GCIA Practical Assignment
Version 2.8

Prepared by Brian Credeur
Revised on May 26, 2001

Table of Contents

TABLE OF CONTENTS I

GIAC PRACTICAL ASSIGNMENT 1

ASSIGNMENT 1 – NETWORK DETECTS 1

DETECT 1 – INTERESTING PACKET 1
DETECT 2 – PORTMAPPER REVISIT 3
DETECT 3 – SMB PROBE 4
DETECT 4 – SYNSCAN 6
DETECT 5 – FTP PROBES, USING GUEST@HERE.COM 8

ASSIGNMENT 2 – DESCRIBE THE STATE OF INTRUSION DETECTION 11

ATTACK SYNOPSIS 11
ATTACK TECHNIQUE 11
TRACES OF THE ATTACK 12
PROTECTION AGAINST THIS ATTACK 13
CONCLUSION 13
REFERENCES 13

ASSIGNMENT 3 – "ANALYZE THIS" SCENARIO 13

EXECUTIVE SUMMARY 13
ANALYSIS OF ALERTS 14

GIAC Practical Assignment

Assignment 1 – Network Detects

Detect 1 – Interesting Packet

0. Trace

```
216.13.170.3 (*Trolling for DNS/TCP, interesting src port # and seq #)
*** localhost can't find 216.13.170.3: Non-existent host/domain
Server:  localhost
Address:  127.0.0.1

--------------------------------------------------
Feb 14 15:12:46 gateway kernel: Packet log: input DENY eth1 PROTO=6
216.13.170.3:33000 MY.NETWORK.0.1:53 L=40 S=0x10 I=14116 F=0x0000 T=236
```

1. Source of trace

Linux 2.2 firewall, running IPChains 1.3.

2. Detect was generated by

Linux IPChains packet log.

3. Probability the source address was spoofed

Very low. The string "PROTO=6" in the packet log identifies this packet as having and IP protocol number of 6, which is TCP. TCP scans need to receive a response from their stimulus to be of value to the attacker. The exception would be a decoy scan to mislead the intrusion analyst or overload them ("hide in the noise"). This is the only packet of its type received, so the decoy scenario is most likely not the case.

4. Description of attack

This attack is a reconnaissance effort, attempting to locate DNS servers listening on TCP port 53. Attacks on DNS servers are particularly popular at this time, due to recent publicity for another vulnerability in BIND.

Issued January 29, 2001, the CERT Advisory CA-2001-02: Multiple Vulnerabilities in BIND (http://www.cert.org/advisories/CA-2001-02.html) describes various vulnerabilities found in the widely used DNS server, ISC BIND. Most of the excitement was centered around the buffer overflow in the transaction signature (TSIG) handling code, as detailed in the CERT Vulnerability Note VU#196945 (http://www.kb.cert.org/vuls/id/196945). This vulnerability affected all versions of BIND 8 prior to 8.2.3. With a successful buffer overflow exploit, the attacker could potentially execute code on the DNS server with the privileges of the account under which the service is run—typically, root.

5. Attack mechanisms

The scanner is able to note the availability of a DNS server, listening on TCP port 53, based on the target's response. A TCP reset would be the normal response to such a packet if a service were actually running on that port, so the attacker could consider it a successful probe if they get such a response from this stimulus.

The packet is composed as though it is part of a connection already established with an internal host. This is a trick used to circumvent a firewall's rules. Some firewalls will only filter out packets sent to start a TCP connection (ones that have the SYN flag set), however, this packet has a value set for its sequence number. This makes it appear as though the packet was part of an already established connection and the firewall may let it through, unhindered.

Additionally, the source port of 33000 is interesting, because this is a high number for an ephemeral or client port. Unless a system is very busy or has been running for a very long period of time a port number this high is not a normal occurrence. Given the nice, rounded value of the number and its conjunction with a TCP connection to a DNS server, leads one to believe that this packet was part of a large scan and/or generated by a scanner tool. This information could be used as a signature to better identify and track this particular attack in the future.

6. Correlations

There have been various DNS exploits reported over the years to response centers. The attacker's IP address is within the block registered to MetroNet and a search on the GIAC site returned http://www.sans.org/y2k/021901-1400.htm which contains a report of another IP address in MetroNet's address space performing a slightly different DNS scan just two days earlier. This attack may not be related to the others, however, it could indicate a larger problem that company might need to address.

