495) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:48 Router_addr 122897: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1498) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:50 Router_addr 122898: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1503) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:52 Router_addr 122899: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1500) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:55 Router_addr 122900: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1505) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
May 22 05:50:59 Router_addr 122901: %SEC-6-IPACCESSLOGP: list 120 denied tcp
192.168.20.17(1507) (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80), 1 packet
(snip)
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL log

May 22 05:48:34 [timestamp] Router_addr 122890: %SEC-6-IPACCESSLOGP: list 120 [pattern matching ACL list specified was detected] denied [action] tcp [protocol] 192.168.20.17(1317) [source IP and port] (Vlan1000 xxxx.yyyy.zzzz) -> my.web.server(80) [destination IP and port], 1 packet

3. Probability the source address was spoofed: Most definitely, since 192.168.x.x addressed are reserved and not routed on the internet.

4. Description of attack: For about 30 minutes, the attacker uses a spoofed source address to send packets at short intervals (as few as 3 seconds) to the http port of one of our web servers. Since the packets are being sent to one machine only- a known web server, and the source address is spoofed, I'd bet this is a denial-of-service attack. I'd have to look at the actual tcp packets to be certain. (I sure wish I had access to tcpdump logs of this!)

5. Attack mechanism: Like telnet and other tcp services, http uses the tcp 3-way handshake for connections. The web server responds to the client's initial SYN with a SYN-ACK. The web server will then wait for an ACK from the client before establishing the connection. Since the source/client IP is unroutable, the http server will sit and wait for that final ACK which it will never receive. When some finite number of "waiting" connections is exceeded, the http server will no longer be able to respond to legitimate requests, and therefore a denial-of-service takes place. I could think of more benign explanations if only the source IP was not an unroutable address (and we do not use 192.168 addresses) and the attempts occur in rather short time intervals. The source ports increasing, but by only a few with each attempt, probably indicates there is little else running on the source system.

6. Correlations: TCP SYN flooding of a specific port/service was discussed at SANS2000 (San Jose) and in the accompanying text 2.2 page 150.

7. Evidence of active targeting: The attack targeted a known web server (which serves an extremely popular page) and only that host.

8. Severity: (Criticality + Lethality) + (System + Network Countermeasures)

criticality = 4 (web server)
lethality = 4 (denial of service)
system CM = 5 (OSs patched and up-to-date)
network CM = 4 (packets denied at router)

severity = -1

9. Defensive recommendation: Defensives are fine, because unroutable source addresses are denied by the router. However the attacker could try again, this time using a "legitimate" but spoofed address. A stateful firewall will be able to watch for and block inbound SYNs from spoofed addressed, so be sure the firewall admins are doing just that.

10. Multiple choice question:

This trace best describes a:

a. network mapping expedition
b. normal http traffic

c. probe for web servers
d. tcp SYN flooding attack

Detect 4

```
Jun  6 13:55:49 Router_addr 147582: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1149) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.23.74(23), 1 packet
Jun  6 13:55:59 Router_addr 147584: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1273) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.23.91(23), 1 packet
Jun  6 13:56:10 Router_addr 147586: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1479) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.98(23), 1 packet
Jun  6 13:56:13 Router_addr 147587: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1523) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.18(23), 1 packet
Jun  6 13:56:29 Router_addr 147588: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1790) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.16(23), 1 packet
Jun  6 13:57:02 Router_addr 147591: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(2491) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.20.55(23), 1 packet
Jun  6 13:57:07 Router_addr 147592: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(2604) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.78(23), 1 packet
Jun  6 13:57:17 Router_addr 147593: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(2777) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.47(23), 1 packet
Jun  6 13:57:27 Router_addr 147595: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(2974) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.23.99(23), 1 packet
Jun  6 13:57:29 Router_addr 147596: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(3032) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.20.95(23), 1 packet
(snip)
Jun  6 13:58:08 Router_addr 147598: %SEC-6-IPACCESSLOGP: list 150 denied tcp
210.110.247.244(1479) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.98(23), 2 packets
(snip)
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL log

