********** GCIA Certification **********

Ten Detects with Analysis

Patrick Fahy

6/15/00

Detect 1

```
05/28/00 12:53:10.224408 www.yaleclub.or.kr.0 > workstation1.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:10.325599 www.yaleclub.or.kr.0 > workstation2.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:10.571267 www.yaleclub.or.kr.0 > mailserver.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:10.902967 www.yaleclub.or.kr.0 > workstation3.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:10.906450 www.yaleclub.or.kr.0 > linux1.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.000934 www.yaleclub.or.kr.0 > windowz1.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.248024 www.yaleclub.or.kr.0 > workstation4.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.423942 www.yaleclub.or.kr.0 > workstation5.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.525135 www.yaleclub.or.kr.0 > mailserver2.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.583547 www.yaleclub.or.kr.0 > workstation7.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.585658 www.yaleclub.or.kr.0 > unixlogger.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.864510 www.yaleclub.or.kr.0 > rcomms.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:11.971107 www.yaleclub.or.kr.0 > unix2.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:12.063146 www.yaleclub.or.kr.0 > unix3.pop-2: SF
491126784:491126784(0) win 512
05/28/00 12:53:12.104985 www.yaleclub.or.kr.0 > unix4.pop-2: SF
491126784:491126784(0) win 512
```

Name: www.yaleclub.or.kr
[whois.arin.net]
Address: **210.118.8.50**
Asia Pacific Network Information Center (APNIC)
These addresses have been further assigned to Asia-Pacific users.
inetnum: 210.118.0.0 - 210.118.31.255
netname: ELIMNET
country: KOREA
remarks: ISP in Korea
source: APNIC

1. **Source of trace:**

   a. My network

2. **Detect was generated by:**

   a. Shadow IDS

b. Explanation of fields

```
05/28/00 12:53:12.104985 [timestamp] www.yaleclub.or.kr.0 [source IP
address.port]> unix4.pop-2 [destination IP address.port]: SF [flags]
491126784:491126784(0) [beginning sequence # : ending sequence # (data
bytes)] win 512 [window size]
```

3. Probability that the source address was spoofed:

a. Low. IP address range is registered to APNIC. Further investigation revealed that the source IP address may have originated from an ISP in Seoul, South Korea.

4. Description of the attack:

a. The attacker scans the network looking for vulnerable systems running pop-2 services. The attacker is seeking to exploit flaws such as buffer overflow vulnerabilities to gain instant root-level access.

5. Attack mechanism:

a. The attacker uses an impossible flag combination to probe machines for listening pop-2 servers on port 109. Scanning with the SYN-FIN bits set sometimes will elude security systems filtering on SYN only. Buffer overflow vulnerabilities could be exploited. For example, if the USER command is followed by an argument of over 1000 characters, the input buffer will be overflowed, and data from the argument will be passed to the system to be executed at the privilege level of the resident mail server program.

In this trace, the packets were custom built due to the fact that the SYN and FIN flags are never set simultaneously in normal TCP connections. Notice that the sequence numbers and source ports are static and never change as the attacker scans the network. Another good indication that these packets were crafted is the use of source port zero.

6. Correlations:

a. This attack was described in detail during the intrusion detection and packet filtering lecture at SANS2000 in San Jose on May 9th. Also, references can be found on page 114 of the 2.2 student guide and page 168 of 2.4/2.5..

b. CVE-1999-0006
Buffer overflow in POP servers based on BSD/Qualcomm's
qpopper allows remote attackers to gain root access using a
long PASS command.

CVE-1999-0920
Buffer overflow in the pop-2d POP daemon in the IMAP package allows remote attackers to gain privileges via the FOLD command.

7. Evidence of active targeting:

a. General scanning. Attacker is targeting many hosts and servers on the network.

8. Severity:

a. (Criticality of target + Lethality of attack) - (System + Net Countermeasures) = Severity

b. (4 + 5) - (5 + 2) = 2

9. Defense recommendations:

a. Router defenses were not sufficient to block this attack. Recommend that router ACLs be updated to block all unused ports. Additionally, firewall purchase and deployment is recommended. NMAP was launched as a confidence test against the network to ensure that all POP-2 services were disabled. Test was negative. All POP-2 services were found to be disabled and host based defenses were fine.

10. Multiple choice question:

a. This trace is an example of?

A) SYN flood
B) Source routing
C) Christmas tree scan
D) SYN-FIN-SourcePort-0 scan

b. Answer: D

Detect 2

```
05/30/00 19:59:35.872594 dialup2-110.home.se.2666 > windowz8.imap2: S
111:111(0) win 0
05/30/00 19:59:35.873656 dialup2-110.home.se.2666 > mailserver2.imap2:
S 111:111(0) win 0
05/30/00 19:59:35.874267 dialup2-110.home.se.2666 > unixlogger.imap2:
S 111:111(0) win 0
05/30/00 19:59:35.880651 dialup2-110.home.se.2666 > windowz2.imap2: S
111:111(0) win 0
05/30/00 19:59:35.881415 dialup2-110.home.se.2666 > linux2.imap2: S
111:111(0) win 0
05/30/00 19:59:35.882253 dialup2-110.home.se.2666 > windowz6.imap2: S
111:111(0) win 0
05/30/00 19:59:35.890781 dialup2-110.home.se.2666 > rcomms.imap2: S
111:111(0) win 0
05/30/00 19:59:35.893057 dialup2-110.home.se.2666 > unix3.imap2: S
111:111(0) win 0
05/30/00 19:59:35.894322 dialup2-110.home.se.2666 > unix4.imap2: S
111:111(0) win 0
05/30/00 19:59:35.898914 dialup2-110.home.se.2666 > windowz7.imap2: S
111:111(0) win 0
06/03/00 19:04:45.553656 d212-151-235-114.swipnet.se.2666 >
unix3.imap2: S 111:111(0) win 0
06/03/00 19:04:45.723739 d212-151-235-114.swipnet.se.2666 >
mailserver.imap2: S 111:111(0) win 0
06/03/00 19:04:45.750762 d212-151-235-114.swipnet.se.2666 >
```

```
linux1.imap2: S 111:111(0) win 0
```