The CERT Advisory CA-2001-02: Multiple Vulnerabilities in BIND (http://www.cert.org/advisories/CA-2001-02.html) describes the "exploit of the day", the TSIG buffer overflow, and various other vulnerabilities found in the widely used DNS server, ISC BIND.

I was unable to find any reports of attacks on DNS services with a signature of a TCP source port of 33000.

7. Evidence of active targeting

It is unlikely that this attack is directed specifically at this host. This host is serving as a public DNS and is listed in WHOIS; however, the connection is most likely just part of a larger-range network scan and not a focused attack. A sweep would be easier to detect if there were data for other IP addresses in the same block.

8. Severity

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

Criticality	4	This is a DNS probe of a DNS server
Lethality	1	Packet was dropped and logged by packet filter
System	4	Server contains up-to-date kernel and system patches
Network	4	Firewall contains tight firewall rules with logging and up-to-date patches

9. Defensive recommendation

Given the timing between the issuance of the CERT Advisory and the particulars of the BIND vulnerability VU#196945 (http://www.kb.cert.org/vuls/id/196945) and this probe for DNS servers accepting TCP connections the protection afforded by the firewall is welcome.

The attack was unsuccessful, because the firewall stopped this connection. It is recommended that the firewall continue to disallow connections to TCP port 53, especially since we do not need it. We are not doing any zone transfers, do not have large entries, or any other operations that would warrant such connections from the Internet.

10. Multiple choice test question

What are some types of exploits that exist with respect to DNS over TCP?

A. DNS poisoning
B. Buffer overflow

C. Zone transfer
D. All of the above

Answer: D

Detect 2 – Portmapper Revisit

0. Trace

```
212.103.193.6 (*Trolling for portmapper/TCP, two times around)
*** localhost can't find 212.103.193.6: Non-existent host/domain
Server:  localhost
Address:  127.0.0.1

--------------------------------------------------
Feb 16 18:41:45 gateway kernel: Packet log: input DENY eth1 PROTO=6
212.103.193.6:1163 MY.NETWORK.0.1:111 L=60 S=0x00 I=28629 F=0x4000 T=42
Feb 17 15:52:35 gateway kernel: Packet log: input DENY eth1 PROTO=6
212.103.193.6:2308 MY.NETWORK.0.1:111 L=60 S=0x00 I=54852 F=0x4000 T=42
```

1. Source of trace

Linux 2.2 firewall, running IPChains 1.3.

2. Detect was generated by

Linux IPChains packet log.

3. Probability the source address was spoofed

Very low. The string “PROTO=6” in the packet log identifies this packet as having and IP protocol number of 6, which is TCP. TCP scans need to receive a response from their stimulus to be of value to the attacker.

4. Description of attack

The scanner is looking for accessible RPC portmap services, and interestingly enough has come back a second time.

5. Attack mechanisms

Typically, once a scanner has found a listener that it is looking for the attacker returns to attempt some type of exploit for that service. In this particular case; however, the “revisit” is actually just a second scan, identical to the first. The original packet was denied by the firewall (indicated by the “DENY” string in the packet log), so the scanner could not have concluded that the service it was looking for was available. Most likely, the scanner was restarted or is just being through by making a second pass approximately 21 hours after the first.

6. Correlations

There are a good number of IDS numbers listed for RPC attacks (RPC Info Query, IDS013 - RPC - portmap-request-mountd, IDS15 - RPC - portmap-request-status, …). The connection attempt was stopped, however, before any more packets were sent, so further details on the intent of the attack are unknown.

7. Evidence of active targeting

It is unlikely that this attack is directed specifically at this host. This host is serving as a public DNS and is listed in WHOIS; however, the connection is most likely just part of a larger-range network scan and not a focused attack. A sweep would be easier to detect if there were data for other IP addresses in the same block.