```
Jun  6 13:55:49 [timestamp] Router_addr 147582: %SEC-6-IPACCESSLOGP: list 150
[pattern matching ACL list specified was detected] denied [action taken]
tcp [protocol] 210.110.247.244(1149) [source IP and port] (Vlan1000
xxxx.yyyy.zzzz) -> my.network.23.74(23) [destination IP and port], 1 packet
```

3. Probability source address was spoofed: Low. The address space 210.110.128.0 - 210.110.255.255 belongs to KREONET, and ISP in Korea. Why bother spoofing? Besides, the hacker must use his/her own true IP address to get responses from the scanned hosts.

4. Description of attack: Scan of telnet port only. They could use the responses to determine if telnet is open and do some OS determination. Could be a QueSO scan. (The default port scan for QueSO is 80, so the attacker would have modified thw code to include port 23.)

5. Attack mechanism: The attacker sends legitimate tcp packets with the SYN flag set to the target. If the target replies with a SYN-ACK, then he/she can assume telnet is listening on that port. Then the attacker can send carefully-crafted impossible packets (with different flags set like SYN-ACK with ACK number set to zero, PUSH only, FIN only, etc) to the host, and the host's response will indicate its OS. If I had access to tcpdump output of these packets, I could example the flags for impossible combinations, and determine if the hacker is indeed attempting OS determination or just looking for open telnet ports.

6. Correlations: QueSO is described in CERT IN-98.04 and was discussed by Vicki Irwin at SANS (book 2.2 page 170).

7. Evidence of active targeting: Yes, this attack was directed at my network, and each host was probed at least twice. (But I only included one duplicate example to save space.)

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 3 (mix of machine types and functions)
lethality = 3 (recon)
system CM = 5 (OSs patched and up-to-date)
network CM = 4 (packets were denied by the router)

severity = -3

9. Defensive recommendations: Defenses are fine, as the packets were denied access by the router.

10. Multiple choice question:

One possible explanation for this trace could be

a. a search for mail servers

b. normal inbound ssh traffic
c. a Teardrop attack
d. OS determination

Detect 5

```
Mar 23 11:47:44 Router_addr 72075: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1189) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 1 packet
Mar 23 11:49:17 Router_addr 72077: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1208) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 1 packet
Mar 23 11:53:34 Router_addr 72085: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1189) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 3 packets
Mar 23 11:54:34 Router_addr 72086: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1208) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 3 packets
Mar 24 11:28:01 Router_addr 72778: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1319) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 1 packet
Mar 24 11:33:10 Router_addr 72784: %SEC-6-IPACCESSLOGP: list 100 denied tcp
129.93.34.67(1319) (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070), 3 packets

Apr 10 10:25:57 Router_addr 45575: %SEC-6-IPACCESSLOGP: list 130 denied tcp
192.168.10.11(1703) (Fddi1/0 xxxx.yyyy.zzzz) -> my.host.two(7070), 1 packet
Apr 10 10:31:42 Router_addr 45579: %SEC-6-IPACCESSLOGP: list 130 denied tcp
192.168.10.11(1703) (Fddi1/0 xxxx.yyyy.zzzz) -> my.host.two(7070), 3 packets
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL log

Mar 23 11:47:44 [timestamp] Router_addr 72075: %SEC-6-IPACCESSLOGP: list 100 [pattern matching ACL list specified was detected] denied [action taken] tcp [protocol] 129.93.34.67(1189) [source IP and port] (Vlan1000 xxxx.yyyy.zzzz) -> my.host.one(7070) [destination IP and port], 1 packet

3. Probability source address was spoofed: In the March 23 detect, the source address was most likely not spoofed, as it belongs to the University of Nebraska- Lincoln (though the host could be compromised). The source host in the April 10 detect is definitely forged since the address is unroutable.

4. Description of attack: To be honest, I'm not sure. I would not have suspected any malicious activity, but for the 192.168 source address. Port 7070/tcp is assigned to ARCP, "asynchronous remote copy program."

(www.nas.nasa.gov/Groups/WAN/documents/arcp.html#HDR2.1). I was not able to find any references to ARCP in any CVE, CERT, or NASIRC (NASA Incident Response Center) alert. I did learn more about port 7070- it's the unregistered default port for RealAudio.

