Global Information Assurance Certification Paper

GIAC Intrusion Detection Curriculum Practical Assignment for SNAP San Jose May 8-13, 2000 by:
William Davis

Detect 1

```
May  1 13:26:54 rt1 2634: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.8 (8/0), 1 packet
May  1 13:26:54 rt1 2635: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.63 (8/0), 1 packet
May  1 13:26:54 rt1 2636: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.64 (8/0), 1 packet
May  1 13:26:54 rt1 2637: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.127 (8/0), 1 packet
May  1 13:26:54 rt1 2638: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.128 (8/0), 1 packet
May  1 13:26:54 rt1 2639: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.191 (8/0), 1 packet
May  1 13:26:54 rt1 2640: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.192 (8/0), 1 packet
May  1 13:26:55 rt1 2641: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
  196.1.142.4 -> 192.168.1.254 (8/0), 1 packet
```

1. Source of Trace:

   My network

2. Detect was generated by:

   Cisco ACL Logs

   Description of Cisco log fields:
   May 1 13:26:54 [*timestamp*] rt1 [*hostname*] 2634: [*message number:*]
   %SEC-6-IPACCESSLOGDP: *[%facility-subfacility-severity-Mnemonic*]
   list 111 [*ACL list responsible for action*] denied [*action*]
   icmp [*transport protocol*] 196.1.142.4 [*source ip*] ->
   192.168.1.8 [*destination ip*] (8/0) [*icmp type/code*], 1 packet [# *of packets*]

3. Probability the source address was spoofed:

   The address as reported by the ARIN Whois web site is from an ISP in Jamaica with host names of JOL1.JOL.COM.JM and NS1.JOL.COM.JM, suggesting it might be the ISP's nameserver.

   Low - There is a possibility the address could be spoofed to cause a DoS Attack to the spoofed address, but the above patterned occurred only once, suggesting the attacker was interested in receiving the responses.

4. Description of Attack:

   a. Attacker is sending ICMP echo requests to possible broadcast addresses for a subnetted class B, or Class C address space. This is a signature of "Clever Mapping", a Netmask-Based Broadcast network mapping.

   b. Note however, this differs from the typical signature of "Clever Mapping,"

in that the attacker does not send echo requests to the .0 and .255 addresses and instead uses the .8 address and .254 address. This may be an attempting to avoid detects from routers that block .0 and .255 broadcasts. While the .8 address is an alternate all zeros broadcast address, the .254 address would never be a valid broadcast address for any useable subnet. (For a discussion on subnet masks, refer to RFC 1878, and two good articles in SunExpert: Henry, S. Lee, "Demystifying Netmasks," Sun Expert, V9, N5, pp43-45. Henry, S. Lee, "Variable-Length Subnet Masking, " Sun Expert, V9, N11, pp38-40.)

5. Attack Mechanism:

   a. Echo requests to subnet broadcast addresses can result in all systems on that subnet responding with an echo-reply. By sending echo requests to all of the most common subnet broadcast addresses, the attacker can map the entire address space if the network allows outbound echo-replies.

6. Correlation:

   a. This method of network mapping was described as "Clever mapping" in the SANS GIAC course notes for "TCP/IP for Intrusion Detection and Perimeter Defense" May, 8, 2000, page 5-15.

   b. This method is also described as "Netmask-Based Broadcasts" in Northcutt, S., Network Intrusion Detection, An Analyst's Handbook, New Riders, 1999, pp126-127.

7. Evidence of active targeting:

   The attack was directed at this subnet address space.

8. Severity: -4

   (Criticality + Lethality) - (System + Network Countermeasures) = Severity
   3 1 - 4 + 4 = -4

   Criticality = 3 -- Subnet Broadcast Addresses were specifically targeted
   Lethality = 1 -- Attack will not do damage, but could expose network infrastructure
   System = 4 -- Mix of new and old OS's, but all systems fully patched
   Network = 4 -- Restrictive network firewall and router ACL lists

9. Defensive recommendation:

   The defenses were sufficient against this attack. The router ACl list did not allow incoming icmp echo requests.

10. Multiple choice question:

    The above trace is best described as:
    a. Network mapping using random addresses
    b. Denial of Service from spoofed address
    c. Network mapping using broadcast addresses
    d. Echo-Chargen attack
    Answer: C

Detect 2

```
Subnet #1
18/05/2000 18:37:38.446846  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.128,543 PR tcp len 20 40 -SF
18/05/2000 18:37:38.599267  le0 @151:11 b 194.89.196.201 -> 192.168.156.128 PR icmp
len 20 56 icmp 11/0 for 192.168.156.128,543 - ns2.keminmaa.fi,543 PR tcp len 20 40
18/05/2000 18:37:38.768088  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.144,543 PR tcp len 20 40 -SF
18/05/2000 18:37:38.771066  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.143,543 PR tcp len 20 40 -SF
18/05/2000 18:37:38.775141  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.141,543 PR tcp len 20 40 -SF
18/05/2000 18:37:39.338911  le0 @151:11 b 194.89.196.201 -> 192.168.156.165 PR icmp
len 20 56 icmp 11/0 for 192.168.156.165,543 - ns2.keminmaa.fi,543 PR tcp len 20 40
18/05/2000 18:37:39.788090  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.195,543 PR tcp len 20 40 -SF
18/05/2000 18:37:39.938195  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.202,543 PR tcp len 20 40 -SF
18/05/2000 18:37:39.947196  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.203,543 PR tcp len 20 40 -SF
18/05/2000 18:37:39.967179  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.204,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.027141  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.207,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.065829  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.209,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.107502  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.211,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.146865  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.213,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.184284  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.215,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.207052  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.216,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.245704  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.218,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.266752  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.219,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.406155  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.226,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.426894  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.227,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.465604  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.229,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.489596  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.230,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.587531  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.235,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.785863  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.245,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.804315  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.246,543 PR tcp len 20 40 -SF
18/05/2000 18:37:40.837037  le1 @250:6 b ns2.keminmaa.fi,543 ->
192.168.156.247,543 PR tcp len 20 40 -SF
```

```
Subnet #2
May 18 18:29:58.544443 hme0 @0:14 b ns2.keminmaa.fi,klogin ->
192.168.100.28,klogin PR tcp len 20 40 -SF 417631600 504652186 1028 IN
May 18 18:29:59.504605 hme0 @0:15 b ns2.keminmaa.fi,klogin ->
192.168.100.8,klogin PR tcp len 20 40 -SF 710755890 1758060403 1028 IN
May 18 18:29:59.910203 hme0 @0:14 b ns2.keminmaa.fi,klogin ->
192.168.100.5,klogin PR tcp len 20 40 -SF 710755890 1758060403 1028 IN
May 18 18:30:00.558286  le0 @0:12 b 194.252.152.4,klogin ->
192.168.100.20,klogin PR tcp len 20 40 -SF 417631600 504652186 1028 IN
May 18 18:30:01.348621 hme0 @0:14 b ns2.keminmaa.fi,klogin ->
192.168.100.3,klogin PR tcp len 20 40 -SF 710755890 1758060403 1028 IN
May 18 18:30:02.287182 hme0 @0:14 b ns2.keminmaa.fi,klogin ->
192.168.100.30,klogin PR tcp len 20 40 -SF 417631600 504652186 1028 IN
```

1. Source of Trace:

   Subnet #1: My network
   Subnet #2: A separate subnet within the same class B network

2. Detect was generated by:

   a. IP Filter log

      IP Filter is a packet filtering firewall
      (see URL: http://coombs.anu.edu.au/ipfilter/)

   b. Description of IP Filter log
      18/05/2000 18:37:38.446846[*time-stamp*] le1[*interface*]
      @250:6[*rule-set group:number*] b[*action b=block p=pass*]
      ns2.keminmaa.fi,543[*source ip,port*] ->
      192.168.156.128,543[*destination ip,port*] PR tcp[*transport protocol*]
      len 20[*IP header length*] 40[*total packet length*]
      -SF[*tcp flags sequence numbers window size* ***or*** *icmp message type*]
      for[*packet description which caused icmp message --* ***icmp only***]

3. Probability the source address was spoofed:

   Low: Attacker may want to see the response to these packets.

4. Description of Attack:

   a. This trace is of a port scan of two subnets within a class B network
      for an active service on port 543.
   b. The scan uses the impossible TCP flag SYN-FIN combination,
      indicating the packets were crafted.
   c. Port 543 is commonly used by klogind, the Kerberos Authenticated Service.
   d. The scan was probably made through the entire class B network address
      space, since two subnets within the class B were both targeted.
   e. It is possible the source address is a compromised name server
      ns2.keminmaa.fi = 194.252.152.4

5. Attack Mechanism:

   a. The attacker sends connection requests for a specific port/service they
      are seeking to exploit.
   b. A system running the a service on that port will respond to the
      source address with a SYN-ACK packet, indicating to the attacker,

a potential service to exploit.
c. If the system is not running a service on that port, it will respond with a RESET, informing the attacker the service is not available.
d. If the host does not exist, the router may send an icmp "destination unreachable" message, informing the attacker the service is not available.
e. The SYN-FIN combination is used by the attacker in hopes of eluding some firewall and ID systems.

6. Correlation:

a. The SYN-FIN Scanning is described on Page 114 of Intrusion Detection and Packet Filtering: How It Really Works by: Vicki Irwin & Hal Pomeranz, Sans GIAC Course 2.2, May 9, 2000

b. It is interesting to note that the CERT advisory CA-2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services was released on May 17th, 2000. The attacker had identified an exploit and was scanning for vulnerable systems the **next day** after the CERT advisory was released.

c. There was also a CERT Advisory, CA-2000-03, Continuing Compromises of Nameservers Advisory, which indicates continuing active targeting of DNS servers to gain privileged compromise of the systems. Since the system, ns2.keminmaa.fi, was able to respond to DNS queries, it is likely this has become a compromised system.