Address: **212.0.0.0**
[whois.arin.net]
European Regional Internet Registry/RIPE
These addresses have been further assigned to European users.
Netblock: 212.0.0.0 - 212.255.255.255

Name: dialup2-110.home.se
Address: **212.75.65.238**
netname: ITV-SE
country: SWEDEN
source: RIPE

Name: d212-151-235-114.swipnet.se
Address: **212.151.235.114**
netname: SE-SWIPNET-990408
country: SWEDEN
source: RIPE

1. Source of trace:

a. My network

2. Detect was generated by:

a. Shadow IDS

3. Probability that the source address was spoofed:

a. Low. IP addresses from a range of IP addresses registered to RIPE. Further investigation revealed that the IP addresses may have originated from ISPs in Sweden.

4. Description of the attack:

a. The attackers scan the network looking for vulnerable operating systems running IMAP services. The attackers are seeking to gain root access by exploiting buffer overflow vulnerabilities. For example, imapd core dumps in Linux can reveal shadowed passwords.

5. Attack mechanism:

a. The attackers are probing for IMAP servers listening on port 143. The remote mail access protocol services are especially vulnerable to attack because of the open nature of mail service access. Attackers know this and often look for flaws in remote mail services such as IMAP to gain root access. In this detect, the packets were custom built due to the fact that the sequence numbers and source ports are static and never change as the attacker scans network machines. Also, notice that seq/ack numbers 111:111 and source port 2666 were used. This signature has been seen before and is described as the YA Signature IMAP exploit.

6. Correlations:

a. Two separate scans occurred using the The YA Signature IMAP attack. The attacks originated from two separate ISPs in Sweden and there may be a clear link here. Also, this type of attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 203 of the 2.5 student guide.

b. CVE-1999-0005
Arbitrary command execution via IMAP buffer overflow in authenticate command.

CVE-1999-0042
Buffer overflow in University of Washington's
implementation of IMAP and POP servers.

CVE-1999-0920
Buffer overflow in the pop-2d POP daemon in the IMAP
package allows remote attackers to gain privileges via the
FOLD command.

CVE-2000-0053
Microsoft Commercial Internet System (MCIS) IMAP
server allows remote attackers to cause a denial of service via a malformed
IMAP request.

CVE-2000-0233
SuSE Linux IMAP server allows remote attackers to bypass IMAP
authentication and gain privileges.

7. Evidence of active targeting:

a. General scanning. Attacker is targeting many hosts on the network.

8. Severity:

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (4 + 5) - (5 + 2) = 2

9. Defense recommendations:

a. Router defenses were not sufficient to block this attack. Recommend that the router ACLs be updated to block all unused ports. Firewall purchase and deployment is recommended. NMAP was launched as a confidence test against the network to ensure that all IMAP services were disabled. Test was negative. All IMAP services were found to be disabled and host based defenses were fine.

10. Multiple choice question:

a. IMAP services are found on port?

A) 53
B) 110
C) 143
D) 109

b. Answer: C

Detect 3

```
05/28/00 09:13:07.422915 206.176.81.2.1939 > mailserver2.pop-3: S
524969305:524969305(0) win 32120 (DF)
05/28/00 09:13:07.423717 206.176.81.2.1716 > unix5.pop-3: S
1136684933:1136684933(0) win 32120(DF)
05/28/00 09:13:07.429476 206.176.81.2.2955 > windowz5.pop-3: S
968301875:968301875(0) win 32120  (DF)
05/28/00 09:13:10.375263 206.176.81.2.1716 > unix5.pop-3: S
1136684933:1136684933(0) win 32120(DF)
05/28/00 09:13:10.384280 206.176.81.2.2098 > unix3.pop-3: S
4066131156:4066131156(0) win 32120  (DF)
05/28/00 09:13:10.392844 206.176.81.2.1944 > workstation6.pop-3: S
342058513:342058513(0) win 32120  (DF)
05/28/00 09:13:10.395201 206.176.81.2.1986 > workstation3.pop-3: S
4198659242:4198659242(0) win 32120(DF)
05/28/00 09:13:10.403209 206.176.81.2.2095 > science1.pop-3: S
1342132460:1342132460(0) win 32120  (DF)
05/28/00 09:13:10.405103 206.176.81.2.1989 > unix4.pop-3: S
248004379:248004379(0) win 32120 (DF)
05/28/00 09:13:10.415194 206.176.81.2.2953 > workstation4.pop-3: S
4080759647:4080759647(0) win 32120(DF)
05/28/00 09:13:10.417111 206.176.81.2.3088 > workstation5.pop-3: S
1430640343:1430640343(0) win 32120 (DF)
05/28/00 09:13:10.429783 206.176.81.2.2999 > workstation7.pop-3: S
3842655878:3842655878(0) win 32120 (DF)
05/28/00 09:13:10.434512 206.176.81.2.2789 > linux1.pop-3: S
4290039877:4290039877(0) win 32120 (DF)
```

Address: **206.176.81.2**
[whois.arin.net]
Netname: SDNET-BLK-2
country: US Pierre, SD 57501
Netblock: 206.176.0.0 - 206.176.127.255

1. **Source of trace:**

    a. My network

2. **Detect was generated by:**

    a. Shadow IDS

3. **Probability that the source address was spoofed:**

    a. Low. IP address registered to SDNET, an ISP in Pierre, SD.

4. **Description of the attack:**

    a. The attacker scans the network looking for vulnerable POP-3 ports. The attacker is doing reconnaissance work and is seeking to exploit known buffer overflow vulnerabilities and gain access.

