Global Information Assurance Certification Paper

SANS 2000
GIAC Intrusion Detection Curriculum

Practical Assignment for SNAP San Jose, May 8 - 13, 2000

Submitted by

Mou-Liang Kung

Please Note:

1. All detects are collected from a class C network. The class C network is divided into two subnets. Subnet1 includes IP-addresses X.X.X.0 - 127 and Subnet2 includes X.X.X.129 - 254. Two separate IDS monitoring stations running WinDump were used to collect traffic on these two subnets.
2. The traffic dump file is then processed using "grep" utility to extract TCP-related traffic pattern "S", "F", "R", "ack". Again, "grep" was used to extract patterns that contain ports used for exploitation, e.g. 7, 19, 21, 23, 53, 80, 110, ... 65535. Only externally initiated traffic are examined and included in this Practical Assignment. The source domain name or IP address lookup was conducted by browsing http://swhois.net/
3. Tables of port assignments and trojan port numbers are obtained from http://www.xploiter.com/tambu/port.ini, ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers, and http://secure-me.net/trojans.

==========

Detect 1

==========

04:21:44.903869 202.235.50.12**.65535** > Subnet2.189**.8080: S** 1081475072:1081475072(0) win 512 (ttl 241, id 16502)

4500 0028 4076 0000 f106 5435 caeb 320c
xxxx xxxx **ffff 1f90 4076 0000 0000 0000**
5002 0200 18b8 0000 0000 0000 0000

04:21:44.905420 Subnet2.189.8080 > 202.235.50.12.65535: R 0:0(0) ack 1081475073 win 0 (ttl 128, id 46437)

1. Source of trace

This traffic pattern was detected on a Subnet2 on June 7, 2000.

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n -x**

The format of the trace:

time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

Since an attempt to establish a TCP connection was shown in order to collect information, the address was not spoofed. The IP number 202.235.50.12 can not be inverse-mapped to a domain name. However, using Smart Whois query, it revealed that the IP address range 202.232.0.0 - 202.235.255.255 (JPNIC-NET-JP) is owned by Japan Network Information Center.

4. Description of attack:

The high TCP port "SYN"ed to a remote port 8080 becomes a familiar pattern recently. Notice the sequence number **0x4076 0000** (very artificial!), win size **0x 0200 and** the TCP payload is **0000 0000 0000 ....** , they look somewhat familiar *(Please see the later Correlations section to see the similarity).* It is a crafted packet.

5. Attack mechanism:

Attacks on WinGate Proxy Server version 2.1 for Windows surfaced in 1998. The Rhino Team advisories stated that "The problem is in the WinGate LogFile service (TCP port 8010) being accessible to anyone by default and poor programming on the part of Deerfield Communications Company. If the LogFile service is not reconfigured after install then any remote user can access the WinGate servers hard drive having read access to any file on the same drive as the WinGate installation." (http://207.98.195.250/advisories/05.htm).

The detect of SYN attempt on port 8080 may be a precursor to the WinGate Logfile attack. If the WinGate proxy server is identified, an attack may be launched on TCP Port 8010 where the WinGate LogFile Service is listening.

6. Correlations:

The detect is almost identical to those found in Arrigo's contribution (http://www.sans.org/y2k/052300-0800.htm)

```
05/20-02:24:12.104358 207.78.247.50:65535 -> 192.168.1.103:8080
TCP TTL:240 TOS:0x0 ID:16454
S***** Seq: 0x40460000 Ack: 0x0 Win: 0x200
00 00 00 00 00 00 ......
```

and Phillip's contribution (http://www.sans.org/y2k/052500.htm)

```
05/23-23:12:51.188133 207.78.247.50:65535 -> xxx.yyy.zzz.137:8080 TCP TTL:236
TOS:0x0 ID:22354 **S***** Seq: 0x57520000 Ack: 0x0 Win: 0x200
00 00 00 00 00 00 ......
```

7. Evidence of active targeting:

An interesting thing is that no host scan or port scan from this source address can be found in the evening archive from the last two weeks. Different addresses must have been used in prior reconnaissance efforts to identify my host.

8. Severity:

Component	Score	Reason
Criticality	1.5	Although a specific server is targeted (3), WinGate proxy server is not installed (0). So it averaged out to 1.5
Lethality	0	It was only a probe and no WinGate Proxy was installed
System Countermeasures	3	Most unused ports closed
Network Countermeasures	0	Router does not block TCP and UDP port 8080 or 8010
Severity Score	-1.5	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

If WinGate is running, one should upgrade it to the latest version (version 4). On version 2.1, the LogFile Service should not be bound to any incoming interface.

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

a) The unusual part of the captured traffic is the destination port 8080.
b) The unusual part of the captured traffic is the source port 65535.
c) The unusual part of the captured traffic is source IP address.
d) The unusual part of the captured traffic is that ACK field contains all 0s.

Answer: b

==========

Detect 2

==========

```
19:30:01.132532 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:01.379528 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:01.625532 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:01.872536 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:02.118535 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:02.365035 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:02.612540 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:02.858536 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:03.102540 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:03.348546 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:03.595547 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
19:30:03.841556 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
(snip ...)
19:31:00.640364 128.125.251.210 > 255.255.255.255: icmp: echo request (ttl 245, id 12311)
```

1. Source of trace

This is detected on Subnet2 on May 24, 2000.

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n**

The format of the trace:
time src.port > dst.port protocol-type length(time-to-live, ID#).

3. Probability the source address was spoofed

The source address must be spoofed, since ping broadcast has been sent out at a rapid pace with the same ID number. Each ping was repeated exactly 4 times a second. There is no follow-up traffic from the source host after pings lasted 1 minute. Subsequently, I contacted the Data Network Operations of the University of Southern California who owns the source IP address. A reply was received on June 7, 2000 as follows: *"We do filter outbound traffic to prevent standard directed broadcast and smurfish attacks on other sites. There is the possibility that our address wasn't spoofed and an attack slipped out during a update to a filter. However, updates take seconds not a full minute so those chances are remote."*

4. Description of attack:

This could be a DoS attack on the host 128.125.251.210. The IP-address is spoofed to generate icmp echo request at high frequency (4 pings per second) to our subnet. The same ID number 12311 confirms that the packets were crafted.

5. Attack mechanism:

This DOS attack is known as the SMURF Attack in which routers, with broadcast ON, cooperated with the attacker by broadcasting Ping from a spoofed victim to all subnet hosts so that echo replies will be directed to the victim.

6. Correlations:

Although prior broadcast Pings received from other sites include:

Date	Duration	Source	Average Num of Pings/sec	ID number
5/17/00	14:07:11 - 15:26:57	157.193.56.103	3	n/a
5/19/00	1:30:16 - 1:31:02	192.55.214.69	2	8296, 8297 alternating
5/19/00	22:54:23 - 23:04:19	195.159.0.151	7	13471
5/19/00	23:03:40 - 23:05:21	206.184.139.136	1.5	8973
5/20/00	14:32:29-14:34:02	216.2.8.6	7.5	2574

No correlation can be found. However, traffic with sources 195.159.0.151 and 216.2.8.6 both may be spoofed since the Pings were rapid (> 7 pings/sec) as seen in a Smurf Attack.

7. Evidence of active targeting:

The pattern suggests that the packets invite echo replies from multiple hosts back to the source host.

8. Severity:

Component	Score	Reason
Criticality	2	No specific local host was spoofed or targeted (0). However, local hosts are now known to intruders whether they may become accomplices for future DoS attacks (4)
Lethality	2	Any time broadcast is permitted to come in, traffic increases.
System Countermeasures	4	Most hosts have disabled chargen and echo TCP and UDP ports ports.
Network Countermeasures	0	Router (maintained by a contractor) did not turn off echo broadcast
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Smurf attack can be blocked by firewall or properly configured routers (with broadcast turned OFF).