7. Evidence of active targeting:

The attack was directed at both my subnet and another subnet within the same Class B network, looking for a know vulnerable service. My subnet was not specifically singled out within the Class B network.

8. Severity: -4

```
(Criticality + Lethality) - (System + Network Countermeasures) = Severity
    3            1            4 + 4 = -4
 Criticality = 3 -- Scanning specifically for Kerberos servers
 Lethality   = 1 -- Attack will not do damage, no Kerberos servers on my subnet
 System      = 4 -- Mix of new and old OS's, but all systems fully patched
 Network     = 4 -- Restrictive network firewall
```

9. Defensive recommendations:

The defenses were sufficient against this attack. However, the DMZ system did respond with TCP RESET packets, identifying that hosts existed at those IP's. Individual firewalls or a DMZ firewall should be implemented to prevent responding to services not specifically allowed. Note: In this case, the TCP response packets may not have reached their destination, as evidenced by the icmp "time exceeded" messages sent to our subnet by 194.89.196.201, a system or router in the Finnish Telecom IP block.

10. Multiple choice question:
The SYN-FIN flag combination in the above trace is
a. A valid response when the requested service is unavailable
b. An illegal flag combination
c. An attempt to bypass detection by firewalls and ID systems
d. Both b and c.
ANSWER: D

Detect 3

```
09/01/2000 13:05:51.965393  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.228 PR icmp len 20 56 icmp 3/1
  for 192.168.156.228,17083 - lon-c45-004-vty230.as.wcom.net,telnet PR tcp len 20 40
09/01/2000 13:12:30.922618  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,telnet
  -> 192.168.156.141,58270 PR tcp len 20 40 -AR
09/01/2000 13:13:47.308249  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ftp
  -> 192.168.156.203,38184 PR tcp len 20 40 -AR
09/01/2000 13:13:58.276423  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,telnet
  -> 192.168.156.144,23934 PR tcp len 20 40 -AR
09/01/2000 13:15:01.513978  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ftp
  -> 192.168.156.218,52726 PR tcp len 20 40 -AR
09/01/2000 13:15:01.579466  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,telnet
  -> 192.168.156.195,29137 PR tcp len 20 40 -AR
09/01/2000 13:16:20.896788  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ftp
  -> 192.168.156.218,48551 PR tcp len 20 40 -AR
09/01/2000 13:16:20.899094  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ftp
  -> 192.168.156.215,7627 PR tcp len 20 40 -AR
09/01/2000 13:17:08.350183  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ssh
  -> 192.168.156.213,28381 PR tcp len 20 40 -AR
09/01/2000 13:17:48.929289  le1 @250:13 b lon-c45-004-vty230.as.wcom.net,ftp
  -> 192.168.156.245,32123 PR tcp len 20 40 -AR
09/01/2000 13:26:02.725542  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.234 PR icmp len 20 56 icmp 3/1
  for 192.168.156.234,27918 - lon-c45-004-vty230.as.wcom.net,ssh PR tcp len 20 40
09/01/2000 13:27:49.762467  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.159 PR icmp len 20 56 icmp 3/1
  for 192.168.156.159,38701 - lon-c45-004-vty230.as.wcom.net,telnet PR tcp len 20 40
09/01/2000 13:37:11.078974  le0 @0:32 b lon-ppp2-fddi0-0-0.wan.wcom.net
  -> 192.168.156.236 PR icmp len 20 56 icmp 11/0
  for 192.168.156.236,64401 - lon-c45-004-vty230.as.wcom.net,ftp PR tcp len 20 40
09/01/2000 13:37:11.082149  le0 @0:32 b lon-ppp1-fddi0-0-0.wan.wcom.net
  -> 192.168.156.235 PR icmp len 20 56 icmp 11/0
  for 192.168.156.23,36328 - lon-c45-004-vty230.as.wcom.net,ftp PR tcp len 20 40
09/01/2000 13:38:45.970343  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.248 PR icmp len 20 56 icmp 3/1
  for 192.168.156.248,63839 - lon-c45-004-vty230.as.wcom.net,ftp PR tcp len 20 40
09/01/2000 13:43:38.757722  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.254 PR icmp len 20 56 icmp 3/1
  for 192.168.156.254,48131 - lon-c45-004-vty230.as.wcom.net,ssh PR tcp len 20 40
09/01/2000 13:48:33.129889  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.178 PR icmp len 20 56 icmp 3/1
  for 192.168.156.178,18628 - lon-c45-004-vty230.as.wcom.net,ftp PR tcp len 20 40
09/01/2000 13:55:08.257413  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.219 PR icmp len 20 56 icmp 3/1
  for 192.168.156.219,32589 - lon-c45-004-vty230.as.wcom.net,telnet PR tcp len 20 40
09/01/2000 13:59:23.471992  le0 @0:32 b lon-c45-004-eth01.as.wcom.net
  -> 192.168.156.178 PR icmp len 20 56 icmp 3/1
  for 192.168.156.178,56854 - lon-c45-004-vty230.as.wcom.net,telnet PR tcp len 20 40
```

Additional Information:

The above trace is representative of one hour during an event that occurred continually from 14:37 on January 8, 2000 until 11:08 on January 10, 2000. There was some sporadic occurrences on the evening of January 7th and the morning of the 8th. Notably, this occurred over the first weekend after the transition to Y2K.

1 Source of Trace:

a. My network

2. Detect was generated by:

a. IP Filter log

IP Filter is a packet filtering firewall
(see URL: http://coombs.anu.edu.au/ipfilter/)

b. Explanation of fields:
09/01/2000 13:59:23.471992 [*timestamp*] le0 [*interface*]
@0:32 [*rule-set group:number*] b [*action b=block p=pass*]
lon-c45-004-eth01.as.wcom.net [*source address/port*]
-> 192.168.156.178 [*destination address/port*] PR icmp [*transport protocol*]
len 20 [*ip header length*] 56 [*packet length*]
icmp 3/1[*tcp flags* ***or*** *icmp type/code*]
for 192.168.156.178,56854 - lon-c45-004-vty230.as.wcom.net,telnet
PR tcp len 20 40[*original packet information that caused error message in format as described above*]

3 Probability the source address was spoofed:

a. Low - the source address appears to be the target, it is our address space that is being used in spoofing against the target.

b. The target, lon-c45-004-vty230.as.wcom.net, is thought to be part of the UUNET/WorldCOM address space in London England, possibly a port on a terminal server of a modem pool. (See Additional Comments below)

4. Description of Attack:

a. What the trace above is showing are icmp destination host unreachable messages or tcp ACK/Reset responses sent to queries supposedly originating from hosts on my network. Since many of the IP addresses are not in use on my network, it was obvious my address space was being spoofed to conceal the attackers true source. What I was seeing was merely the echoes, the second order effect, of an attack against the target lon-c45-004-vty230.as.wcom.net.

b. All packets received by my network would elicit no response from any of my systems.

c. The attacker id attempting to repeatedly initiate connections to the target system. Although this trace shows only a portion of what the target may be experiencing, it is possible it may be under a DoS attack or host reconnaissance.

5. Attack Mechanism:

   a. The attacker uses address from my network as the source/port of packets that are crafted and then sent to the target system.

6. Correlation:

   a. Responses from spoofing are described in section 6, pages 31-34 of "TCP/IP for Intrusion Detection and Perimeter Defense" by Hal Pomeranz, SANS GIAC Course 2.1, May 8, 2000.

7. Evidence of active targeting:

   The attack was not directed at this subnet address space, rather, this address space was used to conceal the source of an attack against another target.

8. Severity: -6

   (Criticality + Lethality) - (System + Network Countermeasures) = Severity
   1 + 1 - 4 + 4 = -6
   Criticality = 1 -- Subnet was not specifically targeted
   Lethality = 1 -- Attack will not do damage
   System = 4 -- Mix of new and old OS's, but all systems fully patched
   Network = 4 -- Restrictive network firewall and router ACL lists

9. Defensive recommendation:

   a. The defenses were sufficient against this attack. The firewall ruleset did not allow either incoming/outgoing icmp destination unreachable or time exceeded messages or incoming connections to ephemeral ports that are not explicitly permitted or stateful.

   b. Additionally, the firewall rules deny outgoing traffic that has source IPs that are not within our address space, preventing our system from taking part in an attack that uses spoofing to conceal the attackers true source address.

   c. A recent RFC, rfc 2827, discusses best current practices for defeating DoS attacks which employ IP source address spoofing.

10. Multiple choice question:

   The above trace is an example of:
   a. A network scan for ftp, ssh and telnet
   b. An attack employing spoofing against network 192.168.156.0
   c. Second order effect
   d. A false positive, this is normal ICMP/TCP traffic
   Answer: C

Additional Comments:

The reason I included this trace was because the echoes I was seeing were very intriguing, and produced more questions than answers.

Some facts I found interesting:

a. The event took place over the first weekend after "Y2K"

b. The attacker sent approximately 20 TCP packets, supposedly from our network, each hour for 44 hours.

c. The attacker concentrated only on ports 21 22 and 23, commonly used for ftp, ssh and telnet.

d. A complex pattern emerged when looking at all 44 hours.

1. The only times ACK/Reset packets occur are from the target IP and usually only occur during at most a 15 minute window.