5. **Attack mechanism:**

a. The attacker probes the network for POP-3 servers on port 110. Remote mail access protocol services are especially vulnerable to attack because of the open nature of mail service access. Attackers know this and often look for flaws in remote mail services such as POP-3 to gain root access. As discussed, if the USER command is followed by an argument of over 1000 characters, the input buffer will be overflowed, and data from the argument will be passed to the system to be executed at the privilege level of the mailserver program.

In this particular detect, the packets are probably not custom built due to the fact that the sequence numbers and source ports change randomly. However, this attack appears to have been script driven; it lasted only 3 seconds and thirteen machines were scanned.

6. Correlations:

a. A similar attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 212 of the 2.5 student guide.

b CVE-1999-0006
Buffer overflow in POP servers based on BSD/Qualcomm's
qpopper allows remote attackers to gain root access using a
long PASS command.

CVE-1999-0272
Denial of service in Slmail v2.5 through the POP3 port.

CAN-2000-0016
** CANDIDATE (under review) ** Buffer overflow in Internet Anywhere
POP3 Mail Server allows remote attackers to cause a denial of service or
execute commands via a long username.

7. Evidence of active targeting:

a. General scanning. Attacker is targeting many hosts on the network.

8. Severity:

a. (Critical + Lethal) - (System + Countermeasures) = Severity

b. (4 + 5) - (5 + 2) = 2

9. Defense recommendations:

a. Router defenses were not sufficient to block this attack. Recommend that router ACLs be updated to block all unused services. Firewall purchase and deployment is recommended. NMAP was launched as a confidence test against the network to ensure that all POP-3 services were disabled. Test was negative. All POP-3 services were found to be disabled and host based defenses were fine.

10. Multiple choice question:

a. In this trace, (DF) indicates?

A) Do not fragment
B) Data fragment

C) Data FIN
D) Drop fragment

b. Answer: A

Detect 4

```
08:20:26.541962 omega.ensam.inra.fr.4371 > switch2.netbios-ssn: S
2002600485:2002600485(0) win 32120  (DF)
08:20:26.543859 omega.ensam.inra.fr.4369 > switch1.netbios-ssn: S
2012695354:2012695354(0) win 32120  (DF)
08:20:26.549098 omega.ensam.inra.fr.4377 > mailserver.netbios-ssn: S
2011383470:2011383470(0) win 32120  (DF)
08:20:26.551998 omega.ensam.inra.fr.4380 > unix7.netbios-ssn: S
2007441660:2007441660(0) win 32120  (DF)
08:20:26.562097 omega.ensam.inra.fr.4396 > unix9.netbios-ssn: S
2013756517:2013756517(0) win 32120  (DF)
08:20:26.566015 omega.ensam.inra.fr.4404 > unix4.netbios-ssn: S
2001186663:2001186663(0) win 32120  (DF)
08:20:26.607509 omega.ensam.inra.fr.4439 > develop1.netbios-ssn: S
2005024195:2005024195(0) win 32120  (DF)
08:20:26.608107 omega.ensam.inra.fr.4440 > unix2.netbios-ssn: S
2012680981:2012680981(0) win 32120  (DF)
08:20:26.608737 omega.ensam.inra.fr.4441 > unix3.netbios-ssn: S
2010500245:2010500245(0) win 32120  (DF)
08:20:26.627900 omega.ensam.inra.fr.4468 > linux1.netbios-ssn: S
1999611780:1999611780(0) win 32120  (DF)
08:20:26.629274 omega.ensam.inra.fr.4469 > linux2.netbios-ssn: S
2006026794:2006026794(0) win 32120  (DF)
08:20:26.639594 omega.ensam.inra.fr.4487 > unix1.netbios-ssn: S
2002711419:2002711419(0) win 32120  (DF)
08:20:26.664702 omega.ensam.inra.fr.4494 > mailserver2.netbios-ssn: S
2004906404:2004906404(0) win 32120  (DF)
08:20:26.750268 omega.ensam.inra.fr.4577 > adminlog1.netbios-ssn: S
2005037187:2005037187(0) win 32120  (DF)
08:20:26.755249 omega.ensam.inra.fr.4587 > adminlog2.netbios-ssn: S
2015833888:2015833888(0) win 32120  (DF)
08:20:26.761509 omega.ensam.inra.fr.4592 > rcomms.netbios-ssn: S
2003782108:2003782108(0) win 32120  (DF)
```

Name: omega.ensam.inra.fr
[whois.arin.net]
Address: **147.99.7.8**
Netname: INRA-VERSAILLES
Netnumber: 147.99.0.0
Country: FRANCE

1. Source of trace:

a. My network

2. **Detect was generated by:**

    a. Shadow IDS

3. **Probability that the source address was spoofed:**

    a. Low. IP address may have originated from INRA-VERSAILLES, an ISP in Versailles, France.

4. **Description of the attack:**

    a. The attacker scans the network searching for vulnerable operating systems running NETBIOS Session services on port 139. The attacker is doing reconnaissance work and seeking to exploit known vulnerabilities. For example, Windows NT comes with its NetBIOS services started by default; these services provide the file sharing service, remote management etc. These services should be turned off when connecting an NT machine to the net.

5. **Attack mechanism:**

    a. Apparently script driven, the attacker scanned sixteen machines in one second. The packets do not appear to be custom built due to the fact that the sequence numbers and source ports are random throughout the scan. After performing the reconnaissance work for systems listening on port 139, an attack would work by exploiting Windows 95 or Windows NT systems that have a known bug that could be triggered which could cause nasty results. This is done by sending OOB (Out Of Band) data to an established connection with a Windows user. Apparently Windows doesn't know how to handle OOB, so weird things happen such as the entire screen turning white/blue. Windows also sometimes has trouble handling network traffic after an attack. Rebooting should fix whatever problems this attack causes. This type of an attack is also known as WinNuke and can be further identified by the urgent flag set.