A further search on port 7070 revealed a CVE candidate for a DOS by sending malformed input to this RealNetworks RealServer port. Since the source address ws forged for the April 10 attack, and "my.host.two" is a major web server, I'd have to put my money on this DOS. (I *really* wish I had some tcpdump output for this trace!)

5. Attack mechanism: As mentioned above, the attacker sends malformed packets to the RealServer port in the hopes of causing a denial-of-service.

I am not exactly sure this is what's happening, but it's possible. (Perhaps someone is trying to access some audio streaming. My.host.two is running a RealAudio server.)

The reason the port 7070 detect from March 23 was included is because I determined my.host.one belongs to the *same person* (out of several hundred people in my network space) as my.host.two. In both cases, port 7070 was the only port examined by the source IP, and during each time period the source address probed only these hosts. Very odd indeed! I'm almost inclined to think the attack was directed against the person and not the host! (I talked to the machines' owner and she does not know anyone at the UN-L address nor anything much about RealServer.) To add more to the story, my.host.two had a user account compromised a month or so earlier. There's just too many coincidences here for me to write off this detect. I guess I'll be scratching my head on this one for a while, and keeping an eye out for more port 7070 probes.

6. Correlations: The DOS scenario is decribed in CAN-2000-0272. The bugtraq reference contained therein says "The Exploit: It will take down the RealServer causing it to stop all streaming media brodcasts, making it non-functional, (until Reboot)."

7. Evidence of active targeting: Yes, this attack was directed against two specific hosts, belonging to the same person. (So perhaps it was the person being attacked!)

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 4 (my.host.two is a major web server)
lethality = 2 (who cares if audio doesn't work for a bit)
system CM = 5 (OSs patched and up-to-date)
network CM = 4 (packets were blocked)

severity = -3

9. Defensive recommendations: Defenses are fine, as the packets (and unroutable addresses) were denied access by the router. Also, just in case it was the DOS attack, neither machine is running RealServer.

]

10. Multiple choice question:

This attack could be

a. against an unregistered service
b. a back door search
c. network mapping
d. the Ping of Death

Detect 6

```
Apr 14 10:19:31 Router_addr 47464: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 1 packet
Apr 14 10:24:55 Router_addr 47467: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 79 packets
Apr 14 10:29:55 Router_addr 47469: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 35 packets
Apr 14 10:34:55 Router_addr 47471: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 18 packets
Apr 14 10:39:55 Router_addr 47473: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 6 packets
Apr 14 10:44:55 Router_addr 47475: %SEC-6-IPACCESSLOGDP: list 130 denied icmp
192.168.10.11 (Fddi1/0 xxxx.yyyy.zzzz) -> my.web.server (3/1), 1 packet
```

1. Source of trace: My network

2. Detect was generated by: Cisco ACL log

Apr 14 10:19:31 [timestamp] Router_addr 47464: %SEC-6-IPACCESSLOGDP: list 130 [pattern matching ACL list specified was detected] denied [action taken] icmp [protocol] 192.168.10.11 [source IP] (Fddi1/0 xxxx.yyyy.zzzz) [network] -> my.web.server [destination IP] (3/1) [host unreachable], 1 packet

3. Probability source address was spoofed: Definitely, since 192.168.x.x addresses are unroutable on the internet.

4. Description of attack: Looks very much like a popular icmp DOS. If they were just trying to determine the system type and/or architecture of the web server by sending unexpected packets (stealth scanning- see Correlations section), then the source address would exist so the server response(s) could collected.

5. Attack mechanism: The attacker is sending "host unreachable" packets from a spoofed address to one of our main web servers. This must be malicious, as the source address is unroutable and outgoing icmp, such as ping requests, are blocked (but not logged). So my web server obviously could not be initiating the icmp exchange. This must be a script generating the packets, as the web server received them *exactly* every 5 minutes.

6. Correlations: CVE-1999-0214. Description- Denial of service by sending forged ICMP unreachable packets.

7. Evidence of active targeting: Yes, the attack was against one major web server.

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 4 (web server)
lethality = 4 (denial of service)
system CM = 5 (OSs patched and up-to-date)
network CM = 4 (packets blocked at router)

severity = -1

9. Defensive recommendations: Defenses are fine, as icmp packets (and unroutable addresses) were denied access by the router.