2. All icmp messages came from one of eight sources

a. Four of these sources return icmp 11/0 (TTL = 0)

```
lon-ppp1.fdd3-1-0.wan.wcom.net  195.232.0.37
lon-ppp2.fddi0-0-0.wan.wcom.net 195.232.0.39
lon-ppp1.fddi0-0-0.wan.wcom.net 195.232.94.71
lon-ppp2.fdd3-1-0.wan.wcom.net  195.232.94.69
```

b. The remaining sources returned icmp 3/1 (Host Unreachable)

```
lon-C45-001-eth01.as.wcom.net   (unable to determine IP)
lon-C45-002-eth01.as.wcom.net   (unable to determine IP)
lon-C45-004-eth01.as.wcom.net   (unable to determine IP)
lon-core1-atm6-0-2.wan.wcom.net 195.232.0.173
```

3. The target during the entire 44 hour attack remained the same:
   lon-c45-004-vty230.as.wcom.net
   However the preliminary traces showed three other targets were also selected before settling on the above target:
   lon-c45-001-vty18.as.wcom.net
   lon-c45-002-vty250.as.wcom.net
   mfs-pci-bqi-vty4.as.wcom.net (ip 212.211.8.4)

e. The cryptic system names elicit some possible functionality:

```
eth01 - an ethernet interface on a router
fddi  - an fddi interface on a router
atm   - an atm interface on a router

vty### - a port on a terminal server assigned an ip address

ppp - point to point protocol
as - access server
wan - wide area network
```

f. The RIPE whois site yielded the following information for the IP's above
    a. 212.211.0.0 - 212.211.23.255 UUNET London PPP Client Pool
    b. 195.232.94.0 - 195.232.94.255 UUNET London PPP Infrastructure
    c. 195.232.0.0 - 195.232.0.255   European Core Network Infrastructure

What's going on here?

What seems to be occurring is repeated attempts to initiate connections to a specific terminal server port on a general ISP's PPP modem pool using a spoofed address.

Why would you want to do this?

Possible scenarios

a. This attack could be a Denial of Service attack against the UUNET PPP Client Pool in London, England, seeking to overwhelm the resources of the terminal server or router with connection attempts. However, due to the low number of responses echoed to our network, this would have to be only part of a distributed attack that we were seeing. It would have been interesting to know if the rest of our Class B address space was being used to spoof, a good reason for sharing information and installing multiple sensors.

b. The attacker could be monitoring for "live" connections. From the "echos" I saw, I could tell when someone had logged into the port. It one of those systems supported telnet, ftp or ssh, I might be able to connect to that system if I were truly the source of that probe. During this trace, that did not appear to be the case, but there may have been other ports that were being monitored. Again, our address space could have been used as part of a smoke screen to conceal an address where the responses could be received by the attacker.

I would be interested to know of other possible reasons.

Detect 4

```
Oct 20 01:50:07 rt1 780: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.206 (8/0), 1 packet
Oct 21 09:28:14 rt1 782: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.92 (8/0), 1 packet
Oct 21 22:00:13 rt1 783: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.136 (8/0), 1 packet
Oct 22 10:23:26 rt1 784: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.114 (8/0), 1 packet
Oct 22 21:53:56 rt1 785: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.29 (8/0), 1 packet
Oct 23 09:00:27 rt1 786: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.89 (8/0), 1 packet
Oct 23 20:05:15 rt1 787: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.214 (8/0), 1 packet
Oct 24 07:05:32 rt1 788: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.138 -> 192.168.156.80 (8/0), 1 packet
Oct 24 18:18:39 rt1 789: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.158 (8/0), 1 packet
Oct 26 15:25:34 rt1 801: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.254 (8/0), 1 packet
Oct 27 02:53:36 rt1 803: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.3 (8/0), 1 packet
Oct 27 14:31:31 rt1 805: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.13 (8/0), 1 packet
Oct 28 01:53:48 rt1 806: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.49 (8/0), 1 packet
Oct 28 13:10:54 rt1 807: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.135 -> 192.168.156.227 (8/0), 1 packet
Oct 29 00:23:51 rt1 808: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.21 (8/0), 1 packet
Oct 29 11:45:37 rt1 809: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.179 (8/0), 1 packet
Oct 29 22:54:46 rt1 814: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.44 (8/0), 1 packet
Oct 30 10:06:06 rt1 815: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.105 (8/0), 1 packet
Oct 30 21:16:21 rt1 817: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.141 -> 192.168.156.148 (8/0), 1 packet
Oct 31 07:22:49 rt1 818: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.240 (8/0), 1 packet
Oct 31 18:34:54 rt1 819: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.141 -> 192.168.156.23 (8/0), 1 packet
Nov  1 05:56:33 rt1 820: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.138 -> 192.168.156.100 (8/0), 1 packet
Nov  1 17:20:50 rt1 821: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.138 -> 192.168.156.162 (8/0), 1 packet
Nov  2 04:33:42 rt1 824: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.136 -> 192.168.156.143 (8/0), 1 packet
Nov  2 15:54:00 rt1 826: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.103 (8/0), 1 packet
Nov  3 03:10:47 rt1 828: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.138 -> 192.168.156.251 (8/0), 1 packet
Nov  3 14:18:35 rt1 829: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.140 -> 192.168.156.112 (8/0), 1 packet
```

```
Nov  4 01:19:59 rt1 830: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.138 -> 192.168.156.232 (8/0), 1 packet
Nov  4 12:15:52 rt1 833: %SEC-6-IPACCESSLOGDP: list 111 denied icmp
216.206.191.139 -> 192.168.156.69 (8/0), 1 packet
```

1. Source of Trace:

   My network

2. Detect was generated by:

   Cisco ACL logs

   Description of Cisco log fields:

   Oct 20 01:50:07 [*timestamp*] rt1 [*hostname*] 780:[*message number*:]
   %SEC-6-IPACCESSLOGDP: [%*facility-subfacility-severity-Mnemonic*]
   list 111 [*ACL list responsible for action*] denied [*action*]
   icmp [*transport protocol*] 216.206.191.139[*source ip*]
   -> 192.168.156.206[*destination ip*]
   (8/0)[*icmp type/code*], 1 packet[# *of packets*]

3. Probability the source address was spoofed:

   Low - The attacker may want to receive responses to the packets sent to my
         network.

   The ip addresses are part of the QWest block, a large ISP.

4. Description of Attack:

   a. The attacker is sending icmp echo request packets to random IP addresses
      within my network's address space.

   b. The attacker sends only a maximum of two requests per day for a period of
      15 days.

   c. The requests originate from 6 different IP's, all within a tight range
      from 216.206.191.135 to 216.206.191.141

   d. The attack is a Network Mapping attack and is an example
      of a "Low and Slow" ping sweep.

5. Method of Attack:

   a. The attacker sends icmp echo requests to IP addresses within a networks
      address space. If allowed, systems that reside at those addresses will
      respond with an icmp echo reply, alerting the attacker to the presence of
      a host at that specific address.

   b. The attacker limits the icmp requests to only one or two per day in an
      attempt to avoid detection by ID systems or firewalls. These systems may
      look for many rapidly sent requests to a number of hosts, or set a
      threshold that is often higher than 4 per hour. This technique is often
      referred to as "low and slow."

6. Correlation:

   a. ICMP-based network mapping is a common reconnisance technique and has been described on page 71 of "Intrusion Detection and Packet Filtering: How It Really Works" by: Vicki Irwin & Hal Pomeranz, Sans GIAC Course 2.2, May 9, 2000

   b. In Northcutt, S., Network Intrusion Detection, An Analyst's Handbook, New Riders, 1999, p125, the "low and slow" method is considered as one of the best stealth techniques.

7. Evidence of active targeting:

   The attack was directed at this subnet address space.

8. Severity: -5

   (Criticality + Lethality) - (System + Network Countermeasures) = Severity
   2 1 - 4 + 4 = -5

   Criticality = 2 – Random hosts were targeted
   Lethality = 1 -- Attack will not do damage, but could expose network infrastructure
   System = 4 -- Mix of new and old OS's, but all systems fully patched
   Network = 4 -- Restrictive network firewall and router ACL lists

9. Defensive recommendation:

   The defenses were sufficient against this attack. The router ACl list did not allow incoming icmp echo requests.

10. Multiple choice question:

    "Low and Slow" is considered to be:
    a. a network scan of low numbered ports
    b. a scan for the more unreliable UDP ports
    c. an effective stealth technique
    d. common in covert channel attacks
    Answer: C

Detect 5

```
09/02/2000 15:01:36.806208  le1 @0:9 b 169.254.184.182,137 ->
169.254.255.255,137 PR udp len 20 96
09/02/2000 15:01:36.806680  le1 @0:9 b 169.254.184.182,137 ->
169.254.255.255,137 PR udp len 20 96
09/02/2000 15:01:36.807148  le1 @0:9 b 169.254.184.182,137 ->
169.254.255.255,137 PR udp len 20 96
09/02/2000 15:01:36.813671  le1 @200:1 b 192.168.156.141 ->
  169.254.184.182 PR icmp len 20 56 icmp 3/3
  for 169.254.184.182,137 - 169.254.255.255,137 PR udp len 20 96
09/02/2000 15:01:36.815516  le1 @200:1 b 192.168.156.141 ->
  169.254.184.182 PR icmp len 20 56 icmp 3/3
  for 169.254.184.182,137 - 169.254.255.255,137 PR udp len 20 96
09/02/2000 15:01:36.817471  le1 @200:1 b 192.168.156.141 ->
  169.254.184.182 PR icmp len 20 56 icmp 3/3
  for 169.254.184.182,137 - 169.254.255.255,137 PR udp len 20 96
```

1. Source of Trace:

   My network

2. Detect was generated by:

   a. IP Filter Log

   b. Description of fields:

   09/02/2000 15:01:36.806208[*time-stamp*] le1[*interface*]
   @0:9[*rule-set group:number*] b[*action b=block p=pass*]
   169.254.184.182,137[*source ip,port*] ->
   169.254.255.255,137[*destination ip,port*] PR udp[*transport protocol*]
   len 20[*IP header length*] 96[*total packet length*]
   [*tcp flags sequence numbers window size* ***or*** *icmp message type*]
   for[*packet description which caused icmp message --* ***icmp only***]

3. Probability the source address was spoofed:

   a. High -- The source address was generated from within my network and
      does not lie within my network's address space.

   b. The IP address information retrieved from the ARIN Whois website was:
        169.254.0.0 - 169.254.255.255
        For use with Link Local Networks
        Information Sciences Institute
        University of Southern California

4. Description of Attack:

   a. These packets were outbound from my network to the internet and
      contained source addresses not within my networks address space.

   b. The packets were udp packets using the netbios name service port 137.

   c. This appears to be a possible DoS attack against the spoofed address
      using attacks such as:
      CVE-1999-0288 Denial of service in WINS with malformed data to port 137

CVE-1999-0810 Denial of service in Samba NETBIOS name service daemon (nmbd).

d. It appeared as if someone had compromised a host on my network was attempted a spoofed attack against the source address.