6. **Correlations:**

    a This attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 212 of the 2.5 student guide and page 193 of the 2.3 student guide.

    b. CVE-1999-0153
    Windows 95/NT out of band (OOB) data denial of service through NETBIOS port, aka WinNuke.

7. **Evidence of active targeting:**

    a. General scanning. Attacker is targeting many hosts on the network.

8. **Severity:**

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (4 + 2) - (5 + 2) = -1

9. Defense recommendations:

a. Router defenses were not sufficient to block this attack. Recommend that the router ACLs be updated. Firewall purchase and deployment is recommended. NMAP was launched as a confidence test against the network to ensure that NETBIOS services were disabled on port 139. Test was negative. Host NETBIOS Session services were found to be disabled and host based defenses were fine.

10. Multiple choice question:

a. This detect indicates?

A) Destination scanning
B) TCP Port scanning
C) Network pinging
D) Network mapping

b. Answer: B

Detect 5

```
03:47:07.544911 c729196-a.saltlk1.ut.home.com.32046 > linux1.sunrpc: S
4250789:4250789(0) win 8192  (DF)
03:47:07.588622 c729196-a.saltlk1.ut.home.com.32060 > work4.sunrpc: S
4250796:4250796(0) win 8192  (DF)
03:47:07.632784 c729196-a.saltlk1.ut.home.com.32066 > windoz7.sunrpc:
S 4250866:4250866(0) win 8192  (DF)
03:47:08.620881 c729196-a.saltlk1.ut.home.com.32060 > dialer.sunrpc: S
4272940:4272940(0) win 8192  (DF)
03:47:31.920359 c729196-a.saltlk1.ut.home.com.32064 > datagrb.sunrpc:
S 4296236:4296236(0) win 8192  (DF)
03:47:31.955745 c729196-a.saltlk1.ut.home.com.32073 > windoz1.sunrpc:
S 4296239:4296239(0) win 8192  (DF)
03:47:32.218265 c729196-a.saltlk1.ut.home.com.32023 > unixlog.sunrpc:
S 4296536:4296536(0) win 8192  (DF)
03:47:32.227491 c729196-a.saltlk1.ut.home.com.32024 > unix6.sunrpc: S
4296536:4296536(0) win 8192  (DF)
03:47:32.322808 c729196-a.saltlk1.ut.home.com.32033 > work1.sunrpc: S
4296636:4296636(0) win 8192  (DF)
03:47:32.363541 c729196-a.saltlk1.ut.home.com.32038 > rcomms.sunrpc: S
4296639:4296639(0) win 8192  (DF)
```

Address: **24.13.130.169**
[whois.arin.net]

Name: c729196-a.saltlk1.ut.home.com
@Home Network (NETBLK-UT-TCI-SALTLK-1)
24.13.128.0 - 24.13.135.255

1. **Source of trace:**

   a. My network

2. **Detect was generated by:**

   a. Shadow IDS

3. **Probability that the source address was spoofed:**

   a. Low. IP address registered to an ISP in Salt Lake City, UT.

4. **Description of the attack:**

   a. The attacker scans the network looking for vulnerable systems running the Sun RPC (rpcbind, portmapper) service on port 111. This service will help the attacker scanning the system learn about other RPC-based programs that may be running. The attacker is seeking to exploit flaws in RPC programs. The attacker may only be interested in reconnaissance and at a later date perform an attack. The packets do not appear to be crafted and the attack lasted 25 seconds.

5. **Attack mechanism:**

   a. The first stage of the attack was reconnaissance, which entailed scanning the network looking for port vulnerabilities and holes. In this case, if an intrusion attack had occurred, it would have consisted of the attacker exploiting identified RPC programs running on a system. The attacker would perform the RPC portmapper dump command (rpcinfo -p system) against a vulnerable system to gain information. RPC portmapper dump would render a list of RPC programs on the machine and tip off the attacker to any existing holes that could be exploited in RPC programs. For example, a buffer overflow attack could be initiated and is a very common exploit. A buffer overflow attack is the result of a programming mistake of not double-checking input, and allowing large input (user login name of 1000 characters) to overflow into another memory location, causing the system to crash or allowing arguments to be passed for access.

6. **Correlations:**

   a. This attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 269 of the 2.5 student guide.

   b. CVE-1999-0018
   Buffer overflow in statd allows root privileges.

   CVE-1999-0019
   Delete or create a file via rpc.statd, due to invalid information.

   CVE-1999-0493
   rpc.statd allows remote attackers to forward RPC calls to the local operating system via the SM_MON and SM_NOTIFY commands, which in turn could be used to remotely exploit other bugs such as in automountd.

CVE-1999-0189
Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111

7. **Evidence of active targeting:**

a. General scanning. Attacker is targeting many hosts on the network.

8. **Severity:**

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (4 + 5) - (5 + 2) = 2

9. **Defense recommendations:**

a. Router defenses were not sufficient to block this attack. Recommend that the router ACLs be updated. Firewall purchase and deployment is recommended. NMAP was launched as a confidence test against the network to ensure that the vulnerable services were disabled. Test was negative. RPC services were found to be disabled and host based defenses were fine.

10. **Multiple choice question:**

a. In this trace, destination port 111/tcp is found in the?