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

a) Smurf attack on Subnet2 hosts
b) Smurf attack on source host
c) Host scans on Subnet2
d) Host scans on source network

Answer: b

==========

Detect 3

==========

```
17:36:28.303001 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:28.877971 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:29.707928 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:29.719424 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:29.768424 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:30.277901 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:30.468889 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:30.537386 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:36:30.576882 213.255.7.252.25882 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
(snip ...)
17:53:47.013365 213.255.7.252.27920 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.039864 213.255.7.252.46272 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.119863 213.255.7.252.46272 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.150852 213.255.7.252.46272 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.252854 213.255.7.252.63884 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.340851 213.255.7.252.27920 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.381347 213.255.7.252.27920 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.420346 213.255.7.252.27920 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.442339 213.255.7.252.63884 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.481843 213.255.7.252.16435 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
```

```
17:53:47.510840 213.255.7.252.63884 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
17:53:47.549337 213.255.7.252.63884 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
(snip ...)
17:53:57.688830 213.255.7.252.53085 > 255.255.255.255.19: udp 0 (ttl 237, id 1)
```

1. Source of trace

This is detected on Subnet1 on May 18, 2000. The storm of broadcast traffic began at 17:36:28 and ended at 17:53:57 .

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n**

The format of the trace:
time src.port > dst.port protocol-type length(time-to-live, ID#).

3. Probability the source address was spoofed

The source IP address is mapped to tnt2.TO1.albacom.net. The address range 213.255.0.0 - 213.255.7.255 belongs to Albacom Dial Services, an ISP. We ruled out the possibility that the source address is a spoofed address, since the source port is not the echo port (port 7) associated with chargen-attack. Therefore, the source is the real and actively seeking hosts with open chargen service to become its accomplices to DoS attacks later.

4. Description of attack:

A common exploit on chargen port (TCP/UDP port 19) is to setup a communication between an echo port and a chargen port on two separate machines. At the first glance, it seemed that the source host is broadcasting many datagrams of length 0 to the chargen UDP port (19) within Subnet1 trying to find which hosts which will respond with a random number of characters. The source host port (25882) found on the initial batch of packets were identical. It may seem that a Denial of Service attack was launched on the spoofed source host. However, the source port numbers soon fell randomly between 15417 - 65495. Another careful examination of the port numbers reveals that random port numbers were not random after all. The same set of a few port numbers was randomly sequenced to disguise as random. Therefore, it is determined that it is a reconnaissance effort to find hosts with chargen port open to be used for a DoS attack on some host later.

5. Attack mechanism:

None of the traffic targeted hosts using chargen TCP port (19). If TCP port was used, then a stream of characters will be sent back to the source until the source host quits. In this case, the source host has no interest in doing so.

6. Correlations:

From 19:21:31 to 19:21:57 on May 22, 2000, the following trace was collected from the Subnet2:

```
19:21:31.934975 193.224.148.2.23959 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.080970 193.224.148.2.42240 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.085963 193.224.148.2.41893 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
```

```
19:21:32.178965 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.230960 193.224.148.2.41893 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.251461 193.224.148.2.10400 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.298959 193.224.148.2.10400 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.299453 193.224.148.2.10400 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.691938 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.705936 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.733935 193.224.148.2.23959 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.755935 193.224.148.2.23959 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.814933 193.224.148.2.10400 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.856430 193.224.148.2.41893 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.901930 193.224.148.2.41893 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.915919 193.224.148.2.10400 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:32.916420 193.224.148.2.41893 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:33.353407 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:33.510398 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
19:21:33.511392 193.224.148.2.3265 > 255.255.255.255.19: udp 0 (ttl 242, id 1)
```

The IP Address: 193.224.148.2 is inverse mapped to ns.szgti.kando.hu. The IP addresses ranging from 193.224.148.0 to 193.224.148.255 are owned by Institute of Computer Engineering, Kando Kalman Technical College, Hungary.

7. Evidence of active targeting:

The same scanning patterns was found on Subnet2. The source host is real. Both sources hosts probably are compromised by attackers to launch DoS on some victim.

8. Severity:

Component	Score	Reason
Criticality	4	No specific local servers are targeted. However acquiring knowledge of which hosts provide chargen service can be used to attack any hosts, internal or external.
Lethality	2	Local hosts may be identified and used as accomplices for DoS attacks toward themselves
System Countermeasures	4	Most hosts have disabled chargen TCP and UDP ports and echo ports as well
Network Countermeasures	0	No Firewall for the subnets to block TCP and UDP port 19.
Severity Score	2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Both TCP and UDP chargen ports should be disabled so that no host will become accomplices to DoS attacker. On Windows NT, "Simple TCP/IP Services" should be disabled from the network icon in the control panel.

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

a) the source host is spoofed
b) the source host is real
c) It is a chargen DoS attack on all subnet hosts.
d) It is a chargen DoS attack on the source host.

Answer: b

==========

Detect 4

==========

22:34:29.593042 210.110.247.244.4964 > 255.255.255.255.**32773: S** 3366586379:3366586379(0) win 32120 <mss 1460,sackOK,timestamp 5652020[|tcp]> (DF) (ttl 47, id 50215)
22:34:29.885647 210.110.247.244.1050 > Subnet2.189.32773: S 3360291041:3360291041(0) win 32120 <mss 1460,sackOK,timestamp 5652065[|tcp]> (DF) (ttl 47, id 50276)
22:34:29.886166 Subnet2.189.32773 > 210.110.247.244.1050: R 0:0(0) ack 3360291042 win 0 (ttl 128, id 36402)

1. Source of trace

This is detected on a Subnet2 on June 6, 2000

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n -x**

The format is: time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

The source host IP address does not inverse-map to a domain name. It is in the range 210.110.128.0 - 210.110.255.255 owned by KREONET , an ISP in Korea. Since an attempt was made to establish a TCP connection to probe a SunRPC port, the address was not spoofed.

4. Description of attack:

It is curious that there was no prior trace of any UDP probe for live portmap port (111) by utilities such as *rpcinfo* or *netbula* for Windows. The initial broadcast fishing for live 32773 port ended without responses. Subsequently, a TCP connection is attempted on high-number port (32773) of a specific host. It looks like the source host is determined to fish for live 32773 port. There are two possibilities: the source host either is looking for an RPC service to exploit or looking for certain planted trojan to link up.

5. Attack mechanism:

This intruder simply roams around probing for live RPC service at port 32773 on a potential victim. This trace actually shows that blocking portmap 111 at the router (no portmap 111 probe precedes the trace) does not discourage intruders from accessing RPC ports directly. The intruder may be looking for some RPC service to exploit. For example, some RPC daemon may let users exit to shell to execute arbitrary commands as the superuser. It is also possible that the intruder

is looking for or a possible trojan planted through some e-mail attachment at the target.

6. Correlations:

Since the destination host rejected the connection request, no related traffic is ever found since.

7. Evidence of active targeting:

Since Sun RPC use 32000 or higher port numbers, the intruder is targeting Unix-like or Linux hosts. The probe was for a specific target at a specific port. The act of bypassing portmap to access RPC service indicates that it is a deliberate probe.

8. Severity:

Component	Score	Reason
Criticality	5	A local host running IDS was targeted.
Lethality	1	If RPC service is live at 32773, it may be exploited. If a trojan was planted, then the finding of trojan port is lethal
System Countermeasures	5	The destination host has been configured as an IDS, not to respond to most of the services.
Network Countermeasures	0	No Firewall or router to block high-number TCP and UDP ports
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

High-number port RPC services should be closed or filtered at the router.