10. Multiple choice question:

This trace shows

a. an nmap scan in action
b. host mapping
c. a DOS attempt
d. someone accessing web pages

Detect 7

```
Jun  9 10:25:13 Router_addr 156860: %SEC-6-IPACCESSLOGP: list 100 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.a.31(53), 1 packet
Jun  9 10:25:16 Router_addr 156863: %SEC-6-IPACCESSLOGP: list 100 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.a.214(53), 1 packet
Jun  9 10:25:19 Router_addr 156864: %SEC-6-IPACCESSLOGP: list 100 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.b.79(53), 1 packet
Jun  9 10:25:33 Router_addr 156866: %SEC-6-IPACCESSLOGP: list 100 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.a.40(53), 1 packet
Jun  9 10:25:34 Router_addr 156867: %SEC-6-IPACCESSLOGP: list 150 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.e.52(53), 1 packet
Jun  9 10:25:34 Router_addr 156868: %SEC-6-IPACCESSLOGP: list 150 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.e.102(53), 1 packet
Jun  9 10:25:36 Router_addr 156869: %SEC-6-IPACCESSLOGP: list 150 denied tcp
195.76.27.44(65535) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.e.152(53), 1 packet
```

1. Source of trace: My network

2. Detect was generated by: Cisco ACL log

Jun 9 10:25:13 [timestamp] Router_addr 156860: %SEC-6-IPACCESSLOGP: list 100
[pattern matching ACL list specified was detected] denied[action taken]
tcp [protocol] 195.76.27.44(65535) [source IP and port]
(Vlan1000 xxxx.yyyy.zzzz) -> my.network.a.31(53) [destination IP and port],
1 packet

3. Probability address was spoofed: Low. The IP address belongs to "SSC sistemas de Informacion" in Spain (according to www.ripe.net), and needs to obtain information from the target.

4. Description of Attack: This is an attempt to find DNSs in my network and then probably attempt to do zone transfers. The signature source "port 0" (since port 66635 = port 0), is present.

5. Attack mechanism: The attacker is attempting to find DNSs by probing port 53 on my network machines. If a response is received the next step would be to attempt a zone transfer. Note signature "source port 0", since port 65535 is port 0. Since DNSs of networks can be obtained pretty easily with "whois" and other resources, this is probably a very novice hacker playing with a new script, since none of the machines targeted are DNSs. Or maybe they are looking for rogue or slave DNSs on the network.

6. Correlations: Zone transfers and DNS scans are described everywhere, including (at least) SANS book 2.4 pg 290 (including the "port 0" signature).

7. Evidence of active targeting: They look to be examining many/all machines in my network for DNS servers. (Too bad we don't log these attempts to all machine).

8. Severity: (criticality + lethality) - (system + network countermeasures)

> criticality = 3 (mix of machine types and functions)
> lethality = 4 (could possibly find a DNS and do a zone transfer)
> system CM = 5 (OSs patched and up-to-date)
> network CM = 4 (port 53 is blocked at the router)

severity = -2

9. Defensive recommendations: Defines are good. The router blocks connections to port 53 , and none of the machines listed are DNSs.

10. Multiple choice question:

This trace is an example of a

> a. zone transfer attempt
> b. denial of service
> c. socks scan
> d. wrong number