A) ICMP message header
B) TCP segment header
C) UDP datagram header
D) IP datagram header

b. Answer: B

Detect 6

```
03:59:58.010668 pelc.casablanca.cz.4575 > windowz3.domain: 9146 inv_q+
[b2&3=0x980] A? . (27)
03:59:58.036967 pelc.casablanca.cz.4797 > workstation1.domain: 9146
inv_q+ [b2&3=0x980] A? . (27)
03:59:58.735675 pelc.casablanca.cz.1137 > mailserver.domain: 5869
inv_q+ [b2&3=0x980] A? . (27)
03:59:59.577807 pelc.casablanca.cz.1401 > linux1.domain: 5869 inv_q+
[b2&3=0x980] A? . (27)
03:59:59.594823 pelc.casablanca.cz.1438 > windowz1.domain: 5869 inv_q+
[b2&3=0x980] A? . (27)
03:59:59.865198 pelc.casablanca.cz.datametrics > unix9.domain: 154
inv_q+ [b2&3=0x980] A? . (27)
04:00:00.032456 pelc.casablanca.cz.1749 > workstation4.domain: 154
inv_q+ [b2&3=0x980] A? . (27)
04:00:00.217610 pelc.casablanca.cz.2478 > mailserver2.domain: 154
inv_q+ [b2&3=0x980] A? . (27)
04:00:00.258105 pelc.casablanca.cz.2524 > unixlogger.domain: 154
inv_q+ [b2&3=0x980] A? . (27)
```

```
04:00:00.269399 pelc.casablanca.cz.2536 > linux2.domain: 154 inv_q+
[b2&3=0x980] A? . (27)
04:00:00.295248 pelc.casablanca.cz.2594 > workstation7.domain: 154
inv_q+ [b2&3=0x980] A? . (27)
04:00:00.477907 pelc.casablanca.cz.3407 > rcomms.domain: 154 inv_q+
[b2&3=0x980] A? . (27)
04:00:00.518473 pelc.casablanca.cz.3511 > unix2.domain: 154 inv_q+
[b2&3=0x980] A? . (27)
```

Name: pelc.casablanca.cz
[whois.arin.net]
Address: 195.22.42.129

European Regional Internet Registry/RIPE
These addresses have been further assigned to European users.
inetnum: 195.22.42.0 - 195.22.42.255
netname: CZ-CASABLANCA
country: CZECH REPUBLIC
source: RIPE

1. **Source of trace:**

   a. My network

2. **Detect was generated by:**

   a. Shadow IDS

3. **Probability that the source address was spoofed:**

   a. Low. IP address is from a range of IP addresses registered to RIPE. Further investigation revealed that the address may have originated from an ISP in the Czech Republic.

4. **Description of the attack:**

   a. The attacker scanned the network looking for vulnerabilities to exploit in un-patched or older version BIND servers by performing inverse queries. Older versions of BIND are vulnerable to exploits using this inverse query method of attack. The attack consisted of 13 machines being scanned in two seconds. The source ports varied and no DNS servers were scanned.

5. **Attack mechanism:**

   a. BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check a memory copy when responding to an inverse query request. An improperly or maliciously formatted inverse query on a TCP stream can crash the server or allow an attacker to gain root privileges.

6. **Correlations:**

   a. This attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 10th. Also, references can be found on page 231 of the 2.3 student guide.

b. CVE-1999-0009
Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.

CVE-1999-0275
Denial of service in Windows NT DNS servers by flooding
port 53 with too many characters.
References: XF:nt-dnscrash, XF:nt-dnsver, MS:Q169461

CVE-1999-0010
Denial of Service vulnerability in BIND 8 Releases via
maliciously formatted DNS messages.

CVE-1999-0024
DNS cache poisoning via BIND, by predictable query IDs.

CVE-1999-0101
Buffer overflow in AIX and Solaris "gethostbyname" library
call allows root access through corrupt DNS host names.

7. Evidence of active targeting:

a. General scanning. Attacker is targeting many hosts on the network.

8. Severity:

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (4 + 5) - (5 + 2) = 2

9. Defense recommendations:

a. Router defenses were not sufficient to block this attack. Recommend that the router ACLs be updated. Firewall purchase and deployment is recommended. Recommend disabling inverse queries, upgrade to BIND 8.1.2, or apply the necessary patch (if required) on DNS servers.

10. Multiple choice question:

a. In this detect, [b2&3=0x980] represents:

A) Normal query (980)
B) Byte multiplier (980)
C) Time to live (ttl)(980)
D) Inverse query (980)

b. Answer: D

Detect 7

```
06/06/00   13:54:58.463166   195.182.169.4.domain   >   switch1.domain:   SF
425838104:425838104(0) win 1028
06/06/00   13:54:58.503284   195.182.169.4.domain   >   swicth2.domain:   SF
425838104:425838104(0) win 1028
06/06/00  13:54:58.633322  195.182.169.4.domain     >  mailserver.domain:  SF
425838104:425838104(0) win 1028
```

```
06/06/00    13:54:58.683124    195.182.169.4.domain    >    unix1.domain:    SF
425838104:425838104(0) win 1028
06/06/00 13:54:58.903841 195.182.169.4.domain        > mailserver2.domain: SF
425838104:425838104(0) win 1028
06/06/00 13:54:58.954415 195.182.169.4.domain        > development.domain: SF
425838104:425838104(0) win 1028
06/06/00    13:54:59.003572    195.182.169.4.domain    >    unix2.domain:    SF
425838104:425838104(0) win 1028
06/06/00    13:54:59.126040    195.182.169.4.domain    >    unix4.domain:    SF
425838104:425838104(0) win 1028
06/06/00    13:54:59.162432    195.182.169.4.domain    >    unix6.domain:    SF
425838104:425838104(0) win 1028
06/06/00   13:54:59.869935  195.182.169.4.domain       >  science2.domain:   SF
118313227:118313227(0) win 1028
06/06/00    13:55:00.462865    195.182.169.4.domain    >    linux2.domain:    SF
1960974483:1960974483(0) win 1028
06/06/00 13:55:02.641704 195.182.169.4.domain        > adminlogger.domain: SF
1344512094:1344512094(0) win 1028
06/06/00    13:55:02.854851    195.182.169.4.domain    >    linux4.domain:    SF
1344512094:1344512094(0) win 1028
06/06/00    13:55:02.941566    195.182.169.4.domain    >    rcomms.domain:    SF
1344512094:1344512094(0) win 1028
```

Address: 195.182.169.4
[whois.arin.net]
European Regional Internet Registry/RIPE
inetnum: 195.182.169.0 - 195.182.169.31
netname: WEBNETICS
descr: Nottingham
country: GREAT BRITAIN
source: RIPE

1. **Source of trace:**

   a. My network

2. **Detect was generated by:**

   a. Shadow IDS

3. **Probability that the source address was spoofed:**

   a. Low. IP address from a block of IP addresses registered to RIPE. Further investigation revealed that the address may have originated from an ISP, Webnetics Internet Solutions, Nottingham, Great Britain.