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

a) A corrupted packet gone astray
b) A deliberate probe for a well-known RPC service
c) A deliberate probe for a Windows target
d) A deliberate probe for a Unix target

Answer: d

==========

Detect 5

==========

```
00:16:03.685947 207.174.228.81.111 > 255.255.255.255.111: SF 1081904820:1081904820(0)
win 1028 (ttl 30, id 39426)
00:16:03.744441 207.174.228.81.111 > Subnet1.3.111: SF 1081904820:1081904820(0) win
1028 (ttl 30, id 39426)
00:16:03.771940 207.174.228.81.111 > Subnet1.4.111: SF 1081904820:1081904820(0) win
1028 (ttl 30, id 39426)
00:16:03.784940 207.174.228.81.111 > Subnet1.5.111: SF 1081904820:1081904820(0) win
1028 (ttl 30, id 39426)
00:16:03.804438 207.174.228.81.111 > Subnet1.6.111: SF 1081904820:1081904820(0) win
1028 (ttl 30, id 39426)
```

00:16:04.235415 207.174.228.81.111 > Subnet1.26.111: SF 1081904820:1081904820(0) win 1028 (ttl 30, id 39426)
00:16:04.235529 Subnet1.26.111 > 207.174.228.81.111: R 0:0(0) ack 1081904822 win 0 (ttl 128, id 32426)
00:16:06.085824 207.174.228.81.111 > Subnet1.120.111: SF 481594681:481594681(0) win 1028 (ttl 30, id 39426)
00:16:06.086631 Subnet1.120.111 > 207.174.228.81.111: S 2450796248:2450796248(0) ack 481594682 win 32696 <mss 536> (DF) (ttl 64, id 1243)
00:16:06.141522 207.174.228.81.111 > Subnet1.120.111: R 481594682:481594682(0) win 0 (ttl 243, id 14057)
00:16:06.225318 207.174.228.81.111 > 255.255.255.255.111: SF 481594681:481594681(0) win 1028 (ttl 30, id 39426)
00:16:06.231327 207.174.228.81.2253 > Subnet1.120.111: S 1866959324:1866959324(0) win 32120 <mss 1460,sackOK,timestamp 70578858[|tcp]> (DF) (ttl 52, id 14065)
00:16:06.231662 Subnet1.120.111 > 207.174.228.81.2253: S 2439339937:2439339937(0) ack 1866959325 win 32120 <mss 1460,sackOK,timestamp 29467498[|tcp]> (DF) (ttl 64, id 1244)
00:16:06.288263 207.174.228.81.2253 > Subnet1.120.111: . ack 1 win 32120 <nop,nop,timestamp 70578864 29467498> (DF) (ttl 52, id 14075)
00:16:06.288317 207.174.228.81.951 > Subnet1.120.111: S 1866927620:1866927620(0) win 32120 <mss 1460,sackOK,timestamp 70578864[|tcp]> (DF) (ttl 52, id 14076)
00:16:06.288769 Subnet1.120.111 > 207.174.228.81.951: S 2438684520:2438684520(0) ack 1866927621 win 32120 <mss 1460,sackOK,timestamp 29467504[|tcp]> (DF) (ttl 64, id 1245)
00:16:06.341523 207.174.228.81.951 > Subnet1.120.111: . ack 1 win 32120 <nop,nop,timestamp 70578869 29467504> (DF) (ttl 52, id 14078)
00:16:06.341847 207.174.228.81.951 > Subnet1.120.111: P 1:45(44) ack 1 win 32120 <nop,nop,timestamp 70578869 29467504> (DF) (ttl 52, id 14079)
00:16:06.342231 Subnet1.120.111 > 207.174.228.81.951: . ack 45 win 32120 <nop,nop,timestamp 29467509 70578869> (DF) (ttl 64, id 1246)
00:16:06.343489 Subnet1.120.111 > 207.174.228.81.951: P 1:73(72) ack 45 win 32120 <nop,nop,timestamp 29467509 70578869> (DF) (ttl 64, id 1247)
00:16:06.396289 207.174.228.81.951 > Subnet1.120.111: . ack 73 win 32120 <nop,nop,timestamp 70578875 29467509> (DF) (ttl 52, id 14081)
00:16:06.396327 207.174.228.81.951 > Subnet1.120.111: F 45:45(0) ack 73 win 32120 <nop,nop,timestamp 70578875 29467509> (DF) (ttl 52, id 14082)
00:16:06.396741 Subnet1.120.111 > 207.174.228.81.951: . ack 46 win 32120 <nop,nop,timestamp 29467515 70578875> (DF) (ttl 64, id 1248)
00:16:06.396989 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29467515 70578875> (DF) (ttl 64, id 1249)
00:16:06.397807 207.174.228.81.2253 > Subnet1.120.111: F 1:1(0) ack 1 win 32120 <nop,nop,timestamp 70578875 29467498> (DF) (ttl 52, id 14087)
00:16:06.398140 Subnet1.120.111 > 207.174.228.81.2253: . ack 2 win 32120 <nop,nop,timestamp 29467515 70578875> (DF) (ttl 64, id 1250)
00:16:06.398336 Subnet1.120.111 > 207.174.228.81.2253: F 1:1(0) ack 2 win 32120 <nop,nop,timestamp 29467515 70578875> (DF) (ttl 64, id 1251)
00:16:06.465423 207.174.228.81.2253 > Subnet1.120.111: . ack 2 win 32120 <nop,nop,timestamp 70578880 29467515> (DF) (ttl 52, id 14089)
00:16:06.914232 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29467567 70578875> (DF) (ttl 64, id 1252)
00:16:07.954322 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29467671 70578875> (DF) (ttl 64, id 1253)
00:16:10.034516 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29467879 70578875> (DF) (ttl 64, id 1254)
00:16:14.194893 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29468295 70578875> (DF) (ttl 64, id 1255)
00:16:22.515668 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29469127 70578875> (DF) (ttl 64, id 1256)

00:16:39.157185 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29470791 70578875> (DF) (ttl 64, id 1257)
00:17:12.440267 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29474119 70578875> (DF) (ttl 64, id 1258)
00:18:19.006388 Subnet1.120.111 > 207.174.228.81.951: F 73:73(0) ack 46 win 32120 <nop,nop,timestamp 29480775 70578875> (DF) (ttl 64, id 1259)
00:18:19.061198 207.174.228.81.951 > Subnet1.120.111: R 1866927666:1866927666(0) win 0 (ttl 243, id 17952)

1. Source of trace

This is detected on Subnet1 on June 4, 2000.

2. Detect was generated by:

windump -vv -n -x

time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

The host name is "is.the.administrator.of.aekpani.net", an ISP site address. Since the site is an ISP "administrator" site, it must be live all the time. In addition, this three-way TCP handshaking to collect RPC service information can not take place without the real IP address used. Therefore, there is no chance of IP-spoofing.

4. Description of attack:

On June 4, 2000, the traffic pattern showed that there was an initial SYN/FIN RPC-portmap (TCP port 111) scan to look for a Unix-like box on Subnet1. Hosts in Subnet1: Subnet1.3, Subnet1.4, Subnet1.5, Subnet1.6, Subnet1.26, Subnet1.120 were all SYN/FIN scanned. Since Subnet1.120 is a Linux box (Redhat Linux 6.0), TCP connection was initiated and some data were pushed from the source to Subnet1.120. A e-mail was sent to the System Administrator of the source host for explanation, e-mail was bounced-back.

5. Attack mechanism:

The SYN/FIN flag combination is used to avoid being detected by old IDS which only looks for SYN flag alone. It is a stealth host scan crafted by some script. This is a scripted probe looking for hosts with live 111 port to return a RST response. The intruder succeeded in getting a RST from Subnet1.120. It immediately launched a TCP connection to look for RPC services. An exchange took place, the intruder succeeded in getting some RPC service information. Later on, the Linux box mysteriously crashed during the time IDS station was not sniffing. There was no data to examine whether RPC-related exploits were launched later causing the crash. The Linux box running on a Pentium Pro 180 was maintained by a person who has since left. No detailed information was available on the box.

6. Correlations:

Shortly after on the same day, a similar trace was collected from a different IDS monitoring Subnet2. Since there is no Unix or Linux box on Subnet2, the SYN/FIN traffic ended quickly.

```
00:24:47.533229 207.174.228.81.111 > 255.255.255.255.111: SF 481594681:481594681(0) win
1028 (ttl 30, id 39426)
00:24:48.755727 207.174.228.81.111 > Subnet2.189.111: SF 1241481493:1241481493(0) win
1028 (ttl 30, id 39426)
00:24:48.756736 Subnet2.189.111 > 207.174.228.81.111: R 0:0(0) ack 1241481495 win 0 (ttl
128, id 29196)
00:24:50.072740 207.174.228.81.111 > 255.255.255.255.111: SF 1708688560:1708688560(0)
win 1028 (ttl 30, id 39426)
```

There was no further related traffic after that.