5. Attack Mechanism:

a. The attacker sends a broadcast request from a spoofed address, the target host, to the target network. The network nameservers may flood the target host with responses, or themselves be affected by malformed data.

b. Since the attack was limited to this one occurrence, this would have to be a distributed DoS to be effective for any length of time.

c. I checked to see if this could be a legitimate NETBIOS broadcast from within my network and discovered a recently returned field laptop.

d. This was a **False positive**

6. Correlation:

a. This was a misconfiguration of a Win98 Laptop's ethernet NIC. The above pattern was repeated each time the TCP/IP properties for the NIC were set to a DHCP style interface, and then connected directly to my network, which does not use DHCP, using this interface. The laptop is primarily used offsite, but on rare occasions, is directly connected to upgrade software by the user. It appears the IP 169.254.184.182 was used as a default address by the NIC.

7. Evidence of active targeting: None

8. Severity: -7

```
(Criticality + Lethality) - (System + Network Countermeasures) = Severity
    1        +    0       -       4 + 4 = -7
 Criticality = 1 -- Destination was broadcast address
 Lethality   = 0 -- Attack was false positive
 System      = 4 -- Mix of new and old OS's, but all systems fully patched
 Network     = 4 -- Restrictive network firewall
```

9. Defensive recommendations:

None. Defenses were sufficient to detect and stop an attempt at a spoofed Attack from within our system. In this case, it was a false positive due to A NIC configuration error.

10 Multiple choice question:

Spoofing Attacks originating from within a network can be prevented by:
a. Preventing outbound traffic with source addresses outside the network address space.
b. Blocking all outbound traffic
b. Preventing inbound traffic with source addresses outside the network address space.
d. Installing a firewall
Answer: A

Detect 6

IP Filter Log:

```
12/06/2000 02:21:47.065873  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:48.470245  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:49.980080  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:51.101938  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:52.574933  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:54.098457  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:55.769459  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:21:55.789692  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
.
.
.
12/06/2000 02:29:06.974641  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
12/06/2000 02:29:08.425862  le0 @150:2 b dial-195-82-27-
149.GW4.ALA1.Nursat.net,137 -> web.server.com,137 PR udp len 20 78
```

Supporting TCP dump log:

```
02:21:46.083293 dial-195-82-27-149.GW4.ALA1.Nursat.net.4367 > web.server.com.80:
S 6450349:6450349(0) win 8192 <mss 1460> (DF)
02:21:46.085015 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4367:
S 1526188326:1526188326(0) ack 6450350 win 8760 <mss 1460> (DF)
02:21:46.913388 dial-195-82-27-149.GW4.ALA1.Nursat.net.4367 > web.server.com.80:
. ack 1526188327 win 8760 (DF)
02:21:47.046649 dial-195-82-27-149.GW4.ALA1.Nursat.net.4367 > web.server.com.80:
P 6450350:6450715(365) ack 1526188327 win 8760 (DF)
02:21:47.046973 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 45771)
                        4500 004e b2cb 0000 6d11 6836 c352 1b95
                        c0a8 9c63 0089 0089 003a d554 b82c 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
02:21:47.048610 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4367:
. ack 6450715 win 8760 (DF)
02:21:48.451587 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 47307)
                        4500 004e b8cb 0000 6d11 6236 c352 1b95
                        c0a8 9c63 0089 0089 003a d552 b82e 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
02:21:49.128181 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4367:
P 1526188327:1526188747(420) ack 6450715 win 8760 (DF)
02:21:49.130835 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4367:
F 1526188747:1526188747(0) ack 6450715 win 8760 (DF)
02:21:49.961417 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 49611)
                        4500 004e c1cb 0000 6d11 5936 c352 1b95
```

```
                        c0a8 9c63 0089 0089 003a d550 b830 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
02:21:50.099801 dial-195-82-27-149.GW4.ALA1.Nursat.net.4367 > web.server.com.80:
F 6450715:6450715(0) ack 1526188747 win 8340 (DF)
02:21:50.101036 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4367:
. ack 6450716 win 8760 (DF)
02:21:50.102467 dial-195-82-27-149.GW4.ALA1.Nursat.net.4367 > web.server.com.80:
. ack 1526188748 win 8340 (DF)
02:21:50.144732 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
S 6450373:6450373(0) win 8192 <mss 1460> (DF)
02:21:50.146256 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
S 1526802418:1526802418(0) ack 6450374 win 8760 <mss 1460> (DF)
02:21:50.964437 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
. ack 1526802419 win 8760 (DF)
02:21:51.079323 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
P 6450374:6450753(379) ack 1526802419 win 8760 (DF)
02:21:51.080897 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
. ack 6450753 win 8760 (DF)
02:21:51.083241 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 52427)
                        4500 004e cccb 0000 6d11 4e36 c352 1b95
                        c0a8 9c63 0089 0089 003a d54e b832 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
02:21:51.087432 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
P 1526802419:1526803879(1460) ack 6450753 win 8760 (DF)
02:21:52.430055 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
. ack 1526803879 win 8760 (DF)
02:21:52.432563 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
. 1526803879:1526805339(1460) ack 6450753 win 8760 (DF)
02:21:52.433798 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
. 1526805339:1526806799(1460) ack 6450753 win 8760 (DF)
02:21:52.556255 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 53451)
                        4500 004e d0cb 0000 6d11 4a36 c352 1b95
                        c0a8 9c63 0089 0089 003a d54c b834 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
02:21:53.728506 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
. ack 1526805339 win 8760 (DF)
02:21:53.731024 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
. 1526806799:1526808259(1460) ack 6450753 win 8760 (DF)
02:21:53.732256 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
. 1526808259:1526809719(1460) ack 6450753 win 8760 (DF)
02:21:53.974056 dial-195-82-27-149.GW4.ALA1.Nursat.net.4368 > web.server.com.80:
. ack 1526806799 win 8760 (DF)
02:21:53.975732 web.server.com.80 > dial-195-82-27-149.GW4.ALA1.Nursat.net.4368:
FP 1526809719:1526810346(627) ack 6450753 win 8760 (DF)
02:21:54.079786 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 58827)
                        4500 004e e5cb 0000 6d11 3536 c352 1b95
                        c0a8 9c63 0089 0089 003a d54a b836 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
```

```
.
.
.
02:29:06.949604 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50
02:29:07.842267 dial-195-82-27-149.GW4.ALA1.Nursat.net.4464 > web.server.com.80:
R 6836485:6836485(0) win 0 (DF)
02:29:08.400674 dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 109, id 56275)
                        4500 004e dbd3 0000 6d11 3f2e c352 1b95
                        c0a8 9c63 0089 0089 003a d3b8 b9c8 0010
                        0001 0000 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
```

Supporting HTTP Server Log:

```
dial-195-82-27-149.gw4.ala1.nursat.net - - [12/Jun/2000:02:21:49 -0600] "GET /
HTTP/1.0" 302 228 "http://www.epa.gov/ozone/othlinks.html" "Mozilla/4.0
(compatible; MSIE 5.0; Windows 95; DigExt)"
dial-195-82-27-149.gw4.ala1.nursat.net - - [12/Jun/2000:02:21:51 -0600] "GET
/home_page.html HTTP/1.0" 200 7681 "http://www.epa.gov/ozone/othlinks.html"
"Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)"
.
.
.
dial-195-82-27-149.gw4.ala1.nursat.net - - [12/Jun/2000:02:29:01 -0600] "GET
/site_14.jpg HTTP/1.0" 200 0 "http://home_page.html" "Mozilla/4.0 (compatible;
MSIE 5.0; Windows 95; DigExt)"
dial-195-82-27-149.gw4.ala1.nursat.net - - [12/Jun/2000:02:29:05 -0600] "GET
/site_15.jpg HTTP/1.0" 200 4217 "http://home_page.html" "Mozilla/4.0
(compatible; MSIE 5.0; Windows 95; DigExt)"
```

1. Source of Trace:

   My network

2. Detect was generated by:

   a. IP Filter log

      Description of Fields:

      12/06/2000 02:21:47.065873[*time-stamp*] le0[*interface]*
      @150:2[*rule-set group:number*] b[*action b=block p=pass*]
      dial-195-82-27-149.GW4.ALA1.Nursat.net,137[*source ip,port*] ->
      web.server.com,137[*destination ip,port*] PR udp[*transport protocol*]
      len 20[*IP header length*] 78[*total packet length*]

   b. **Supporting information in:**

      1. tcpdump of shadow sensor log:
      02:21:47.046973[*time-stamp*] dial-195-82-27-149.GW4.ALA1.Nursat.net.netbios-ns
      [*source ip,port*] > web.server.com.netbios-ns[*destination ip,port*]:
      udp[*transport protocol*] 50[*payload size*] (ttl 109, id 45771)

2. http server log
dial-195-82-27-149.gw4.ala1.nursat.net[*source address*] - -
[12/Jun/2000:02:21:49 -0600][*timestamp*] "GET / HTTP/1.0"[*http request*]
302[*response code*] 228[*# of bytes transmitted*]
http://www.epa.gov/ozone/othlinks.html[*referring URL*]
"Mozilla/4.0 (compatible; MSIE 5.0; Windows 95; DigExt)"[*source browser info*]

3. Probability the source address was spoofed:

Low -- although the RIPE Whois website gave a description of IP 195.82.27.149 as belonging to Nursat in Almaty, Kazakstan, the web logs indicated what I would consider normal interactive communication, although it was a simple browse of the initial web pages.