4. **Description of the attack**:

   a. The attacker performs a SYN-FIN scan of the network searching for vulnerabilities in older versions of BIND. The source ports remained static and sequence numbers appear anomalous. As discussed, the SF flags should never be set simultaneously in normal connections. The attack lasted four seconds and fourteen machines were scanned. The packets were custom built.

5. **Attack mechanism:**

   a. BIND 4.9 releases prior to BIND 4.9.7 and BIND 8 releases prior to 8.1.2 do not properly bounds check many memory references in the server and the resolver. An improperly or maliciously formatted DNS message can cause the server to read from invalid memory locations, yielding garbage record data or crashing the server. Many DNS utilities that process DNS messages (e.g., dig, nslookup) also fail to do proper bounds checking.

6. **Correlations:**

a. Similar attacks were described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 209 of the 2.3 student guide.

b. CVE-1999-0833
Buffer overflow in BIND 8.2 via NXT records.

CVE-1999-0275
Denial of service in Windows NT DNS servers by flooding port 53 with too many characters. References: XF:nt-dnscrash, XF:nt-dnsver, MS:Q169461

CVE-1999-0010
Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.

CVE-1999-0024
DNS cache poisoning via BIND, by predictable query IDs.

CVE-1999-0101
Buffer overflow in AIX and Solaris "gethostbyname" library
call allows root access through corrupt DNS host names.

7. **Evidence of active targeting:**

a. General scanning. Attacker is targeting many hosts on the network.

8. **Severity:**

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (4 + 4) - (5 + 2) = 1

9. **Defense recommendations:**

a. Router defenses were not sufficient to block this attack. Recommend that the router ACLs be updated. Firewall purchase and deployment is recommended. Test was negative. Host and server services on port 53 were found to be disabled and defenses were fine. If required, recommend upgrades and patches be installed to keep DNS servers secure.

10. **Multiple choice question:**

a. Zone transfers occur on port?

A) 53/udp
B) 53/icmp
C) 53/tcp

D) 53/snmp

b. Answer: C

Detect 8

```
May 31 04:56:03 router.1 70335: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 05:01:17 router.1 70340: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 07:34:41 router.1 70445: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 07:51:19 router.1 70456: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 15:45:03 router.1 70806: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 18:35:18 router.1 70857: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 19:11:25 router.1 70865: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 19:16:25 router.1 70866: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
May 31 22:11:33 router.1 70896: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
Jun  1 09:31:36 router.1 70957: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
Jun  1 15:45:00 router.1 71087: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
Jun  1 16:18:41 router.1 71091: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 2 packets
Jun  1 16:23:41 router.1 71092: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
Jun  1 17:43:57 router.1 71117: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 1 packet
Jun  1 18:36:43 router.1 71139: %SEC-6-IPACCESSLOGP: list 103 denied udp
204.30.214.249(3216) -> adminlogger(514), 2 packets
```

Address: 204.30.214.249
[whois.arin.net]
NETCOM On-Line Communication Services, Inc. (NETBLK-NETCOM254)
San Jose, CA 95128
Netname: NETCOM254
Netblock: 204.30.0.0 - 204.33.255.255

1. **Source of trace:**

   a. My network

2. **Detect was generated by:**

   a. Cisco router ACL logs

   b. Explanation of fields

Jun 1 18:36:43 [timestamp] **router.1** [hostname of router] **71139: %SEC-6-IPACCESSLOGP: list 103** [router type & access list responsible] **denied**

```
[ACL action taken] udp [transport protocol] 204.30.214.249(3216)[source IP
address & port #]-> adminlogger(514),[dest address & port#] 2 packets [# of
packets]
```

3. **Probability that the source address was spoofed:**

   a. Low. IP address registered to NETCOM, an ISP in San Jose, CA.

4. **Description of the attack:**

   a. Attacker repeatedly pounds away possibly trying to gain root access by buffer overflow exploit. The attack occurs over 38 hours and in not successful. Source and destination IP addresses and port numbers remained static and attack tempo was inconsistent.

5. **Attack mechanism:**

   a. Attacker attempting buffer overflow or DoS as described in CVE-1999-0099, CVE-1999-0566, CVE-1999-0831.

6. **Correlations**:

   a. CVE-1999-0099
   Buffer overflow in syslog utility allows local or remote
   attackers to gain root privileges.

   CVE-1999-0566
   An attacker can write to syslog files from any location,
   causing a denial of service by filling up the logs, and hiding
   activities.

   CVE-1999-0831
   Denial of service in Linux syslogd via a large number of
   connections.

   CVE-1999-0063
   Cisco IOS 12.0 and other versions can be crashed by
   malicious UDP packets to the syslog port.

7. **Evidence of active targeting:**

   a. Attacker is targeting this specific host.

8. **Severity:**

   a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

   b. (3 + 5) - (5 + 5) = -2

9. **Defense recommendations:**

   a. Defenses are fine. The router ACL blocked the attack.

10. **Multiple choice question:**

   a. IP header protocol 17 defines?