8. Severity

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

Criticality	3	This is a portmapper probe of a server that is running portmapper
Lethality	1	Packet was dropped and logged by packet filter
System	4	Server contains up-to-date kernel and system patches
Network	4	Firewall contains tight firewall rules with logging and up-to-date patches

9. Defensive recommendation

The attack was unsuccessful, because the firewall stopped this connection. It is recommended that the firewall continue to disallow connections to port 111, as we are not providing any services to the Internet that would warrant such connections.

10. Multiple choice test question

What is the scanner expecting to see in order to know a host has the TCP service it is looking for available?

A. Sending a SYN and receiving a SYN-ACK
B. Sending a SYN and receiving no response
C. Sending a SYN-ACK and receiving a SYN-ACK
D. Sending a SYN-ACK and receiving no response

Answer: A

Detect 3 – SMB Probe

0. Trace

```
208.206.75.2 (*Trolling for smb/UDP, interesting source port [670 is VACDSM-
SWS])
Server:  localhost
Address:  127.0.0.1

Name:    ben.bpai.com
Address:  208.206.75.2

--------------------------------------------------
Mar 27 20:21:50 gateway kernel: Packet log: input DENY eth1 PROTO=17
208.206.75.2:670 MY.NETWORK.0.1:137 L=78 S=0x00 I=18439 F=0x0000 T=112
Mar 27 20:21:52 gateway kernel: Packet log: input DENY eth1 PROTO=17
208.206.75.2:670 MY.NETWORK.0.1:137 L=78 S=0x00 I=1545 F=0x0000 T=111
Mar 27 20:21:53 gateway kernel: Packet log: input DENY eth1 PROTO=17
208.206.75.2:670 MY.NETWORK.0.1:137 L=78 S=0x00 I=17163 F=0x0000 T=111

--------------------------------------------------

03/27-20:21:50.584380 208.206.75.2:670 -> MY.NETWORK.0.1:137
UDP TTL:112 TOS:0x0 ID:18439 IpLen:20 DgmLen:78
Len: 58
83 80 00 00 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/27-20:21:52.072887 208.206.75.2:670 -> MY.NETWORK.0.1:137
UDP TTL:111 TOS:0x0 ID:1545 IpLen:20 DgmLen:78
Len: 58
85 E4 00 00 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/27-20:21:53.604257 208.206.75.2:670 -> MY.NETWORK.0.1:137
UDP TTL:111 TOS:0x0 ID:17163 IpLen:20 DgmLen:78
Len: 58
88 30 00 00 00 01 00 00 00 00 00 00 20 43 4B 41  .0.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1. Source of trace

Linux 2.2 firewall, running IPChains 1.3.

2. Detect was generated by

Linux IPChains packet log and Snort 1.7 packet decode of tcpdump data.

3. Probability the source address was spoofed

Very low. Since there has been no other activity with respect to this IP address, this is most likely a reconnaissance run, whereby the attacker would want to be able to get feedback from this stimulus. Though this packet is UDP and could be a one-shot exploit (meaning the attacker only needs to get the one packet through to the victim to accomplish their objective, a typical SMB probe is expecting to receive reconnaissance.

4. Description of attack

Looks like a probe for SMB shares (Microsoft Networking and Samba).

5. Attack mechanisms

The scanner is looking for responses from SMB servers to note their existence and to, hopefully (for the attacker), find out more information about the server, such as what it is sharing and what type of system it is.

The source port of 670 is odd, however, as most, if not all, implementations of SMB use a source port of 137 for connecting to a destination port of 137. The service registered by IANA for port 670 is VACDSM-SWS, which seems to be unrelated to these SMB services. The fact that this is a privileged port (less than 1024) indicates that the attacker has root/administrator privileges on their system.

6. Correlations

The packet log from the firewall and the Snort packet capture provide two views of the same packets. This reconnaissance technique is known as "SMB Name Wildcard," however, and it is documented at the SANS site at http://www.sans.org/newlook/resources/IDFAQ/port_137.htm.

I was unable to find any reports of attacks on SMB services with a signature of a TCP source port of 670.

7. Evidence of active targeting

It is unlikely that this attack is directed specifically at this host. This host is serving as a public DNS and is listed in WHOIS; however, the connection is most likely just part of a larger-range network scan and not a focused attack. A sweep would be easier to detect if there were data for other IP addresses in the same block.

8. Severity

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

Criticality	3	This is a SMB probe of a server that is running Samba
Lethality	1	Packet was dropped and logged by packet filter
System	4	Server contains up-to-date kernel and system patches, and the SMB service is not listening on the outside interface
Network	4	Firewall contains tight firewall rules with logging and up-to-date patches

9. Defensive recommendation

The attack was unsuccessful, because the firewall stopped this connection. It is recommended that the firewall continue to disallow outside connections to TCP port 137, as we are not providing any services to the Internet that would warrant such connections. (Actually TCP and UDP ports 135-139 are dropped by the firewall, because they are all part of the same protocol suite.)

10. Multiple choice test question

Which OS's are known a default initial TTL of 128?

A. Linux
B. Windows 98
C. Both A & B
D. None of the above

Answer: D
(There is an exception: Windows 98 will use a TTL of 128 when communicating to localhost addresses.)

Detect 4 – SynScan

0. Trace