4. Description of Attack:

a. Although normal requests were being made to our DMZ web site, additional UDP netbios, port 137, packets were intermixed with the traffic to port 80.

5. Attack Mechanism:

a. It is possible to obtain information from hosts running Microsoft Windows by using the NBTSTAT program. The Windows host cannot refuse to answer the request from an NT server. It is possible to determine such properties as machine name, workgroup/domain name and login name.

b. Knowing the domain name and username of a remote system gives the attacker two of three pieces of information required to mount shares. Password cracking or guessing would supply the final piece.

c. This could be described as a reconnaissance attack on a web server to obtain information for further attempts to compromise the system.

d. By intermixing the traffic with normal web traffic, the attacker might hope to obscure the additional udp traffic.

6. Correlation:

a. This method of netbios reconnaissance is described in:
Northcutt, S., Network Intrusion Detection, An Analyst's Handbook,
New Riders, 1999, p133-135.

b. Similar udp traffic was created by using nbtstat from a separate subnet to query a system on my subnet.

```
13:41:13.252416 192.168.100.45.netbios-ns >
web.server.com.netbios-ns: udp 50 (ttl 125, id 63549)
                  4500 004e f83d 0000 7d11 07bc c0a8 642d
                  c0a8 9c63 0089 0089 003a 819d 00ec 0000
                  0001 0000 0000 0000 2043 4b41 4141 4141
                  4141 4141 4141
```

7. Evidence of active targeting:

   a. Our DMZ web server was specifically targeted.

8. Severity: -3

   (Criticality + Lethality) - (System + Network Countermeasures) = Severity
       3   +   1   -   4 + 3 = -3
    Criticality = 3 -- Destination was Web server
    Lethality   = 1 -- Attack will not do damage
    System   = 4 - Older OS, but systems fully patched
    Network   = 3 -- Personal firewall which restricts some traffic

9. Defensive recommendations:

   None. Defenses were sufficient to stop the attempted reconnaissance.
   The DMZ web server runs a "personal firewall" which prohibits
   netbios traffic. Furthermore, the OS is not Windows based and is
   therefore not vulnerable.

10. Multiple Choice Question:

   NBTSTAT can be used to:
   a. Display network statistics
   b. Provide domain name and user name of remote Windows based systems.
   c. Perform IP address lookups
   d. exploit static routing on Windows based systems
   Answer: B

Detect 7

IP Filter Log:

```
02/06/2000 12:57:45.293413  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
02/06/2000 13:01:15.755378  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
02/06/2000 13:01:25.756481  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
03/06/2000 11:07:14.479363  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
03/06/2000 11:12:36.342037  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
03/06/2000 11:12:46.485522  le0 @0:1 b 24.65.253.65.ab.wave.home.com ->
web.server.com PR 54 len 24 (68)
```

Supporting Http server Log:

```
24.65.253.65.ab.wave.home.com - - [02/Jun/2000:12:57:45 -0600] "HEAD / HTTP/1.1"
301 0 "-" "Mozilla/4.5 [en] (Win98; I)"
24.65.253.65.ab.wave.home.com - - [02/Jun/2000:12:57:45 -0600] "HEAD /ABC/
HTTP/1.1" 302 0 "-" "Mozilla/4.5 [en] (Win98; I)"
24.65.253.65.ab.wave.home.com - - [02/Jun/2000:12:57:45 -0600] "HEAD
/ABC/home_page.html HTTP/1.1" 200 0 "-" "Mozilla/4.5 [en] (Win98; I)"

24.65.253.65.ab.wave.home.com - - [03/Jun/2000:11:07:14 -0600] "HEAD / HTTP/1.1"
301 0 "-" "Mozilla/4.5 [en] (Win98; I)"
24.65.253.65.ab.wave.home.com - - [03/Jun/2000:11:07:14 -0600] "HEAD /ABC/
HTTP/1.1" 302 0 "-" "Mozilla/4.5 [en] (Win98; I)"
24.65.253.65.ab.wave.home.com - - [03/Jun/2000:11:07:14 -0600] "HEAD
/ABC/home_page.html HTTP/1.1" 200 0 "-" "Mozilla/4.5 [en] (Win98; I)"
```

Supporting tcpdump log:

```
12:57:44.707319 24.65.253.65.ab.wave.home.com.1728 > web.server.com.80: S
326703:326703(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
12:57:44.709016 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1728: S
3583397621:3583397621(0) ack 326704 win 10192 <mss 1456> (DF)
12:57:44.846772 24.65.253.65.ab.wave.home.com.1728 > web.server.com.80: . ack
3583397622 win 8736 (DF)
12:57:44.859600 24.65.253.65.ab.wave.home.com.1728 > web.server.com.80: P
326704:326830(126) ack 3583397622 win 8736 (DF)
12:57:44.861145 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1728: . ack
326830 win 10192 (DF)
12:57:44.864730 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1728: P
3583397622:3583397812(190) ack 326830 win 10192 (DF)
12:57:45.005597 24.65.253.65.ab.wave.home.com.1728 > web.server.com.80: F
326830:326830(0) ack 3583397812 win 8546 (DF)
12:57:45.006781 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1728: . ack
326831 win 10192 (DF)
12:57:45.096670 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1728: F
3583397812:3583397812(0) ack 326831 win 10192 (DF)
12:57:45.015812 24.65.253.65.ab.wave.home.com.1732 > web.server.com.80: S
327009:327009(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
12:57:45.017269 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1732: S
3583489103:3583489103(0) ack 327010 win 10192 <mss 1456> (DF)
12:57:45.165180 24.65.253.65.ab.wave.home.com.1732 > web.server.com.80: . ack
3583489104 win 8736 (DF)
```

```
12:57:45.166478 24.65.253.65.ab.wave.home.com.1732 > web.server.com.80: P
327010:327136(126) ack 3583489104 win 8736 (DF)
12:57:45.168134 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1732: . ack
327136 win 10192 (DF)
12:57:45.235463 24.65.253.65.ab.wave.home.com.1728 > web.server.com.80: . ack
3583397813 win 8546 (DF)
12:57:45.242430 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
(ttl 11, id 0, optlen=4 IPOPT-148{4})
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c b30c 0000 0101 0602 0404 4800
                        7000 0000 0001
12:57:45.429167 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1732: P
3583489104:3583489296(192) ack 327136 win 10192 (DF)
12:57:45.432915 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1732: F
3583489296:3583489296(0) ack 327136 win 10192 (DF)
12:57:45.572630 24.65.253.65.ab.wave.home.com.1732 > web.server.com.80: . ack
3583489297 win 8544 (DF)
12:57:45.573094 24.65.253.65.ab.wave.home.com.1732 > web.server.com.80: F
327136:327136(0) ack 3583489297 win 8544 (DF)
12:57:45.574312 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1732: . ack
327137 win 10192 (DF)
12:57:45.582486 24.65.253.65.ab.wave.home.com.1740 > web.server.com.80: S
327575:327575(0) win 8192 <mss 1456,nop,nop,sackOK> (DF)
12:57:45.584044 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1740: S
3583619619:3583619619(0) ack 327576 win 10192 <mss 1456> (DF)
12:57:45.723495 24.65.253.65.ab.wave.home.com.1740 > web.server.com.80: . ack
3583619620 win 8736 (DF)
12:57:45.726612 24.65.253.65.ab.wave.home.com.1740 > web.server.com.80: P
327576:327716(140) ack 3583619620 win 8736 (DF)
12:57:45.728301 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1740: . ack
327716 win 10192 (DF)
12:57:45.732237 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1740: P
3583619620:3583619866(246) ack 327716 win 10192 (DF)
12:57:45.735455 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1740: F
3583619866:3583619866(0) ack 327716 win 10192 (DF)
12:57:45.871531 24.65.253.65.ab.wave.home.com.1740 > web.server.com.80: . ack
3583619867 win 8490 (DF)
12:57:45.879663 24.65.253.65.ab.wave.home.com.1740 > web.server.com.80: F
327716:327716(0) ack 3583619867 win 8490 (DF)
12:57:45.880780 web.server.com.80 > 24.65.253.65.ab.wave.home.com.1740: . ack
327717 win 10192 (DF)
13:01:15.754807 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c 230d 0000 0101 0602 0404 4800
                        0000 0000 0001
13:01:25.755750 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c 230d 0000 0101 0602 0404 4800
                        0000 0000 0001
```

Tcpdump of Jun 3rd, 2000 ip-proto-54 traffic only

```
11:07:14.473374 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
(ttl 11, id 0, optlen=4 IPOPT-148{4})
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c 580c 0000 0101 0602 0404 4800
                        cb00 0000 0001
11:12:36.331263 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
(ttl 11, id 0, optlen=4 IPOPT-148{4})
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c 230d 0000 0101 0602 0404 4800
                        0000 0000 0001
11:12:46.474651 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44
(ttl 11, id 0, optlen=4 IPOPT-148{4})
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c 230d 0000 0101 0602 0404 4800
                        0000 0000 0001
```

1. Source of Trace:

   My network

2. Detect was generated by:

   a. IP Filter Log

      Description of Fields

      02/06/2000 12:57:45.293413[*timestamp*] le0[*interface*]
      @0:1[*rule-set group:number*] b[*action b=block p=pass*]
      24.65.253.65.ab.wave.home.com[*source ip,port* ->
      web.server.com[*destination ip,port*]PR 54[*transport protocol*]
      len 24[*IP header length*] (68)[*total packet size*]

   b. **Supporting information in:**

      1. http server log:
         24.65.253.65.ab.wave.home.com[source *address*] - -
         [02/Jun/2000:12:57:45 -0600][*timestamp*]
         "HEAD /ABC/home_page.html HTTP/1.1"[*http request*]
         200[*response code*] 0[*# of bytes transferred*] "-"[*referring URL*]
         "Mozilla/4.5 [en] (Win98; I)"[*source browser info*]

      2. tcpdump of shadow sensor log:
         12:57:45.242430[*timestamp*] 24.65.253.65.ab.wave.home.com[source *ip,port*] >
         web.server.com[destination *ip,port*]: ip-proto-54[*transport protocol*]
         44[*payload size*] (ttl[*time to live*] 11, id 0, optlen=4[*option length*]
         IPOPT-148{4})[*option code*]
                        4600 0044 0000 0000 0b36 b147 1841 fd41
                        c0a8 9c63 9404 0000 0006 0800 0000 0000
                        0006 002c b30c 0000 0101 0602 0404 4800
                        7000 0000 0001 [*packet contents in hex*]

3. Probability the source address was spoofed:

   Low -- The IP address, 24.65.253.65, information from ARIN Whois describes this as belonging to Shaw Fiberlink, an ISP in Calgary, Alberta, Canada. Normal TCP traffic occurs during this trace, so it is likely this is the real address.