A) UDP
B) TCP
C) ICMP
D) SNMP

b. Answer: A

Detect 9

```
May 10 13:18:12 router.1 35655: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.2(137), 1 packet
May 10 13:18:20 router.1 35656: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.3(137), 1 packet
May 10 13:18:28 router.1 35660: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.4(137), 1 packet
May 10 13:18:35 router.1 35661: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.5(137), 1 packet
May 10 13:18:46 router.1 35662: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.6(137), 1 packet
May 10 13:18:53 router.1 35663: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.7(137), 1 packet

********************** All IP addresses in between ************************

May 10 13:50:27 router.1 35935: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.238(137), 2 packets
May 10 13:50:50 router.1 35937: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.239(137), 2 packets
May 10 13:51:25 router.1 35938: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.240(137), 2 packets
May 10 13:53:23 router.1 35939: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.241(137), 2 packets
May 10 13:53:25 router.1 35940: %SEC-6-IPACCESSLOGP: list 101 denied udp
199.174.149.108(1064) -> my.net.box.243(137), 2 packets
```

199.174.149.108
[whois.arin.net]
EarthLink, Inc. (NET-EARTHLINK2000-C)
Pasadena, CA 91107
Netname: EARTHLINK2000-C
Netblock: 199.174.0.0 - 199.174.255.255

1. Source of trace:

a. My network

2. Detect was generated by:

a. Cisco router ACL logs

3. Probability that the source address was spoofed:

a. Low. IP address registered to EarthLink, an ISP in Pasadena, CA.

4. Description of the attack:

a. The attacker scanned the entire address space looking to exploit vulnerabilities in the NetBIOS name service normally found on port 137. The scan lasted 35 minutes. The source IP addresses and port numbers remained static.

5. **Attack mechanism:**

a. Port 137 is used for NetBIOS name service. This is how NetBIOS-based services find each other. On a NetBIOS network, these names uniquely identify the machine and services running on the machine. Machines find each other either using broadcasts or looking them up in a centralized NetBIOS naming server (WINS server). Windows servers use NetBIOS and DNS to resolve IP addresses to names using the "gethostbyaddr()" function.

One such attack, as descibed by CVE-1999-0288 is a Denial of Service in WINS, with malformed data sent to port 137. Another attack relates to obvious vulnerabilities in network file shares.

6. **Correlations:**

a. This attack was described during the network based intrusion detection analysis lecture at SANS2000 in San Jose on May 12th. Also, references can be found on page 292 of the 2.5 student guide.

b. CVE-1999-0288
Denial of service in WINS with malformed data to port 137
(NETBIOS Name Service).

CAN-1999-0520 (under review)
A system-critical NETBIOS/SMB share has inappropriate access
control.

CAN-1999-0544 (under review)
NFS exports system-critical data to the world, e.g. / or a password file.

7. **Evidence of active targeting:**

a. General scanning. Attacker is targeting many hosts on the network.

8. **Severity:**

a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (5 + 2) - (5 + 5) = -3

9. **Defense recommendations:**

a. Defenses are fine. The router ACL blocked the attack.

10. **Multiple choice question:**

a. If a client sends a SYN to an open server port, the server will respond with?