7. Evidence of active targeting:

First a network scan is conducted, then followed by specific targeting going after a system with portmap port open. Once it is found, RPC service information was collected. It is a calculated active targeting.

8. Severity:

Component	Score	Reason
Criticality	5	Specific local servers with SunRPC service found.
Lethality	5	Hosts was targeted for DoS attacks
System Countermeasures	0	The Linux box was installed and maintained by students who did not harden the default Linux installation
Network Countermeasures	0	No Firewall for the subnets to block TCP and UDP port 19.
Severity Score	10	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Port 111 scan can be easily blocked by a router. SYN/FIN scan can be blocked by newer firewalls.

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

a) DoS attack
b) Host Scan
c) Port Scan
d) Normal Traffic

Answer: a

==========

Detect 6

==========

22:56:28.120400 204.176.151.58 > 255.255.255.255: icmp: echo request (ttl 28, id 19500)
22:56:28.121671 204.176.151.58.35397 > 255.255.255.255.80: . ack 1782248661 win 2048 (ttl 25, id 40138)

1. Source of trace

This is detected on Subnet2 on June 5, 2000.

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n -x**

The format of the trace:

time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

No, the source address is not spoofed, since it is an obvious host scan for hosts with live HTTP port 80. The IP address 204.176.151.58 can not be inverse-mapped to any domain name. The IP addresses ranging from 204.176.0.0 to 204.179.255.0 are owned by UUNET Technologies, Inc.

4. Description of attack:

The source host first used Ping to find live hosts in our subnet, then sent a TCP packet of broadcast "ack" to all hosts for live port 80. If a destination host receive an "ack" packet without any existing TCP connection, it will quickly send a RST packet. If the port 80 is not open, then a "connection refused" message will be returned. The RST packets may provide clue to which host may have live 80 port open and which Web server is running. This probe with "ack" packet is considered as a "stealth" host scan, since it tried to avoid firewall filter that blocks all incoming SYN

5. Attack mechanism:

It is a crafted packet used in a very subtle way to avoid detection by old firewalls. The intention of this probe can not be honorable, since no one accesses Web server this way. The intruder may be tempted to try CGI-exploits on web servers he/she can find and get a root shell to take control of the server.

6. Correlations:

Two days later on June 7, 2000, the same traffic pattern reappeared on the same Subnet2

23:25:40.753708 204.176.151.58 > 255.255.255.255: icmp: echo request (ttl 33, id 28347)
23:25:40.755563 204.176.151.58.44620 > 255.255.255.255.80: . ack 4070098745 win 4096 (ttl 31, id 62616)

4500 0028 f498 0000 1f06 434d ccb0 973a
ffff ffff ae4c 0050 b0d0 1183 f298 c739

5010 1000 d8b7 0000 0000 0000 0000

7. Evidence of active targeting:

The intruder is looking for hidden web servers.

8. Severity:

Component	Score	Reason
Criticality	4	There is a web server (that Linux box!) on Subnet1.
Lethality	0	Web server is usually accessible from the Internet
System Countermeasures	3	Since there is a main web server elsewhere, most other workstations do not run web server.
Network Countermeasures	0	No Firewall for the subnets to block TCP and UDP port 80
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

It uses ACK to bypass old IDS or firewall. Therefore, a stateful inspection firewall should be used to keep track of a session state.

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

a) a normal HTTP traffic
b) a normal TCP connection
c) a host scan which may be easily blocked by a firewall
d) a host scan which may easily pass through a firewall

Answer: d

==========

Detect 7

==========

02:57:13.376842 **cdm94-044.silo.tcainternet.com.137 > Subnet1.3.137:** udp 50 (ttl 112, id 64107)
02:57:23.902819 cdm94-044.silo.tcainternet.com.137 > Subnet1.**4.137:** udp 50 (ttl 112, id 364)
02:57:34.423295 cdm94-044.silo.tcainternet.com.137 > Subnet1.**5.137**: udp 50 (ttl 112, id 2156)
02:57:44.939267 cdm94-044.silo.tcainternet.com.137 > Subnet1.**6.137**: udp 50 (ttl 112, id 3948)
03:01:15.764750 cdm94-044.silo.tcainternet.com.137 > **Subnet1.26.137**: udp 50 (ttl 112, id 43116)
03:01:15.764908 Subnet1.26.137 > cdm94-044.silo.tcainternet.com.137: udp 265 (ttl 128, id 45380)
03:01:15.860745 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: S 136234351:136234351(0) win 8192 <mss 1460,nop,nop,sackOK> (DF) (ttl 112, id 43372)
03:01:15.860873 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: S 70497:70497(0) ack 136234352 win 8760 <mss 1460> (DF) (ttl 128, id 45636)
03:01:15.942240 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: . ack 1 win 8760 (DF) (ttl 112, id 43628)
03:01:15.977749 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: P 1:73(72) ack 1 win 8760 (DF) (ttl 112, id 43884)
03:01:15.977888 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: P 1:5(4) ack 73 win 8688 (DF) (ttl 128, id 45892)
03:01:16.069256 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: P 73:231(158) ack 5 win 8756 (DF) (ttl 112, id 44140)

03:01:16.069418 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: P 5:108(103) ack 231 win 8530 (DF) (ttl 128, id 46148)
03:01:16.165750 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: P 231:386(155) ack 108 win 8653 (DF) (ttl 112, id 44396)
03:01:16.292953 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: . ack 386 win 8375 (DF) (ttl 128, id 46404)
03:01:19.187232 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: P 108:147(39) ack 386 win 8375 (DF) (ttl 128, id 46660)
03:01:19.373069 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: . ack 147 win 8614 (DF) (ttl 112, id 44908)
03:01:19.643557 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: F 386:386(0) ack 147 win 8614 (DF) (ttl 112, id 45164)
03:01:19.643678 Subnet1.26.139 > cdm94-044.silo.tcainternet.com.1815: F 147:147(0) ack 387 win 8375 (DF) (ttl 128, id 46916)
03:01:19.720551 cdm94-044.silo.tcainternet.com.1815 > Subnet1.26.139: . ack 148 win 8614 (DF) (ttl 112, id 45420)
03:18:46.994848 cdm94-044.silo.tcainternet.com.137 > 255.255.255.255.137: udp 50 (ttl 112, id 4976)
03:18:48.492267 cdm94-044.silo.tcainternet.com.137 > 255.255.255.255.137: udp 50 (ttl 112, id 5232)
03:18:49.998690 cdm94-044.silo.tcainternet.com.137 > 255.255.255.255.137: udp 50 (ttl 112, id 5488)

1. Source of trace

This is detected on Subnet1 on May 30, 2000.

2. Detect was generated by:

First, WinDump (tcpdump for Windows) was used: **windump -vv -n** . After the suspicious traffic was found (as shown), **windump -vv -n -x** was used, since May 30, 2000.

The format of the trace:

time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

Since an attempt to establish TCP connection was shown to push some kind of information, the address was not spoofed. The Domain name CDM94-044.SILO.TCAINTERNET.COM is mapped to IP Address: 207.50.94.44. The IP addresses ranging from 207.50.80.0 - 207.50.95.255 are owned by Cable & Wireless USA.

During the Memorial Day weekend, several similar intrusions were detected (Please see the ***Correlations*** section). The following source names were found:

Domain name CTS01.CBU.SKYINET.NET is mapped to IP Address: 208.142.164.25. The IP addresses ranging from 208.142.160.0 - 208.142.167.255 are owned by Cable & Wireless USA.
Domain name DIALUP-166.90.234.41.DETROIT1.LEVEL3.NET is mapped to IP Address: 166.90.234.41. The IP addresses ranging from 166.90.0.0 - 166.90.255.255 are owned by Level 3 Communications.

Domain name p209-pm9.integrityonline32.com is mapped to IP Address: 216.136.36.210. The IP addresses ranging from 216.136.32.0 - 216.136.63.255 are owned by Time Warner Telecom, Inc.

4. Description of attack:

The same site Subnet1.26 was repeatedly hit as shown in ***Correlations*** section. However, all hits were preceded by host scans as if these are separate incidences.