4. Description of Attack:

   a. Anomalous traffic, identified as IP protocol 54, NMBA ARP, was detected embedded with legitimate http traffic on our DMZ web server.

   b. The requests to the web site were somewhat unusual, in that only metadata (HEAD request) used for the initial web site. It is only partly unusual, because the referring URL was not the typical URL of some search engine.

   c. The initial SYN packets of each http request used the uncommon TCP option SACK, (see RFC 2018), for selective acknowledgements once communications were established.

   d. The protocol 54 packets did not seem to conform to the actual format described in RFC 1735. The IP header is 24 bytes, specifying option 148, with 4 bytes of option data.

   e. The packets are either seriously malformed packets, or crafted. It is interesting to note the coincidence of the protocol ID number,54 in hex is 0x36, while tcp's protocol ID in hex is 0x06. Furthermore, the supposed options payload of 4 bytes is exceeded.

   f. This same pattern occurred twice, once on June 02 at 1pm, and again on June 03 at 11am. The same three http requests were made, and three anomalous protocol 54 packets were sent the web server. The first packet of the set of three differed slightly from the second two, while the remaining pair were identical, and occurred a few minutes after the last request and been completed.

   g. The purpose of this attack is unknown.

5. Attack Mechanism:

   a. CVE-1999-0817,indicates a "Lynx WWW client allows a remote attacker to specify command-line parameters which Lynx uses when calling external programs to handle certain protocols, e.g. telnet." It may be possible the attacker may be trying something similar, testing effects of uncommon protocols on a remote host.

   b. The attacker may be attempting to hide the anomalous traffic within legitimate http requests.

   c. The packets could be simply malformed packets due to errors in setting the SARK tcp option.

6. Correlation:

   This singular incident, with it's unusual aspects make me very suspicious that this is an attempted attack. However, I have been unable to find any specific incident references to protocol 54.

   I have not seen this occur before.

7. Evidence of Active Targeting:

   The attack was directed specifically at our DMZ web server.

8. Severity: -1

   (Criticality + Lethality) - (System + Network Countermeasures) = Severity
   3 + 3 - 4 + 3 = -1
   Criticality = 3 -- Destination was our Web server
   Lethality = 3 -- Unknown if attack could do damage
   System = 4 – Older OS, but systems fully patched
   Network = 3 -- Personal firewall which restricts some traffic

9. Defensive recommendations:

   The defenses were sufficient to stop the anomalous traffic because packets with options set were not allowed. It is uncertain how the personal firewall would react to unknown protocols and further testing and evaluation would be recommended. The default rule should be defined such that all packets should be blocked, regardless of protocol.

10 Multiple Choice Question:

   11:12:36.331263 24.65.253.65.ab.wave.home.com > web.server.com: ip-proto-54 44 (ttl 11, id 0, optlen=4 IPOPT-148{4})
   4600 0044 0000 0000 0b36 b147 1841 fd41
   c0a8 9c63 9404 0000 0006 0800 0000 0000
   0006 002c 230d 0000 0101 0602 0404 4800
   0000 0000 0001

   The above tcpdump trace indicate a packet with:
   a. IP header length of 24
   b. IP protocol 54
   c. Options data exceeds specified length
   d. All of the above
   Answer: D

Detect 8

Shadow Log: Jun 7, 2000 08:00

```
08:00:49.858418 129.82.139.235.1040 > 192.168.156.255.161: GetRequest(11)
08:00:49.858972 129.82.139.235.1040 > 192.168.156.254.161: GetRequest(11)
08:00:49.859523 129.82.139.235.1040 > 192.168.156.253.161: GetRequest(11)
08:00:49.860075 129.82.139.235.1040 > 192.168.156.252.161: GetRequest(11)
08:00:49.860624 129.82.139.235.1040 > 192.168.156.251.161: GetRequest(11)
08:00:49.861209 129.82.139.235.1040 > 192.168.156.250.161: GetRequest(11)
08:00:49.861726 129.82.139.235.1040 > 192.168.156.249.161: GetRequest(11)
08:00:49.862276 129.82.139.235.1040 > 192.168.156.248.161: GetRequest(11)
.
.
.
08:00:52.324987 129.82.139.235.1040 > 192.168.156.130.161: GetRequest(11)
08:00:52.325541 129.82.139.235.1040 > 192.168.156.129.161: GetRequest(11)
08:00:52.326089 129.82.139.235.1040 > 192.168.156.128.161: GetRequest(11)
08:00:52.332046 129.82.139.235.1040 > 192.168.156.125.161: GetRequest(11)
08:00:53.143960 129.82.139.235.1040 > 192.168.156.94.161: GetRequest(11)
08:00:53.145908 129.82.139.235.1040 > 192.168.156.99.161: GetRequest(11)
08:00:53.145908 129.82.139.235.1040 > 192.168.156.99.161: GetRequest(11)
08:00:53.175050 129.82.139.235.1040 > 192.168.156.91.161: GetRequest(11)
08:00:53.179085 129.82.139.235.1040 > 192.168.156.90.161: GetRequest(11)
08:00:53.988048 129.82.139.235.1040 > 192.168.156.14.161: GetRequest(11)
```

Supporting IP Filter Log:

```
07/06/2000 08:00:49.913720  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.255,161 PR udp len 20 72
07/06/2000 08:00:49.921069  le1 @250:6 b 129.82.139.235,1040 -> 192.168.156.246
161 PR udp len 20 72
07/06/2000 08:00:49.923153  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.245,161 PR udp len 20 72
07/06/2000 08:00:49.931270  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.247,161 PR udp len 20 72
07/06/2000 08:00:50.720193  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.235,161 PR udp len 20 72
07/06/2000 08:00:50.738759  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.219,161 PR udp len 20 72
07/06/2000 08:00:50.740563  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.218,161 PR udp len 20 72
07/06/2000 08:00:50.742356  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.215,161 PR udp len 20 72
07/06/2000 08:00:50.747697  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.209,161 PR udp len 20 72
07/06/2000 08:00:50.749603  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.207,161 PR udp len 20 72
07/06/2000 08:00:50.763749  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.230,161 PR udp len 20 72
07/06/2000 08:00:50.765350  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.229,161 PR udp len 20 72
07/06/2000 08:00:50.766958  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.227,161 PR udp len 20 72
```

```
07/06/2000 08:00:50.768984  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.226,161 PR udp len 20 72
07/06/2000 08:00:50.771701  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.216,161 PR udp len 20 72
07/06/2000 08:00:50.773294  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.213,161 PR udp len 20 72
07/06/2000 08:00:50.775428  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.211,161 PR udp len 20 72
07/06/2000 08:00:50.778202  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.203,161 PR udp len 20 72
07/06/2000 08:00:50.779935  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.204,161 PR udp len 20 72
07/06/2000 08:00:50.796480  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.202,161 PR udp len 20 72
07/06/2000 08:00:50.798159  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.195,161 PR udp len 20 72
07/06/2000 08:00:51.568166  le0 @101:4 b 192.168.156.14 -> 129.82.139.235 PR
icmp len 20 100 icmp 3/3
  for 129.82.139.235,1040 - 192.168.156.165,161 PR udp len 20 72
07/06/2000 08:00:52.371364  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.144,161 PR udp len 20 72
07/06/2000 08:00:52.386656  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.128,161 PR udp len 20 72
07/06/2000 08:00:52.392475  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.143,161 PR udp len 20 72
07/06/2000 08:00:52.402988  le1 @250:6 b 129.82.139.235,1040 ->
192.168.156.141,161 PR udp len 20 72
07/06/2000 08:00:54.043527  le0 @101:4 b 192.168.156.14 -> 129.82.139.235 PR
icmp len 20 100 icmp 3/3
  for 129.82.139.235,1040 - 192.168.156.14,161 PR udp len 20 72
```

Supporting tcpdump of one sample packet:

```
08:00:49.858418 129.82.139.235.1040 > 192.168.156.255.161: GetRequest(11)
                        4500 0048 bc2e 0000 1e11 7ee7 8152 8beb
                        c0a8 9cff 0410 00a1 0034 56e1 302a 0201
                        0004 06 70 7562 6c69 63a0 1d02 0102 0201
                        0002 0100 3012
```

1. Source of Trace:

   My network

2. Detect was generated by:

   a. Shadow IDS

      Description of Shadow log

      08:00:49.858418[*timestamp*] 129.82.139.235.1040[*source ip,port*] >
      192.168.156.255.161[*destination ip,port*]:
      GetRequest(11)[*snmp message*]

   b. Supporting information in:

      IP Filter Log

      07/06/2000 08:00:49.913720[*timestamp*] le1[*interface*]

@250:6[*rule-set group:number*] b[*action b=block p=pass*]
129.82.139.235,1040[*source ip,port*] ->
192.168.156.255,161[*destination ip,port*]
PR udp[*transport protocol*] len 20[*ip header length*] 72[*total packet size*]

3. Probability the source address was spoofed:

   Low -- The IP address was located within our Class B network address space and the attacker might want to receive responses.