```
03/10-14:15:35.607505 200.188.64.82:53 -> MY.NETWORK.0.1:53
TCP TTL:30 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x4BD6D358  Ack: 0x17459F12  Win: 0x404  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

---------------------------------------------------------------------------
------------- SynScan PortScan Alert on Packet from 200.188.64.82 -------------
---------------------------------------------------------------------------


Snort Alerts: eth1-20010310_1350.log from gateway
-----------------------------------------------
```

```
[**] IDS441 - SCAN - Synscan Portscan [**]
03/10-14:15:35.607505 200.188.64.82:53 -> MY.NETWORK.0.1:53
TCP TTL:30 TOS:0x0 ID:39426 IpLen:20 DgmLen:40
******SF Seq: 0x4BD6D358  Ack: 0x17459F12  Win: 0x404  TcpLen: 20
------------------------------------------------------------------------------

/var/log/kernlog on gateway
---------------------------

Mar 10 14:15:35 gateway kernel: Packet log: input DENY eth1 PROTO=6
200.188.64.82:53 MY.NETWORK.0.1:53 L=40 S=0x00 I=39426 F=0x0000 T=30
------------------------------------------------------------------------------
```

1. Source of trace

Linux 2.2 firewall, running IPChains 1.3 and Snort 1.7.

2. Detect was generated by

Linux IPChains packet log and Snort 1.7 alert and packet decode from tcpdump data.

3. Probability the source address was spoofed

Very Low. This scan is most likely an initial pass at mapping DNS servers, so the attacker would want to get feedback from this stimulus.

4. Description of attack

Port 53 is the well-known port for DNS, therefore, this appears to be a reconnaissance run, mapping DNS servers.

5. Attack mechanisms

Connection attempt to a DNS server, using a packet with the SYN and FIN flags set. Some firewalls have been known to allow such packets to pass through their packet-filtering rules unhindered. Packets of this type should not be seen under normal circumstances, therefore, they are indicative of hacker scanning.

According to Paul W. DePriest's article, "The Importance of the Ramen Worm" (http://www.sans.org/infosecFAQ/threats/ramen_worm.htm), the existence of the Ramen Worm was first reported by GIAC on January 18, 2001. When activated, this worm makes a number of modifications to files on the local system, including the defacement of web documents. The worm also performs a synscan of a randomly selected class B network, records potentially exploitable hosts that it finds, and attempts to propagate itself by replicating and executing itself on vulnerable hosts. Paul cited a statistic from a ZDNet News story stating that the "Ramen worm scanned two B-class networks (about 131000 IP addresses) in less than 15 minutes." Based upon this fact, the modified synscan program incorporated by the Ramen Worm appears to be quite fast. The Ramen Worm has a small number of services that it scans for, specifically wu-ftp and rcp.statd vulnerabilities for Red Hat Linux 6.2 and lprng for Red Hat Linux 7.0.

The synscan detected in this trace is probing for TCP port 53, the well-known port for DNS. This is not one of the services that are part of the Ramen Worm signature. However, it could be indicative of a variant of the Ramen Worm, looking for another "popular" exploit with which to propagate itself—the TSIG buffer overflow for ISC BIND version 8. Vulnerable versions of BIND were shipped with both Red Hat Linux 6.2 and 7.0, as well as other Linux distributions and other operating systems (see the CERT Vulnerability Note VU#196945 at http://www.kb.cert.org/vuls/id/196945 for more details on vulnerable systems).

Regardless of whether this synscan is the result of an attacker directly looking for vulnerable DNS servers or if it is a more autonomous attack, such as a network worm, administrators should take note of this activity. A scan of a particular well-known port should prompt administrators to evaluate the security of the systems and any of the corresponding services that they may have available to the outside world.

6. Correlations

Synscans are quite common, and there is a rule readily available for Snort to detect these types of packets. Snort reported the following with its alert message:

```
    [**] IDS441 - SCAN - Synscan Portscan [**]
```

A search of the SANS site for the remote IP address, turned up the following page, indicating that others have also detected suspect activity from this host:
http://www.sans.org/y2k/031201-1100.htm

This alert was triggered because the packet had both the SYN and FIN flags set. Since this is not a normally occurring packet, such a packet is either corrupt or crafted for the purpose of penetrating a firewall.

7. Evidence of active targeting

It is unlikely that this attack is directed specifically at this host. This host is serving as a public DNS and is listed in WHOIS; however, the connection is most likely just part of a larger-range network scan and not a focused attack. A sweep would be easier to detect if there were data for other IP addresses in the same block.

8. Severity

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

Criticality	4	This is a “stealth scan” probing for DNS services on our DNS server
Lethality	1	Packet was dropped and logged by packet filter
System	4	Server contains up-to-date kernel and system patches
Network	4	Firewall contains tight firewall rules with logging and up-to-date patches

9. Defensive recommendation

The attack was unsuccessful, because the firewall stopped this connection. It is recommended that the firewall continue to disallow connections to TCP port 53, especially since we do not need it. We are not doing any zone transfers, do not have large entries, or any other operations that would warrant such connections from the Internet.

10. Multiple choice test question

What type of response is the SYN-FIN scanner hoping to get?

A. ICMP network unreachable
B. TCP reset
C. UDP port unreachable
D. TCP port unreachable

Answer: B

Detect 5 – FTP Probes, Using guest@here.com

0. Trace

Seven incidents were recorded over a period of approximately 2 months. Other FTP connections were attempted, however, the ones addressed here were all attempted using the same anonymous FTP password username ‘guest@here.com’:

```
[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
03/17-01:45:55.441618 MY.NETWORK.0.1:21 -> 64.229.241.208:1731
```

```
TCP TTL:64 TOS:0x0 ID:49173 IpLen:20 DgmLen:107 DF
***AP*** Seq: 0x42F67605  Ack: 0x2E4ED49  Win: 0x7F0A  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
03/17-01:45:55.791571 MY.NETWORK.0.1:21 -> 64.229.241.208:1731
TCP TTL:64 TOS:0x0 ID:49176 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x42F6766E  Ack: 0x2E4ED6E  Win: 0x7F0A  TcpLen: 20


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
03/20-09:08:31.682492 MY.NETWORK.0.1:21 -> 213.56.32.4:2164
TCP TTL:64 TOS:0x0 ID:25573 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x82C74202  Ack: 0x185580D  Win: 0x7D78  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
03/20-09:08:32.125451 MY.NETWORK.0.1:21 -> 213.56.32.4:2164
TCP TTL:64 TOS:0x0 ID:25576 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x82C7424C  Ack: 0x1855832  Win: 0x7D78  TcpLen: 20


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
04/04-05:03:36.172022 MY.NETWORK.0.1:21 -> 193.253.204.190:4335
TCP TTL:64 TOS:0x0 ID:53271 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0xA1F16BE3  Ack: 0xCA15C417  Win: 0x7F80  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
04/04-05:03:36.613533 MY.NETWORK.0.1:21 -> 193.253.204.190:4335
TCP TTL:64 TOS:0x0 ID:53274 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0xA1F16C2D  Ack: 0xCA15C43C  Win: 0x7F80  TcpLen: 20


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
05/02-06:40:28.526073 MY.NETWORK.0.1:21 -> 193.253.196.253:3533
TCP TTL:64 TOS:0x0 ID:11137 IpLen:20 DgmLen:88 DF
***AP*** Seq: 0xD452F004  Ack: 0x98524F6F  Win: 0x7F80  TcpLen: 32
TCP Options (3) => NOP NOP TS: 45675149 332945