Port 137 to port 137 UDP communication, especially with length 50, is typically a NetBIOS name query. However, this type of traffic coming from the Internet is an indication that someone is trying to find unprotected Windows shares. Since Subnet1 is a subnet BAT_CHODE911 is know to probe, this could also be something much more vicious, like a BAT_CHODE911 trojan worm hunting for Windows shares with write access to copy itself over. Once BAT_CHODE911 infected the share, it will dial 911 through the modem and the format all hard drives. (http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=BAT_CHODE911&VSect=T)

5. Attack mechanism:

The sequential host scan pattern, with different ID numbers, indicates that it is run by a script. Once the share is found, the script will proceed to start TCP connection. The traffic may indicate that the share is protected and the attacking script is trying to log in a few times. If not successful, it will start to scan the subnet again. There has been an increase in 137 port probing activity from the Internet as indicated by Bryce Alexander that the increase may be attributed to the popularity of NBTSTAT and the spread of network.vbs worm.

6. Correlations:

A few days later, the same type of traffic was found in several occasions from different hosts on different subnets.

----------On May 31, Subnet1----------

02:30:25.744176 cts01.cbu.skyinet.net.137 > Subnet1.**3.137**: udp 50 (ttl 114, id 23636)
02:30:30.402940 cts01.cbu.skyinet.net.137 > Subnet1.**4.137**: udp 50 (ttl 114, id 24404)
02:30:34.236248 cts01.cbu.skyinet.net.137 > Subnet1.**5.137**: udp 50 (ttl 114, id 24916)
02:30:38.753027 cts01.cbu.skyinet.net.137 > Subnet1.**6.137**: udp 50 (ttl 114, id 26708)
02:32:22.451305 cts01.cbu.skyinet.net.4994 > **Subnet1.26.139: S** 16523424:16523424(0) win 8192 <mss 1460,nop,wscale 0,nop,nop,timestamp[|tcp]> (DF) [tos **0x57**] (ttl 114, id 12117)

4557 0040 2f55 4000 7206 2cda d08e a419
c76f 701a 1382 008b 00fc 20a0 0000 0000
b002 2000 3426 0000 0204 05b4 0103 0300
0101 080a 0000

(Notice that the type of Service 0x57 is unusual, since it is not normal to specify maximize throughput and minimize monetary cost of high priority)

02:32:22.451397 Subnet1.26.edu.139 > cts01.cbu.skyinet.net.4994: **S** 70563:70563(0) **ack** 16523425 win 8760 <mss 1460> (DF) (ttl 128, id 1999)
02:32:23.227781 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: **P** 1:73(72) ack 1 win 8760 (DF) [**tos 0x57]** (ttl 114, id 12629)

4557 0070 3155 4000 7206 2aaa d08e a419
c76f 701a 1382 008b 00fc 20a1 0001 13a4

5018 2238 44fc 0000 8100 0044 2046 4446
4545 4245 4f45
02:32:23.227919 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: P 1:5(4) ack 73 win 8688 (DF) (ttl 128, id 2255)
02:32:26.192354 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: P 1:5(4) ack 73 win 8688 (DF) (ttl 128, id 3791)
02:32:26.804101 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: P 1:73(72) ack 1 win 8760 (DF) [tos 0x57] (ttl 114, id 13141)
4557 0070 3355 4000 7206 28aa d08e a419
c76f 701a 1382 008b 00fc 20a1 0001 13a4
5018 2238 44fc 0000 8100 0044 2046 4446
4545 4245 4f45
02:32:26.804158 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: . ack 73 win 8688 (DF) (ttl 128, id 4047)
02:32:26.844111 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: P 73:231(158) ack 5 win 8756 (DF) [tos 0x57] (ttl 114, id 13397)
4557 00c6 3455 4000 7206 2754 d08e a419
c76f 701a 1382 008b 00fc 20e9 0001 13a8
5018 2234 7049 0000 0000 009a ff53 4d42
7200 0000 0000
02:32:26.844293 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: P 5:108(103) ack 231 win 8530 (DF) (ttl 128, id 4303)
02:32:27.539583 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: P 231:386(155) ack 108 win 8653 (DF) [tos 0x57] (ttl 114, id 13653)
4557 00c3 3555 4000 7206 2657 d08e a419
c76f 701a 1382 008b 00fc 2187 0001 140f
5018 21cd 99c0 0000 0000 0097 ff53 4d42
7300 0000 0010
02:32:27.694521 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: . ack 386 win 8375 (DF) (ttl 128, id 5071)
02:32:30.608825 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: P 108:147(39) ack 386 win 8375 (DF) (ttl 128, id 6863)
02:32:31.286864 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: . ack 147 win 8614 (DF) [tos 0x57] (ttl 114, id 14165)
4557 0028 3755 4000 7206 24f2 d08e a419
c76f 701a 1382 008b 00fc 2222 0001 1436
5010 21a6 969a 0000 0000 0000 0000
02:32:31.494854 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: F 386:386(0) ack 147 win 8614 (DF) [tos 0x57] (ttl 114, id 14421)
4557 0028 3855 4000 7206 23f2 d08e a419
c76f 701a 1382 008b 00fc 2222 0001 1436
5011 21a6 9699 0000 0000 0000 0000
02:32:31.494954 Subnet1.26.139 > cts01.cbu.skyinet.net.4994: F 147:147(0) ack 387 win 8375 (DF) (ttl 128, id 7887)
02:32:32.072327 cts01.cbu.skyinet.net.4994 > Subnet1.26.139: . ack 148 win 8614 (DF) [tos 0x57] (ttl 114, id 14677)
----------On May 31, Subnet1----------
03:23:53.149128 **dialup-166.90.234.41.Detroit1.Level3.net.137 > Subnet1.3.137**: udp 50 (ttl 120, id 64302)
03:24:03.678606 dialup-166.90.234.41.Detroit1.Level3.net.137 > Subnet1.**4.137**: udp 50 (ttl 120, id 5167)
03:24:14.208578 dialup-166.90.234.41.Detroit1.Level3.net.137 > Subnet1.**5.137**: udp 50 (ttl 120, id 9519)
03:24:25.957489 dialup-166.90.234.41.Detroit1.Level3.net.137 > Subnet1.**6.137**: udp 50 (ttl 120, id 13871)

03:29:29.753781 dialup-166.90.234.41.Detroit1.Level3.net.137 > **Subnet1.26.137**: udp 50 (ttl 120, id 59184)
03:29:29.753919 Subnet1.26.137 > dialup-166.90.234.41.Detroit1.Level3.net.137: udp 265 (ttl 128, id 46289)
03:29:31.763660 dialup-166.90.234.41.Detroit1.Level3.net.137 > Subnet1.26.137: udp 50 (ttl 120, id 61488)
03:29:31.763759 Subnet1.26.137 > dialup-166.90.234.41.Detroit1.Level3.net.137: udp 265 (ttl 128, id 47569)
03:29:31.983648 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: **S** 118543928:118543928(0) win 8192 <mss 536,nop,nop,sackOK> (DF) (ttl 120, id 61744)
4500 0030 f130 4000 7806 4989 a65a ea29
c76f 701a 0abe 008b 0710 d638 0000 0000
7002 2000 b61b 0000 0204 0218 0101 0402
03:29:31.983745 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: S 70576:70576(0) ack 118543929 win 8576 <mss 1460> (DF) (ttl 128, id 47825)
03:29:32.193636 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: . ack 1 win 8576 (DF) (ttl 120, id 62000)
03:29:32.194137 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: P 1:73(72) ack 1 win 8576 (DF) (ttl 120, id 62256)
03:29:32.194253 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: P 1:5(4) ack 73 win 8504 (DF) (ttl 128, id 48081)
03:29:32.514119 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: . ack 5 win 8572 (DF) (ttl 120, id 62512)
03:30:15.811997 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: P 73:231(158) ack 5 win 8572 (DF) (ttl 120, id 5425)
03:30:15.812337 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: P 5:108(103) ack 231 win 8346 (DF) (ttl 128, id 52689)
03:30:16.051982 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: P 231:387(156) ack 108 win 8469 (DF) (ttl 120, id 5681)
03:30:16.181447 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: . ack 387 win 8190 (DF) (ttl 128, id 52945)
03:30:19.075751 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: P 108:147(39) ack 387 win 8190 (DF) (ttl 128, id 53201)
03:30:19.381791 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: . ack 147 win 8430 (DF) (ttl 120, id 6193)
03:30:20.241751 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: F 387:387(0) ack 147 win 8430 (DF) (ttl 120, id 6449)
03:30:20.241886 Subnet1.26.139 > dialup-166.90.234.41.Detroit1.Level3.net.2750: F 147:147(0) ack 388 win 8190 (DF) (ttl 128, id 53457)
03:30:20.431738 dialup-166.90.234.41.Detroit1.Level3.net.2750 > Subnet1.26.139: . ack 148 win 8430 (DF) (ttl 120, id 6705)
04:06:12.760526 dialup-166.90.234.41.Detroit1.Level3.net.137 > 255.255.255.255.137: udp 50 (ttl 120, id 3388)
04:06:14.243942 dialup-166.90.234.41.Detroit1.Level3.net.137 > 255.255.255.255.137: udp 50 (ttl 120, id 3900)
04:06:15.750367 dialup-166.90.234.41.Detroit1.Level3.net.137 > 255.255.255.255.137: udp 50 (ttl 120, id 6204)