4. Description of Attack:

   a. The address space of my network is sequentially scanned in reverse order for udp port 161, commonly used for the snmp service.

   b. Systems within the DMZ attempted to respond with icmp port unreachable messages.

   c. This pattern was repeated approximately every 12 hours, and occurred on another subnet within our Class B network.

   d. After I informed the network managers, they suspected that the traffic was typical of misconfigured JetAdmin software. They contacted the person responsible for the offending subnet and found that a new NT system had been installed at that specific IP address. The system was rebuilt and the traffic subsequently ceased.

   e. This appears to be a **false positive** caused by a misconfigured NT system.

5. Attack Mechanism:

   a. SNMP GetRequest messages are sent to all IP addresses within a network.

   b. The SNMP request used the default "public" password, seen in tcpdumps of the packets (06***70 7562 6c69 63***a0), in an attempt to get system information from any system running the SNMP service.

   c. This is a host reconnaissance method, attempting to use a common password on the SNMP service to provide the attacker with valuable system information and network configuration that could lead to exploiting specific OS vulnerabilities and social engineering.

6. Correlation:

   This method of reconnaissance using SNMP is described in:
   Northcutt, S., Network Intrusion Detection, An Analyst's Handbook,
   New Riders, 1999, p132.

7. Evidence of active targeting:

   The attack was directed at the entire Class B network, not our specific subnet.

8. Severity: -7

(Criticality + Lethality) - (System + Network Countermeasures) = Severity
1 + 1 - 4 + 4 = -7
Criticality = 1 -- Destination was entire network address space
Lethality = 1 -- Attack will not do damage, but could reveal systems information
System = 4 – Older OS, but systems fully patched
Network = 4 – Restrictive firewall

9. Defensive recommendations:

The defenses were sufficient to detect and prevent any response to SNMP queries.

10. Multiple choice question:

SNMP scans are often successful because:
a. It is a necessary service that is seldom blocked by a firewall
b. A large number of sites fail to change the default password
c. It uses fragmented UDP as the transport mechanism
d. It is a rarely used attack.
Answer: B

Detect 9

IP Filter log file:

```
09/06/2000 10:53:01.289884  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.128,domain PR tcp len 20 40 -SF
09/06/2000 10:53:01.553755  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.141,domain PR tcp len 20 40 -SF
09/06/2000 10:53:01.590509  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.143,domain PR tcp len 20 40 -SF
09/06/2000 10:53:01.610748  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.144,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.631896  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.195,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.771445  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.202,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.788592  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.203,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.810587  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.204,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.869133  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.207,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.909434  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.209,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.951039  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.211,domain PR tcp len 20 40 -SF
09/06/2000 10:53:02.989991  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.213,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.030181  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.215,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.049858  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.216,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.088753  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.218,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.108627  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.219,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.249631  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.226,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.269905  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.227,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.308662  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.229,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.329288  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.230,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.427987  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.235,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.629341  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.245,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.648646  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.246,domain PR tcp len 20 40 -SF
09/06/2000 10:53:03.669998  le1 @250:6 b 63.226.11.117,domain ->
192.168.156.247,domain PR tcp len 20 40 -SF
```

Supporting tcpdump of Shadow sensor log Jun 9th, 2000:

```
10:52:58.959065 63.226.11.117.domain > 192.168.156.14.domain: SF
1396531279:1396531279(0) win 1028
```

```
10:52:58.960796 192.168.156.14.domain > 63.226.11.117.domain: R 0:0(0) ack
1396531280 win 0 (DF)
10:53:00.482397 63.226.11.117.domain > 192.168.156.90.domain: SF
7267284:7267284(0) win 1028
10:53:00.501290 63.226.11.117.domain > 192.168.156.91.domain: SF
7267284:7267284(0) win 1028
10:53:00.558722 63.226.11.117.domain > 192.168.156.94.domain: SF
7267284:7267284(0) win 1028
10:53:00.561927 192.168.156.94.domain > 63.226.11.117.domain: R 0:0(0) ack
7267285 win 0 (DF)
10:53:00.660028 63.226.11.117.domain > 192.168.156.99.domain: SF
7267284:7267284(0) win 1028
10:53:00.661498 192.168.156.99.domain > 63.226.11.117.domain: R 0:0(0) ack
7267285 win 0 (DF)
10:53:01.181291 63.226.11.117.domain > 192.168.156.125.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.183261 192.168.156.125.domain > 63.226.11.117.domain: R 0:0(0) ack
1869570883 win 0
10:53:01.240988 63.226.11.117.domain > 192.168.156.128.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.242475 192.168.156.128.domain > 63.226.11.117.domain: R 0:0(0) ack
1869570883 win 0 (DF)
10:53:01.259506 63.226.11.117.domain > 192.168.156.129.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.280524 63.226.11.117.domain > 192.168.156.130.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.300963 63.226.11.117.domain > 192.168.156.131.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.320478 63.226.11.117.domain > 192.168.156.132.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.339467 63.226.11.117.domain > 192.168.156.133.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.359025 63.226.11.117.domain > 192.168.156.134.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.379564 63.226.11.117.domain > 192.168.156.135.domain: SF
1869570882:1869570882(0) win 1028
10:53:01.399716 63.226.11.117.domain > 192.168.156.136.domain: SF
1869570882:1869570882(0) win 1028
.
.
.
10:53:01.980016 63.226.11.117.domain > 192.168.156.165.domain: SF
488890765:488890765(0) win 1028
10:53:01.981837 192.168.156.165.domain > 63.226.11.117.domain: R 0:0(0) ack
488890766 win 0 (DF)
10:53:02.000198 63.226.11.117.domain > 192.168.156.166.domain: SF
488890765:488890765(0) win 1028
.
.
.
10:53:03.719545 63.226.11.117.domain > 192.168.156.252.domain: SF
1262613288:1262613288(0) win 1028
10:53:03.739515 63.226.11.117.domain > 192.168.156.253.domain: SF
1262613288:1262613288(0) win 1028
10:53:03.762133 63.226.11.117.domain > 192.168.156.254.domain: SF
1262613288:1262613288(0) win 1028
```

Supporting tcpdump of Shadow sensor log Jun 10th, 2000:

```
15:20:34.793331 194.179.163.253.domain > 192.168.156.14.domain: SF
2123322408:2123322408(0) win 1028 (ttl 17, id 39426)
15:20:34.795051 192.168.156.14.domain > 194.179.163.253.domain: R 0:0(0) ack
2123322409 win 0 (DF) (ttl 17, id 43827)
15:20:36.313615 194.179.163.253.domain > 192.168.156.90.domain: SF
1818512685:1818512685(0) win 1028 (ttl 17, id 39426)
15:20:36.339501 194.179.163.253.domain > 192.168.156.91.domain: SF
1818512685:1818512685(0) win 1028 (ttl 17, id 39426)
15:20:36.390706 194.179.163.253.domain > 192.168.156.94.domain: SF
1818512685:1818512685(0) win 1028 (ttl 17, id 39426)
15:20:36.394037 192.168.156.94.domain > 194.179.163.253.domain: R 0:0(0) ack
1818512686 win 0 (DF) (ttl 17, id 60247)
15:20:36.491461 194.179.163.253.domain > 192.168.156.99.domain: SF
445885294:445885294(0) win 1028 (ttl 17, id 39426)
15:20:36.492898 192.168.156.99.domain > 194.179.163.253.domain: R 0:0(0) ack
445885295 win 0 (DF) (ttl 17, id 45967)
15:20:37.018739 194.179.163.253.domain > 192.168.156.125.domain: SF
445885294:445885294(0) win 1028 (ttl 17, id 39426)
15:20:37.020722 192.168.156.125.domain > 194.179.163.253.domain: R 0:0(0) ack
445885295 win 0 (ttl 255, id 34879)
15:20:37.076271 194.179.163.253.domain > 192.168.156.128.domain: SF
445885294:445885294(0) win 1028 (ttl 17, id 39426)
15:20:37.077826 192.168.156.128.domain > 194.179.163.253.domain: R 0:0(0) ack
445885295 win 0 (DF) (ttl 17, id 43828)
15:20:37.098904 194.179.163.253.domain > 192.168.156.129.domain: SF
445885294:445885294(0) win 1028 (ttl 17, id 39426)
15:20:37.111081 194.179.163.253.domain > 192.168.156.130.domain: SF
445885294:445885294(0) win 1028 (ttl 17, id 39426)
.
.
.

15:20:37.809291 194.179.163.253.domain > 192.168.156.164.domain: SF
1206575727:1206575727(0) win 1028 (ttl 17, id 39426)
15:20:37.819391 194.179.163.253.domain > 192.168.156.165.domain: SF
1206575727:1206575727(0) win 1028 (ttl 17, id 39426)
15:20:37.821107 192.168.156.165.domain > 194.179.163.253.domain: R 0:0(0) ack
1206575728 win 0 (DF) (ttl 17, id 43829)
15:20:37.836398 194.179.163.253.domain > 192.168.156.166.domain: SF
1206575727:1206575727(0) win 1028 (ttl 17, id 39426)
.
.
.
15:20:39.551338 194.179.163.253.domain > 192.168.156.252.domain: SF
1680825193:1680825193(0) win 1028 (ttl 17, id 39426)
15:20:39.570478 194.179.163.253.domain > 192.168.156.253.domain: SF
1680825193:1680825193(0) win 1028 (ttl 17, id 39426)
15:20:39.590372 194.179.163.253.domain > 192.168.156.254.domain: SF
1680825193:1680825193(0) win 1028 (ttl 17, id 39426)
```

1. Source of Trace:

   My network

2. Detect was generated by:

   a. IP Filter log

      Description of Fields:

      09/06/2000 10:53:01.289884[*timestamp*] le1[*interface*]
      @250:*6[rule-set group:number*] b[*action block*]
      63.226.11.117,domain[*source IP,port*] -> 192.168.156.128,domain[*destination IP,port*] PR tcp[*transport protocol*] len *20[IP header length*]
      40[*total packet length*] -SF[*tcp flags*]

   b. Shadow tcpdump file

      10:52:58.959065[*timestamp*] 63.226.11.117.domain[*source IP,port* >
      192.168.156.14.domain[*destination IP,port*]: SF[*tcp flags*]
      1396531279:1396531279[*sequence number*](0)[*payload size*] win 1028[*window size*]

3. Probability the source address was spoofed:

   Low -- Attacker would desire to see responses from sent packets
          According to the ARIN Whois website, the IP address 63.226.11.117
          is part of an 8 ip subnet registered to the Scottsdale Senior Center
          in Scottsdale, Arizona.