Detect 8

```
Mar 21 14:45:12Router_addr 70822: %SEC-6-IPACCESSLOGP: list 150 denied udp
208.247.248.5(3061) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.23.82(137), 2 packets
Mar 21 14:46:12Router_addr 70823: %SEC-6-IPACCESSLOGP: list 150 denied udp
208.247.248.5(3092) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.22.72(137), 1 packet
Mar 21 14:50:12Router_addr 70827: %SEC-6-IPACCESSLOGP: list 150 denied udp
208.247.248.5(3299) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.20.92(137), 1 packet
(snip)
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL logs

Mar 21 14:45:12 [timestamp] Router_addr 70822: %SEC-6-IPACCESSLOGP: list 150
 [pattern matching ACL list specified was detected] denied [action taken]
udp [transport protocol] 208.247.248.5(3061) [source IP and port]
(Vlan1000 xxxx.yyyy.zzzz) [Network] -> my.network.23.82(137) [destination IP
and port], 2 packets

3. Probability address was spoofed: Low, since this address belongs to the ISP "Aero Internet Service" based in northwestern Illinois (which is makes it incredibly unlikely this service is/was used by anyone on my network. Also the hacker must obtain information from the targets.

4. Description of Attack: This is a (good ole) scan for the Netbios Name Service.

5. Attack mechanism: The hacker is hoping to get a response from Netbios, thus telling him/her, for example if the host is a Windows machine. Lots of other useful information can be obtained also.

This could also be a mistake... One of the people in my lab could have taken their Windows laptop off to Illinois and neglected to change the WINS address configuration before borrowing someone's ISP account. However no login attempts from this ISP appear in the system logs.

Since the source port is not 137, this could indicate that a samba system is running.

6. Correlations: Netbios-ns scans are very common (and indeed my router logs are replete with them), and they were discussed in some detail at SANS. CERT Incident Note IN-98.04 discusses how a WindowsNT machine responds to a "queso" scan of port 137. The samba possibility is discussed in SANS 2.4 pg 193.)

7. Evidence of active targeting: Yes, the attack is directed against specific hosts in my network.

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 3 (mix of machine types and functions)
lethality = 3 (most machines hit were not PCs)
system CM = 4 (OSs patched and up-to-date)
network CM = 4 (blocked)

severity = -2

9. Defensive recommendations: Defines are fine. The router blocked udp connections to the network. Each PC should be checked to make sure those that do not need or use Netbios NS should have the service turned off. (As it's turned on by default.)

10. Multiple choice question:

The best description of this attack is

a. a null session
b. Netbios NS scan
c. Windows IIS
d. a Back Oriface scan

Detect 9

```
Mar 31 19:52:29 Router_addr 76334: %SEC-6-IPACCESSLOGP: list 100 denied tcp
203.85.30.129(1348) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.17.102(98), 1 packet
Mar 31 19:52:32 Router_addr 76335: %SEC-6-IPACCESSLOGP: list 100 denied tcp
203.85.30.129(4999) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.16.34(98), 1 packet
Mar 31 19:58:11 Router_addr 76336: %SEC-6-IPACCESSLOGP: list 100 denied tcp
203.85.30.129(1348) (Vlan1000 xxxx.yyyy.zzzz) -> my.network.17.102(98), 1 packet
(snip)
```

1. Source of trace: my network

2. Detect was generated by: Cisco ACL log

Mar 31 19:52:29 [timestamp] Router_addr 76334: %SEC-6-IPACCESSLOGP: list 100
[pattern matching ACL list specified was detected] denied [action taken]
tcp [protocol] 203.85.30.129(1348) [source IP and port] (Vlan1000
xxxx.yyyy.zzzz) [Network] -> my.network.17.102(98) [destination IP and port],
1 packet

3. Probability source address was spoofed: Low, as the hacker needs the scan information returned to him/her. This IP belongs to "OLS Co Ltd" in Hong Kong (according to www.apnic.net).

4. Description of attack: The hacker is most likely probing for for the Linux administration GUI "Linuxconf." I doubt this is a probe for TAC news... (The Stuztzman report on the GIAC site refers to scans to port 98 and TAC news. See www.sans.org/y2k/0114stutzman.htm.)

5. Attack mechanism: If the attacker finds a host running linuxconf, then that service could be exploited with a buffer overflow and thereby providing root access (since the program runs as root).

6. Correlations: The linuxconf buffer overflow exploit is described in CAN-2000-0017.

7. Evidence of active targeting: This attack was directed against various hosts in my network.

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 3 (mix of machine types and functions)
lethality = 5 (root access could be obtained)
system CM = 4 (OSs patched and up-to-date)
network CM = 4 (packets denied at router)

severity = 0

9. Defensive recommendations: Defenses are fine, as the packets were blocked at the router.

10. Multiple choice question:

This attacker is trying to

a. find a back door
b. see if Microsoft NetMeeting is running
c. find hosts with linuxconf
d. use "talk"

Detect 10