----------On June 1, Subnet1----------

04:45:56.960158 **p209-pm9.integrityonline32.com.137 > Subnet1.3.137**: udp 50 (ttl 113, id 28924)
04:46:04.511275 p209-pm9.integrityonline32.com.137 > Subnet1.**4.137**: udp 50 (ttl 113, id 30972)
04:46:12.010398 p209-pm9.integrityonline32.com.137 > Subnet1.**5.137:** udp 50 (ttl 113, id 33020)
04:46:19.533526 p209-pm9.integrityonline32.com.137 > Subnet1.**6.137**: udp 50 (ttl 113, id 35068)

04:50:29.773020 p209-pm9.integrityonline32.com.137 > **Subnet1.26.137**: udp 50 (ttl 113, id 27390)
04:50:29.773159 Subnet1.26.137 > p209-pm9.integrityonline32.com.137: udp 265 (ttl 128, id 55178)
04:50:31.265444 p209-pm9.integrityonline32.com.137 > Subnet1.26.137: udp 50 (ttl 113, id 27902)
04:50:31.265577 Subnet1.26.137 > p209-pm9.integrityonline32.com.137: udp 265 (ttl 128, id 55434)
04:50:31.574403 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: S 27190679:27190679(0) win 8192 <mss 536,nop,nop,sackOK> (DF) (ttl 113, id 28158)

4500 0030 6dfe 4000 7106 66e5 d888 24d2
c76f 701a 085d 008b 019e e597 0000 0000
7002 2000 41b9 0000 0204 0218 0101 0402

04:50:31.574516 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: S 70788:70788(0) ack 27190680 win 8576 <mss 1460> (DF) (ttl 128, id 55690)
04:50:31.885388 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: . ack 1 win 8576 (DF) (ttl 113, id 28414)
04:50:31.885941 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: P 1:73(72) ack 1 win 8576 (DF) (ttl 113, id 28670)
04:50:31.886071 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: P 1:5(4) ack 73 win 8504 (DF) (ttl 128, id 55946)
04:50:32.300366 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: . ack 5 win 8572 (DF) (ttl 113, id 28926)
04:51:15.069363 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: P 73:231(158) ack 5 win 8572 (DF) (ttl 113, id 56830)
04:51:15.069750 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: P 5:108(103) ack 231 win 8346 (DF) (ttl 128, id 56202)
04:51:15.438347 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: P 231:390(159) ack 108 win 8469 (DF) (ttl 113, id 57086)
04:51:15.625364 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: . ack 390 win 8187 (DF) (ttl 128, id 56458)
04:51:18.439585 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: P 108:147(39) ack 390 win 8187 (DF) (ttl 128, id 56714)
04:51:18.811047 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: . ack 147 win 8430 (DF) (ttl 113, id 57598)
04:51:18.964037 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: F 390:390(0) ack 147 win 8430 (DF) (ttl 113, id 57854)
04:51:18.964153 Subnet1.26.139 > p209-pm9.integrityonline32.com.2141: F 147:147(0) ack 391 win 8187 (DF) (ttl 128, id 56970)
04:51:19.254022 p209-pm9.integrityonline32.com.2141 > Subnet1.26.139: . ack 148 win 8430 (DF) (ttl 113, id 58110)

----------On June 1, Subnet1, a different host----------

05:21:38.389771 **p209-pm9.integrityonline32.com.137 > Subnet1.120.137:** udp 50 (ttl 113, id 32013)
05:21:38.391006 Subnet1.120.137 > p209-pm9.integrityonline32.com.137: udp 229 (ttl 64, id
05:21:39.907196 p209-pm9.integrityonline32.com.137 > Subnet1.120.137: udp 50 (ttl 113, id 33549)
05:21:39.908278 Subnet1.120.137 > p209-pm9.integrityonline32.com.137: udp 229 (ttl 64, id 273)
05:21:40.216151 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: S 29058032:29058032(0) win 8192 <mss 536,nop,nop,sackOK> (DF) (ttl 113, id 33805)
05:21:40.216909 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: S 1538105016:1538105016(0) ack 29058033 win 32696 <mss 536,nop,nop,sackOK> (DF) (ttl 64, id 274)
05:21:40.530634 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: . ack 1 win 8576 (DF) (ttl 113, id 34061)

05:21:40.531186 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: P 1:73(72) ack 1 win 8576 (DF) (ttl 113, id 34317)

4500 0070 860d 4000 7106 4e38 d888 24d2
c76f 7078 0a03 008b 01bb 63f1 5bad 9eb9
5018 2180 d967 0000 8100 0044 2046 4945
4e45 4d44 4243

05:21:40.531572 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: . ack 73 win 32624 (DF) (ttl 64, id 275)
05:21:40.696965 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: P 1:5(4) ack 73 win 32696 (DF) (ttl 64, id 277)
05:21:41.185110 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: . ack 5 win 8572 (DF) (ttl 113, id 36365)
05:22:23.807611 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: P 73:231(158) ack 5 win 8572 (DF) (ttl 113, id 54029)
05:22:23.808581 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: P 5:86(81) ack 231 win 32696 (DF) (ttl 64, id 278)
05:22:24.140390 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: P 231:357(126) ack 86 win 8491 (DF) (ttl 113, id 54797)
05:22:24.147252 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: P 86:125(39) ack 357 win 32696 (DF) (ttl 64, id 279)
05:22:24.642432 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: . ack 125 win 8452 (DF) (ttl 113, id 56333)
05:22:24.912419 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: F 357:357(0) ack 125 win 8452 (DF) (ttl 113, id 57101)
05:22:24.912729 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: . ack 358 win 32696 (DF) (ttl 64, id 280)
05:22:24.912920 Subnet1.120.139 > p209-pm9.integrityonline32.com.2563: F 125:125(0) ack 358 win 32696 (DF) (ttl 64, id 281)
05:22:25.261897 p209-pm9.integrityonline32.com.2563 > Subnet1.120.139: . ack 126 win 8452 (DF) (ttl 113, id 58125)
05:23:12.788058 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 25614)
05:23:12.789326 Subnet1.120.137 > p209-pm9.integrityonline32.com.137: udp 229 (ttl 64, id 282)
05:23:14.275981 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 26126)
05:23:14.277063 Subnet1.120.137 > p209-pm9.integrityonline32.com.137: udp 229 (ttl 64, id 283)
05:23:15.779907 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 26638)
05:23:15.780988 Subnet1.120.137 > p209-pm9.integrityonline32.com.137: udp 229 (ttl 64, id 284)

----------On June 1, Subnet2----------

(Notice the broadcast-scan)

05:31:48.170715 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 30990)
05:31:49.671735 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 33550)
05:31:51.184250 p209-pm9.integrityonline32.com.137 > 255.255.255.255.137: udp 50 (ttl 113, id 36622)