4. Description of Attack:

   a. Our entire subnet address space was sequentially scanned for active port 53 services, commonly used for the Domain Name service.

   b. Sequence numbers were identical for a 50 ip address range before changing to an new value. Additionally, the illegal flag combination of SYN FIN was used in each packet. These indicate the packets were crafted.

   c. What made this trace especially interesting was that I was able to contact the system administrator within an hour of the scan. He informed me the IP address was for their NT server that supports a computer lab for senior citizens. He was able to examine the system and take action, in hopes of preventing the attacker from retrieving the information gained by the probe. The next day, we were scanned again, as seen in the second trace above, from a system of the Telesystem Srl ISP in Italy. It produced a very similar signature to the previous day's scan. Perhaps the attacker was thwarted from retrieving the information of the previous day and was forced to rescan. Maybe wishful thinking on my part, it could just be the same tool, coincidentally used on the next day. However, I hadn't seen this particular signature before.

5. Attack Mechanism:

   a. This trace is of a scan for DNS servers within our address space.

   b. A system running the a service on that port will respond to the source address with a SYN-ACK packet, indicating to the attacker,

a potential service to exploit.

c. If the system is not running a service on that port, it will respond with a RESET, informing the attacker the service is not available.

d. By locating active DNS servers, the attacker can then try DoS or system compromises by utilizing an array of vulnerabilities including (to name a just a few):

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-1999-0048	Talkd, when given corrupt DNS information, can be used to execute arbitrary commands with root privileges.
CVE-1999-0101	Buffer overflow in AIX and Solaris "gethostbyname" library call allows root access through corrupt DNS host names.
CVE-1999-0184	When compiled with the -DALLOW_UPDATES option, bind allows dynamic updates to the DNS server, allowing for malicious modification of DNS records.
CVE-1999-0274	Denial of service in Windows NT DNS servers through malicious packet which contains a response to a query that wasn't made.
CVE-1999-0275	Denial of service in Windows NT DNS servers by flooding port 53 with too many characters.

e. The attacker crafted packets, using the illegal flag combination SYN-FIN in a futile hope of avoiding detection by firewall and ID systems.

f. Evidence of a possible, distributed scan came the following day from a second IP address in a different country, indicating a potentially serious, persistent hacker targeting our network.

6. Correlation:

a. The SYN-FIN Scanning is described on Page 114 of Intrusion Detection and Packet Filtering: How It Really Works by: Vicki Irwin & Hal Pomeranz, Sans GIAC Course 2.2, May 9, 2000

b. There was also a CERT Advisory, CA-2000-03, Continuing Compromises of Nameservers Advisory, which indicates continuing active targeting of DNS servers to gain privileged compromise of the systems.

7. Evidence of active targeting:

The attack was directed at our network over two consecutive days from different IP addresses.

8. Severity: -4

```
(Criticality + Lethality) - (System + Network Countermeasures) = Severity
    3             1              4 + 4 = -4
 Criticality = 3 -- Scanning specifically for DNS servers
 Lethality   = 1 -- Attack is a scan and will not do damage
 System      = 4 -- Mix of new and old OS's, but all systems fully patched
 Network     = 4 -- Restrictive network firewall
```

9. Defensive recommendations:

The defenses were sufficient for the internal network which is shielded by a firewall, however, systems in the DMZ did respond with RESET-ACK packets, alerting the attacker to their existence. Improved filtering of unused services would be advisable on the personal firewalls of the DMZ systems, or implementation of a secondary firewall to specifically protect the DMZ systems.

10 Multiple Choice Question:

In the above trace, a RESET-ACK:
a. is an unsolicited response from a spoofing attack
b. indicates a host is present at that IP address
c. indicates the requested service is unavailable
d. Both b and c.
Answer: D

Detect 10

```
21/05/2000 21:48:22.686907  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.128,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:22.932809  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.141,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:22.971515  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.143,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:22.990474  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.144,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.013268  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.195,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.151922  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.202,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.171656  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.203,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.190741  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.204,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.250198  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.207,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.289213  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.209,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.333222  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.211,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.370654  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.213,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.413825  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.215,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.430781  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.216,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.468401  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.218,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.492253  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.219,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.630133  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.226,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.650403  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.227,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.691434  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.229,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.710296  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.230,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:24.813944  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.235,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:25.012166  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.245,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:25.028146  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.246,pop-2 PR tcp len 20 40 -SF
21/05/2000 21:48:25.056889  le1 @250:6 b homer.ligo-la.caltech.edu,pop-2 ->
192.168.156.247,pop-2 PR tcp len 20 40 -SF
```

1. Source of Trace:

   My subnet

2. Detect was generated by:

   a. IP Filter log

   b. Description of IP Filter log

      21/05/2000 21:48:22.686907[timestamp] le1[interface]
      @250:6[rule-set group:number] b[action block]
      homer.ligo-la.caltech.edu,pop-2[source IP,port] ->
      192.168.156.128,pop-2[destination IP,port] PR tcp[transport protocol]
      len 20[IP header length] 40[total packet lenght] -SF[tcp flags]

3. Probability the source address was spoofed:

   Low -- The attacker may want to see the response to the packets sent. Furthermore, the IP address is at an edu domain, which often are subject to system compromises.

4. Description of Attack:

   a. This appears to be a simplistic sequential scan for pop-2 servers.

   b. It is amazing to see a scan like this, more for the fact that pop-2 is so out dated, it is hard to believe the attacker would waste time doing this scan. However, a system may be especially vulnerable if the service has not been maintained and it has been forgotten that it is still running on the system.

   c. The only other notable feature of this scan is the use of the SYN-FIN combination in an attempt to execute a stealthy scan.

   d. This is probably a new "script kiddie" and actually presents a real opportunity for an education in ethics if they could be identified.

   e. This is also a good example of an old attack that is still being used today.

5. Attack Mechanism:

   a. The attacker sends TCP packets with SYN & FIN flags set to port 109 in an attempt to locate a pop-2 server while avoiding detection by firewalls and ID systems.

   b. There are still recent vulnerabilities that have been found in pop2 servers that may be exploited. By locating these severs, an attacker may be able to match an exploit to a system vulnerability. The most recent vulnerability I found was:

      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.

6. Correlation:

   a. The SYN-FIN Scanning is described on Page 114 of Intrusion Detection and Packet Filtering: How It Really Works by: Vicki Irwin & Hal Pomeranz, Sans GIAC Course 2.2, May 9, 2000

7. Evidence of active targeting:

The attack was directed at this network.

8 Severity: -6

(Criticality + Lethality) - (System + Network Countermeasures) = Severity
1 1 4 + 4 = -6
Criticality = 1 -- Scanning specifically for a legacy server
Lethality = 1 -- Attack is a scan and will not do damage
System = 4 -- Mix of new and old OS's, but all systems fully patched
Network = 4 -- Restrictive network firewall

9 Defensive recommendations:

The defenses were sufficient against this attack. No pop-2 servers are in use on this network.

10. Multiple Choice Question:

The purpose of a port scan is to:
a. evaluate system loading
b. determine packet round trip times
c. match an exploit to a system with known vulnerability
d. Denial of Service to the targeted port
Answer: C

Last Updated: January 21st, 2019

Upcoming Training

SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC503: Intrusion Detection In-Depth	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201902,	Feb 27, 2019 - Apr 04, 2019	vLive
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Madrid March 2019	Madrid, Spain	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event
Community SANS New York SEC503	New York, NY	Apr 29, 2019 - May 04, 2019	Community SANS
SANS Security West 2019	San Diego, CA	May 09, 2019 - May 16, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VA	May 19, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, Netherlands	May 20, 2019 - May 25, 2019	Live Event
San Antonio 2019 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	May 28, 2019 - Jun 02, 2019	vLive
SANS San Antonio 2019	San Antonio, TX	May 28, 2019 - Jun 02, 2019	Live Event
SANS London June 2019	London, United Kingdom	Jun 03, 2019 - Jun 08, 2019	Live Event
SANSFIRE 2019	Washington, DC	Jun 15, 2019 - Jun 22, 2019	Live Event
Security Operations Summit & Training 2019	New Orleans, LA	Jun 24, 2019 - Jul 01, 2019	Live Event
SANS Paris July 2019	Paris, France	Jul 01, 2019 - Jul 06, 2019	Live Event
SANS Rocky Mountain 2019	Denver, CO	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Columbia 2019	Columbia, MD	Jul 15, 2019 - Jul 20, 2019	Live Event
SANS Boston Summer 2019	Boston, MA	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Chicago 2019	Chicago, IL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, Denmark	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Network Security 2019	Las Vegas, NV	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, Norway	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS London September 2019	London, United Kingdom	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Online	Anytime	Self Paced