```
pc004456.greek.uidaho.edu - - [12/Apr/2000:13:33:48 -0400] "GET /cgi-
bin/phf?Qname=hacker%0acat%20/etc/passwd HTTP/1.0" 200 631
pc004456.greek.uidaho.edu - - [12/Apr/2000:13:35:13 -0400] "GET /cgi-
bin/phf?Qname=cat%20/etc/passwd HTTP/1.0" 200 85
```

1. Source of trace: my network

2. Detect was generated by: http access log

```
pc004456.greek.uidaho.edu - - [12/Apr/2000:13:33:48 -0400] "GET /cgi-
bin/phf?Qname=hacker%0acat%20/etc/passwd HTTP/1.0" 200 631
```

format: source host - - timestamp "action attempted"

3. Probability source address was spoofed: Low, since the address belongs to the University of Idaho, and especially because the hacker is trying to obtain information from the target web server.

4. Description of attack: The attacker is attempting to exploit the age-old phf hole to obtain the password file from the web server, then later will try to crack the passwords and then log in as a legitimate user. From there he/she could determine if a local exploit exists for a user to obtain root, then go on from there.

5. Attack mechanism: The attacker tries to send a buffer overflow containing the command "cat /etc/passwd" to the PHF cgi-bin script to obtain a copy of the web server's password file. Because the password file is world-readable, if the PHF hole is open, the password file will be displayed in the browser.

6. Correlations: This one has been around for years now, and was discussed at SANS (book 2.4 page 55, 162). CERT 96.06.cgi even has some example code if you want to try it for yourself.

7. Evidence of active targeting: Yes, the hacker went right one of our main web servers, and tried the "cat /etc/passwd" command twice, just to be sure. :-)

8. Severity: (criticality + lethality) - (system + network countermeasures)

criticality = 4 (web server)
lethality = 1 (this exploit is so old I bet no one has it open)
system CM = 5 (OSs patched and up-to-date)
network CM = 4

severity = -4

9. Defensive recommendations: Defenses are fine, as this hole was closed a long time ago. In fact, we have a honeypot set up, so we get an alarm message each time someone tries to the phf exploit, and they get a fake password file. Heh heh heh...

10. Multiple choice question:

This is an example of

a. normal web traffic
b. someone downloading info from a web page
c. the target web server being used as a proxy
d. an attempt to exploit the buffer overflow in phf

Detect 10 prime (for your amusement)

Last winter someone attempted to exploit the (closed) PHF hole on our web servers. Each attempt is recorded, the sysadms are notified via email, and the alarm script output is sent to the local incident response team. If someone tries to finger our machines, the attempts are also logged and they receive notification that our authorities are aware of their attempts to access our systems. (Sorry I don't still have access to these records.)

After a probe of both types described above, we received email from the party we back-fingered, who said he was just "testing our security" and being a "good net citizen." This guy was from Germany, if I recall correctly. We ignored his email of course.

Then just recently he contacted us again, asking for a favor in return since he informed us of our "PHF hole". I thought you might like to read his message. Can you believe his audacity? (Names sanitized to protect the guilty.)

Date: Sun, 21 May 2000 13:57:07 -0400 (EDT)
From: Frank [last_name] <hacker@his.network>
To: admin@my.network
Subject: for information..

Hi Admin,
i got a little question...
If you still remember me, I'am Frank (who reports
you the fake-phf before some month ago)..
Well.. Can i get an user shell at your machine for 1 bg
(ircii+screen) process please?
Well..... you can trust me.. and its just a question.
If not.. it isnt so importan..
If yes.. would be just cool :)
Thank you..
Nickname (Frank [last_name])

I responded (to "admin" only!!), just to give my colleagues a little laugh:

Hi Frank,

Ah, yes we remember you. And thanks again for pointing out the phf "hole." We had not been aware of it.

Since you have been so kind to us in the past, we'd be happy to give you a shell account on [hostname]. Just promise you won't be using IRC 24 hours a day, as [hostname] is one of our main web servers. Please tell us your desired account name and which type of shell you'd like, and we'll get right on it. Typically we provide each of our users with a 200MB home directory. If you'll need more, let us know and we can increase the quota a bit.

Once again, thank for all your help.

Kim, for the system team