A) SYN/ACK
B) FIN/ACK

C) RESET/ACK
D) SYN/FIN

b. Answer: A

Detect 10

```
Jun  2 16:10:37 router.1 71683: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1323) -> WEBSERVER(80), 1 packet
Jun  2 16:10:41 router.1 71684: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1324) -> WEBSERVER(80), 1 packet
Jun  2 16:10:46 router.1 71685: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1325) -> WEBSERVER(80), 1 packet
Jun  2 16:10:47 router.1 71686: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1326) -> WEBSERVER(80), 1 packet
Jun  2 16:13:03 router.1 71687: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.188(4312) -> WEBSERVER(80), 1 packet
Jun  2 16:13:09 router.1 71688: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.188(4314) -> WEBSERVER(80), 1 packet
Jun  2 16:13:21 router.1 71689: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.188(4315) -> WEBSERVER(80), 1 packet
Jun  2 16:24:31 router.1 71690: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1327) -> WEBSERVER(80), 1 packet
Jun  2 16:24:32 router.1 71691: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1328) -> WEBSERVER(80), 1 packet
Jun  2 16:25:09 router.1 71692: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.188(4399) -> WEBSERVER(80), 1 packet
Jun  2 16:27:06 router.1 71693: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1330) -> WEBSERVER(80), 1 packet
Jun  2 17:24:15 router.1 71694: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.1.3.211(2687)      -> WEBSERVER(80), 1 packet
Jun  2 17:29:59 router.1 71695: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.1.3.211(2687)      -> WEBSERVER(80), 5 packets
Jun  2 17:32:31 router.1 71696: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1378) -> WEBSERVER(80), 1 packet
Jun  2 17:32:33 router.1 71697: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(1380) -> WEBSERVER(80), 1 packet
Jun  2 22:14:00 router.1 71775: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.199(3891) -> WEBSERVER(80), 1 packet
Jun  2 22:15:11 router.1 71776: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.199(3893) -> WEBSERVER(80), 1 packet
Jun  2 22:15:13 router.1 71777: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.199(3894) -> WEBSERVER(80), 1 packet
Jun  2 22:43:34 router.1 71778: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1110) -> WEBSERVER(80), 1 packet
Jun  2 22:43:35 router.1 71779: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1112) -> WEBSERVER(80), 1 packet
Jun  2 22:43:37 router.1 71780: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1114) -> WEBSERVER(80), 1 packet
Jun  2 22:43:38 router.1 71781: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1120) -> WEBSERVER(80), 1 packet
Jun  2 22:57:47 router.1 71782: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.197.121(3545) -> WEBSERVER(80), 1 packet
Jun  2 23:07:31 router.1 71783: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1163) -> WEBSERVER(80), 1 packet
Jun  2 23:07:37 router.1 71784: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1164) -> WEBSERVER(80), 1 packet
Jun  2 23:07:47 router.1 71785: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1165) -> WEBSERVER(80), 1 packet
Jun  2 23:07:52 router.1 71786: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1166) -> WEBSERVER(80), 1 packet
Jun  2 23:07:54 router.1 71787: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1167) -> WEBSERVER(80), 1 packet
Jun  2 23:10:20 router.1 71788: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.194.121(1174) -> WEBSERVER(80), 1 packet
Jun  2 23:12:34 router.1 71789: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.168.58(1293) -> WEBSERVER(80), 1 packet
Jun  2 23:18:07 router.1 71790: %SEC-6-IPACCESSLOGP: list 101 denied tcp 192.168.168.58(1293) -> WEBSERVER(80), 5 packets
Jun  2 23:36:26 router.1 71791: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3609) -> WEBSERVER(80), 1 packet
Jun  2 23:36:28 router.1 71792: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3610) -> WEBSERVER(80), 1 packet
Jun  2 23:38:15 router.1 71793: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2136) -> WEBSERVER(80), 1 packet
Jun  2 23:38:17 router.1 71794: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2137) -> WEBSERVER(80), 1 packet
Jun  2 23:40:34 router.1 71795: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2139) -> WEBSERVER(80), 1 packet
Jun  2 23:40:35 router.1 71796: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2140) -> WEBSERVER(80), 1 packet
Jun  2 23:58:02 router.1 71797: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3714) -> WEBSERVER(80), 1 packet
Jun  2 23:58:16 router.1 71798: %SEC-6-IPACCESSLOGP: list 101 denied tcp 172.16.10.51(3468)    -> WEBSERVER(80), 1 packet
Jun  2 23:58:35 router.1 71799: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3718) -> WEBSERVER(80), 1 packet
Jun  3 00:04:07 router.1 71800: %SEC-6-IPACCESSLOGP: list 101 denied tcp 172.16.10.51(3469)    -> WEBSERVER(80), 5 packets
Jun  3 00:07:11 router.1 71801: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2217) -> WEBSERVER(80), 1 packet
Jun  3 00:08:08 router.1 71802: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2285) -> WEBSERVER(80), 1 packet
Jun  3 00:08:13 router.1 71803: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2308) -> WEBSERVER(80), 1 packet
Jun  3 00:08:30 router.1 71804: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2310) -> WEBSERVER(80), 1 packet
Jun  3 00:08:32 router.1 71805: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2311) -> WEBSERVER(80), 1 packet
Jun  3 00:08:33 router.1 71806: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2312) -> WEBSERVER(80), 1 packet
Jun  3 00:22:44 router.1 71807: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2314) -> WEBSERVER(80), 1 packet
Jun  3 00:22:49 router.1 71808: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2315) -> WEBSERVER(80), 1 packet
Jun  3 00:26:15 router.1 71809: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3882) -> WEBSERVER(80), 1 packet
Jun  3 00:26:18 router.1 71810: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3883) -> WEBSERVER(80), 1 packet
Jun  3 00:26:20 router.1 71811: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3884) -> WEBSERVER(80), 1 packet
Jun  3 00:59:52 router.1 71814: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.207.249(1349) -> WEBSERVER(80), 1 packet
Jun  3 01:04:36 router.1 71816: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.207.249(1053) -> WEBSERVER(80), 1 packet
Jun  3 01:13:18 router.1 71818: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3957) -> WEBSERVER(80), 1 packet
Jun  3 01:13:22 router.1 71819: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3958) -> WEBSERVER(80), 1 packet
Jun  3 01:13:24 router.1 71820: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.204(3959) -> WEBSERVER(80), 1 packet
Jun  3 01:23:49 router.1 71821: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2706) -> WEBSERVER(80), 1 packet
Jun  3 01:23:51 router.1 71822: %SEC-6-IPACCESSLOGP: list 101 denied tcp 10.12.252.176(2708) -> WEBSERVER(80), 1 packet
```

[whois.arin.net]
IANA
(RESERVED-6)
Internet Assigned Numbers Authority
Netname: RESERVED-10
Netblock: 10.0.0.0 - 10.255.255.255
Netname: IANA-CBLK1
Netblock: 192.168.0.0 - 192.168.255.0

1. **Source of trace:**

   a. My network

2. **Detect was generated by**:

   a. Cisco router ACL logs

3. **Probability that the source address was spoofed:**

   a. High. These IP addresses were graciously borrowed from a block of addresses reserved by IANA and therefore should never appear as the source address of a packet entering a network.

4. **Description of the attack:**

   a. The attacker used two reserved address families to try tcp connections to port 80 of the webserver. The attack was spaced out over seven hours with the attacker using reserved IP addresses. The attack was not successful.

5. **Attack mechanism:**

   a. The attacker was trying to start TCP connections with the HTTP server by sending the first synchronization (SYN) packet necessary in normal three way handshakes to port 80. A server listening on port 80 would normally respond with a SYN/ACK. Three to six SYN requests per minute could be enough to create a Denial of Service (DoS) situation.

6. **Correlations:**

   a. CVE-1999-0437
   Remote attackers can perform a denial of service in WebRamp
   systems by sending a malicious string to the HTTP port.

   CAN-1999-0107 (under review)
   Buffer overflow in Apache 1.2.5 and earlier allows a remote
   attacker to cause a denial of service with a large number of GET
   requests containing a large number of / characters.

7. **Evidence of active targeting:**

   a. Attacker is targeting a specific host.

8. **Severity:**

   a. (Critical + Lethal) - (System + Net Countermeasures) = Severity

b. (5 + 5) - (5 + 5) = 0

9. Defense recommendations:

a. Defenses are fine. Router ACL blocked the attack.

10. Multiple choice question:

a. If a client sends a SYN to a closed server port, the server will respond with?

A) SYN/ACK
B) FIN/ACK
C) RESET/ACK
D) SYN/FIN

b. Answer: C