(Attack begins)

06:10:21.607837 p209-pm9.integrityonline32.com.137 > Subnet2.189.137: udp 50 (ttl 113, id 13878)
06:10:21.607969 Subnet2.189.137 > p209-pm9.integrityonline32.com.137: udp 247 (ttl 128, id 47555)

06:10:23.111853 p209-pm9.integrityonline32.com.137 > Subnet2.189.137: udp 50 (ttl 113, id 16950)
06:10:23.111993 Subnet2.189.137 > p209-pm9.integrityonline32.com.137: udp 247 (ttl 128, id 48323)
06:10:23.436823 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: S 31468015:31468015(0) win 8192 <mss 536,nop,nop,sackOK> (DF) (ttl 113, id 17206)

4500 0030 4336 4000 7106 910a d888 24d2
c76f 70bd 0d86 008b 01e0 29ef 0000 0000
7002 2000 f753 0000 0204 0218 0101 0402

06:10:23.436935 Subnet2.189.139 > p209-pm9.integrityonline32.com.3462: S 447852:447852(0) ack 31468016 win 8576 <mss 1460> (DF) (ttl 128, id 48579)
06:10:23.778813 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: . ack 1 win 8576 (DF) (ttl 113, id 17462)
06:10:23.780371 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: P 1:73(72) ack 1 win 8576 (DF) (ttl 113, id 17718)
06:10:23.780486 Subnet2.189.139 > p209-pm9.integrityonline32.com.3462: P 1:5(4) ack 73 win 8504 (DF) (ttl 128, id 48835)
06:10:24.185836 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: . ack 5 win 8572 (DF) (ttl 113, id 17974)
06:11:10.921137 Subnet2.189.139 > p209-pm9.integrityonline32.com.3462: P 106:145(39) ack 380 win 8197 (DF) (ttl 128, id 63171)
06:11:11.288672 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: . ack 145 win 8432 (DF) (ttl 113, id 21046)
06:11:12.039692 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: F 380:380(0) ack 145 win 8432 (DF) (ttl 113, id 21302)
06:11:12.039832 Subnet2.189.139 > p209-pm9.integrityonline32.com.3462: F 145:145(0) ack 381 win 8197 (DF) (ttl 128, id 63427)
06:11:12.328182 p209-pm9.integrityonline32.com.3462 > Subnet2.189.139: . ack 146 win 8432 (DF) (ttl 113, id 21558)

7. Evidence of active targeting:

It is actively seeking Windows hosts with unprotected shares.

8. Severity:

Component	Score	Reason
Criticality	5	All hosts were targeted.
Lethality	5	Hosts offering shares were identified and access to the share followed
System Countermeasures	0	Hosts may have the default NT installation setting without system hardening
Network Countermeasures	0	No Firewall to block incoming TCP/UDP ports 137, 138 or 139.
Severity Score	10	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Ports 137, 138, and 139 should be blocked by firewalls. All Windows shares should be protected.

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

a) Targeting Windows hosts
b) Targeting Unix hosts
c) Targeting a trojan port
d) Targeting a SunRPC port

Answer: a

==========

Detect 8

==========

```
----------Group of three SYN---------------------------------
18:36:22.479043 www.rivalcom.net.2400 > Subnet1.120.53: S 1619040197:1619040261(64) win
2048 (ttl 244, id 21821)
                                4500 0068 553d 0000 f406 ec7d d143 7ba9
                                c76f 7078 0960 0035 6080 97c5 0000 0000
                                5002 0800 20f3 0000 0000 0000 0000 0000
                                0000 0000 0000
18:36:22.479192 www.rivalcom.net.2401 > Subnet1.120.53: S 2104147424:2104147488(64) win
2048 (ttl 244, id 27187)
18:36:22.479313 www.rivalcom.net.2402 > Subnet1.120.53: S 628255776:628255840(64) win
2048 (ttl 244, id 23392)
---------Group of three SYN/ACK-------------------------
18:36:22.481571 Subnet1.120.53 > www.rivalcom.net.2402: S 3595354950:3595354950(0) ack
628255777 win 32160 <mss 536> (DF) (ttl 64, id 134)
18:36:22.481695 Subnet1.120.53 > www.rivalcom.net.2401: S 3607420219:3607420219(0) ack
2104147425 win 32160 <mss 536> (DF) (ttl 64, id 133)
18:36:22.481820 Subnet1.120.53 > www.rivalcom.net.2400: S 3603484574:3603484574(0) ack
1619040198 win 32160 <mss 536> (DF) (ttl 64, id 132)
---------Group of three normal RST--------------------
18:36:22.558683 www.rivalcom.net.2402 > Subnet1.120.53: R 628255777:628255777(0) win 0
(ttl 53, id 52347)
18:36:22.558741 www.rivalcom.net.2401 > Subnet1.120.53: R 2104147425:2104147425(0) win 0
(ttl 53, id 52349)
18:36:22.559000 www.rivalcom.net.2400 > Subnet1.120.53: R 1619040198:1619040198(0) win 0
(ttl 53, id 52351)
------- Group of three RST/ACK-------------------------
18:36:22.559067 www.rivalcom.net.2402 > Subnet1.120.53: R 1:1(0) ack 1 win 2048 (ttl 244, id
63728)
18:36:22.559254 www.rivalcom.net.2401 > Subnet1.120.53: R 1:1(0) ack 1 win 2048 (ttl 244, id
53593)
18:36:22.559756 www.rivalcom.net.2400 > Subnet1.120.53: R 1:1(0) ack 1 win 2048 (ttl 244, id
13852)
(6 more identical cycles)
```

1. Source of trace

This is detected on Subnet1 on May 31, 2000.

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -x**

The format of the trace:

time, src.port > dst.port , TCP flags, begin-sequence number: end-sequence number (payload size), window size (time-to-live, ID#)

3. Probability the source address was spoofed

The source domain name is mapped to 209.67.123.171. The IP address ranging from 209.67.0.0 to 209.67.255.255 are owned by Exodus Communications Inc. At the first glance, the intruder is actively searching for DNS server. If it is really the case, then the source domain name is not spoofed. However, there is a remote possibility that the source domain name is spoofed, since TCP was aborted by the source every time the TCP connection was about to be completed. The normal group of 3 RST actually came from the real "www.rivalcom.net" site for a non-existing connection, while the intruder generates a set of RST/ACK with 1:1(0) ACK 1 since it does not know what SYN/ACK sequence number was. The real intruder could be someone on the same net with a network sniffer to collect TCP exchange information.

4. Description of attack:

Suppose a host sent out a SYN for TCP connection. If a response is not received, then it will re-send (after 6 seconds and then 24 seconds for 4.4BSD). In this case, the source www.rivalcom.net sent three rapid SYN in a row is obviously not natural. After the target Subnet1.120 responded with SYN/ACK, the intruder immediately sent back three RST packets followed by another three RST packets. This 3 SYN->3 SYN/ACK->3 RST->3 RST/ACK cycle continues for 7 times. It was a crafted intrusion pattern.

The intruder is searching for DNS server in order to download a host table for DNS zone-transfer. However, the pattern is too unusual to warrant obvious explanation. Here is a remotely probable explanation:

There is a possible DoS attack on a server implemented with blocking sockets. The attacking client immediately sends a RST after the *connect* call. If the RST is received after the server's return from *select* but before the *accept* call, then the completed connection will be removed from queues by RST leaving nothing for the server to call *accept* on. The server will then be blocked. ("Unix Network Programming," by W. Richard Stevens, Prentice Hall PTR, 1998, pp.422-424). Could the intruder be experimenting with similar blocking attack to a target DNS server?

5. Attack mechanism:

This regular probing pattern indicates that each probe is executed from a script, since 3 TCP connections are initiated very quickly which all end in two groups of 3 RST. The same cycle repeats itself at the time:18:36:22, 19:53:21, 23:14:47, 01.57:34, 05:57:18, 06:32:20, and 07:56:37. The time interval between any two adjacent cycles appears to be random and is at least one hour long. This may indicate that the script is invoked manually instead via another script. (It would be interesting to install NMAP and compare the traffic pattern it generates.)

6. Correlations:

No similar pattern has ever been seen on either subnet.

7. Evidence of active targeting:

It is a general scan of the entire subnet for DNS servers, nothing else.

8. Severity:

Component	Score	Reason
Criticality	3	No real DNS server in the subnet except a Linux box with port 53 open.
Lethality	4	The Linux box actually cooperated in establishing a TCP connection and it might be a target for a possible DoS attack
System Countermeasures	5	The Linux box is not a DNS
Network Countermeasures	0	No Firewall for the subnets to block TCP and UDP port 53
Severity Score	2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Port 53 can be easily closed at the firewall.

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

a) DNS Inverse Query
b) DNS Version Scan
c) DNS buffer overflow attack
d) None of the above

Answer: d

==========

Detect 9

==========

```
FWIN,2000/06/02,14:46:44 -5:00 GMT,194.159.136.241:1029,Subnet2.219:80,TCP
FWIN,2000/06/02,14:46:48 -5:00 GMT,194.159.136.241:797,Subnet2.219:53,TCP
FWIN,2000/06/02,14:46:56 -5:00 GMT,194.159.136.241:25,Subnet2.219:3925,TCP
FWIN,2000/06/02,14:46:56 -5:00 GMT,194.159.136.241:35709,Subnet2.219:80,TCP
FWIN,2000/06/02,14:46:56 -5:00 GMT,194.159.136.241:7788,Subnet2.219:49164,TCP
FWIN,2000/06/02,14:46:58 -5:00 GMT,194.159.136.241:1139,Subnet2.219:80,TCP
FWIN,2000/06/02,14:47:00 -5:00 GMT,194.159.136.241:61059,Subnet2.219:1171,TCP
FWIN,2000/06/02,14:47:00 -5:00 GMT,194.159.136.241:4606,Subnet2.219:53,TCP
FWIN,2000/06/02,14:47:00 -5:00 GMT,194.159.136.241:25,Subnet2.219:56666,TCP
```

1. Source of trace

This trace is collected on June 2, 2000 from a workstation installed with a ZoneAlarm personal firewall (from Zone Labs, Inc., http://www.zonelabs.com).

2. Detect was generated by:

The ZoneAlarm keeps an alarm log: ZALog.txt, which has the following format:

FWIN (or OUT), time, src.port, dst.port, protocol type

3. Probability the source address was spoofed

Since an attempt was to collect information on live ports by establishing TCP connections, the address was not spoofed. The domain name of the host

194.159.136.241 is "no-dns-yet.demon.co.uk". The IP addresses ranging from 194.159.136.0 to 194.159.137.255 are owned by Demon Internet in Great Britain.

4. Description of attack:

This is an attack against destination SMTP port 25, DNS TCP port 53 and HTTP TCP port 80. However, other ports 1171, 3925, 49164, and 56666 are not known to be trojan ports.

5. Attack mechanism:

It is a slow scan of open ports for exploitation. Since it was not captured by WinDump, no detail is available for analysis.

6. Correlations:

This pattern launched during the broad-day light (2:46 PM!) has never been seen before on either subnet.

7. Evidence of active targeting:

It is definitely active targeting at Subnet2.219.

8. Severity:

Component	Score	Reason
Criticality	3	Specific host is targeted.
Lethality	2	Probing important ports: 25, 53, 80
System Countermeasures	5	No SMTP server, DNS or Web servers in Subnet2
Network Countermeasures	0	No Firewall for the subnets to block TCP and UDP port 19.
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Ports 25 and 53 should be blocked at the firewall. Any web server should be configured for little else and placed in a DMZ.

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

a) a host scan
b) a port scan
c) a spoofed source IP-address
d) a spoofed target IP-address

Answer: b

==========

Detect 10

==========

[18:35:20.556209 **206.176.81.2.2968** > Subnet1.**3.110: S** 463067560:463067560(0) win 32120 <mss 1460,sackOK,timestamp 34783767[|tcp]> (DF) (ttl 49, id 42734)
18:35:20.556578 206.176.81.2.2970 > Subnet1.**5.110: S** 3867271706:3867271706(0) win
18:35:20.563684 206.176.81.2.2965 > **255.255.255.255**.110: S 3122249090:3122249090(0) win 32120 <mss 1460,sackOK,timestamp 34783767[|tcp]> (DF) (ttl 49, id 42731)
18:35:20.566183 206.176.81.2.2969 > Subnet1.**4.110: S** 718640815:718640815(0) win 32120 <mss 1460,sackOK,timestamp 34783767[|tcp]> (DF) (ttl 49, id 42735)
18:35:20.567183 206.176.81.2.2971 > Subnet1.**6.110**: **S** 3855875180:3855875180(0) win 32120 <mss 1460,sackOK,timestamp 34783767[|tcp]> (DF) (ttl 49, id 42737)
18:35:20.578560 206.176.81.2.2995 > Subnet1.**26.110**: **S** 3008041781:3008041781(0) win 32120 <mss 1460,sackOK,timestamp 34783767[|tcp]> (DF) (ttl 49, id 42761)
18:35:20.578635 Subnet1.**26**.110 > 206.176.81.2.2995: **R** 0:0(0) **ack** 3008041782 win 0 (ttl 128, id 15661)

1. Source of trace

This is detected on Subnet1 on May 28, 2000.

2. Detect was generated by:

WinDump (tcpdump for Windows) was used: **windump -vv -n**

The format of the trace:
time src.port > dst.port protocol-type length(time-to-live, ID#).

3. Probability the source address was spoofed

Since this is an attempt to find hosts with live Pop3 Mail server port (110), the address was not spoofed. The source IP address 206.176.81.2 can not be inverse-mapped to known domain name. The IP addresses ranging from 206.176.0.0 to 206.176.127.255 are owned by SDNet, an ISP.

4. Description of attack:

This is a probe for POP3 Mail server using TCP connection. Since the destination host does not run Pop3 server, the traffic can not be from a legitimate user trying to retrieve mail. It might be that someone is trying to run various Pop3 exploits (e.g. using login/password-guessing program to read someone else's mail or exploit buffer-overflow implementations).

5. Attack mechanism:

There are all kinds of Pop3 server exploits. There are several pop3 password crackers such as pop3.c, and pop3hack.c. There is also a Pop3 exploit for Linux in.pop3d to read unauthorized mails. Some Pop3 servers may suffer from Buffer overflow problem allowing intruders to gain root access.

6. Correlations:

Later on the same day, we found the following on the same subnet :

20:38:44.913596 **206.182.235.227.4473** > Subnet1.**26.110**: **S** 1760278660:1760278660(0) win 32120 <mss 1460,sackOK,timestamp 32256100[|tcp]> (DF) (ttl 51, id 50403)

20:38:44.914626 Subnet1.26.110 > 206.182.235.227.4473: **R** 0:0(0) **ack** 1760278661 win 0 (ttl 128, id 47150)

The source IP address: 206.182.235.227 is inverse-mapped to "habbie227.habibie.net". The IP addresses ranging from 206.182.0.0 to 206.182.255.255 are owned by Infonet Services Corporation.

7. Evidence of active targeting:

A direct Pop3 server access from the Internet is not uncommon. However, host scans for an open Pop3 server using a TCP connection is a deliberate act.

8. Severity:

Component	Score	Reason
Criticality	0	No Pop3 server in the subnet
Lethality	0	No Pop3 mail server
System Countermeasures	5	No Pop3 server
Network Countermeasures	0	Firewall will not be configured to block port 110 so that traveling users may retrieve their mails.
Severity Score	-5	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures)

9. Defensive recommendation:

Apply security patches to the Pop3 server. Qpopper is a popular Pop3 server. Qpopper version prior to 2.5 should not be used since it has a buffer overflow problem to allow intruder to gain root shell access. If Qpopper is used with Kerberos authentication services (versions 4 and 5), then security patches should be applied (http://www.cert.org/advisories/CA-2000-06.html).

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

a) The R flag indicates that there is no exiting TCP connection.
b) The R flag indicates that it is a request for re-send.
c) The R flag indicates that it has been read.
d) None of the above

Answer: d