[**] IDS364 - FTP - Bad Login [**]
05/02-06:40:29.407846 MY.NETWORK.0.1:21 -> 193.253.196.253:3533
TCP TTL:64 TOS:0x0 ID:11140 IpLen:20 DgmLen:74 DF
***AP*** Seq: 0xD452F04E  Ack: 0x98524F94  Win: 0x7F80  TcpLen: 32
TCP Options (3) => NOP NOP TS: 45675237 332966


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
05/11-14:10:13.160261 MY.NETWORK.0.1:21 -> 24.200.66.123:4215
TCP TTL:64 TOS:0x0 ID:31317 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0xA3EC7EB8  Ack: 0xC38CD37D  Win: 0x7D78  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
05/11-14:10:13.676082 MY.NETWORK.0.1:21 -> 24.200.66.123:4215
TCP TTL:64 TOS:0x0 ID:31321 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0xA3EC7F02  Ack: 0xC38CD3A2  Win: 0x7D78  TcpLen: 20


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
05/15-04:41:37.664055 MY.NETWORK.0.1:21 -> 24.200.66.123:1203
TCP TTL:64 TOS:0x0 ID:18394 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x37ABB52F  Ack: 0x9D17ABD7  Win: 0x7D78  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
05/15-04:41:38.625968 MY.NETWORK.0.1:21 -> 24.200.66.123:1203
TCP TTL:64 TOS:0x0 ID:18397 IpLen:20 DgmLen:62 DF
```

```
***AP*** Seq: 0x37ABB579  Ack: 0x9D17ABFC  Win: 0x7D78  TcpLen: 20


[**] BUGTRAQ ID 1471 - FTP - Exploitable proftpd 1.2 server running [**]
05/18-03:01:06.489804 MY.NETWORK.0.1:21 -> 202.109.129.45:2388
TCP TTL:64 TOS:0x0 ID:52209 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x7612FF23  Ack: 0xB501ACF4  Win: 0x7D78  TcpLen: 20

[**] IDS364 - FTP - Bad Login [**]
05/18-03:01:06.928397 MY.NETWORK.0.1:21 -> 202.109.129.45:2388
TCP TTL:64 TOS:0x0 ID:52212 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x7612FF6D  Ack: 0xB501AD19  Win: 0x7D78  TcpLen: 20
```

1. Source of trace

Linux 2.2 firewall, running IPChains 1.3 and Snort 1.7.

2. Detect was generated by

Snort 1.7 alert and packet decode and session tracking from tcpdump data.

3. Probability the source address was spoofed

Very Low. This appears to be a scan of FTP servers, specifically those that allow anonymous users. The attackers would want to be able to receive the victim's response from their stimuli so that they could keep interesting victims on a list and/or immediately attempt to exploit the FTP server.

4. Description of attack

Port 21 is the well-known port for FTP, therefore, this attack, as observed by this system, appears to be a reconnaissance run, mapping FTP servers. The presentation of the username 'guest@here.com' indicates the attacker is looking, specifically for an FTP server that allows anonymous users.

5. Attack mechanisms

FTP servers may allow logins for anonymous users so files may be uploaded and/or downloaded by anyone. This is a common practice, and also common is the practice of making the FTP server's content accessible by a web server to simplify the downloading process for users.

Since this FTP server does not allow anonymous users, no further data was directly available on the attacker's intention. Other detects (such as those reported by Esteban Gutierrez at http://www.sans.org/y2k/030901.htm and Mike Black at http://www.sans.org/y2k/101900.htm) indicate that the attacker seeks to run arbitrary web-server-executable code. The attacker uploads a file to the FTP site and then causes the web server to run that code by accessing an URL, correlating to the location of the uploaded file.

6. Correlations

Correlation from Esteban Gutierrez, found at http://www.sans.org/y2k/030901.htm indicates that the attackers are not just looking for anonymous FTP servers. His traces show the attackers uploading a .asp file (a file extension commonly associated with Active Server Pages) and attempting to access that file from a web browser. If the web server on that system had be able to access that uploaded file and execute it, then the attacker would have been able to execute that and future ASP code on the victim's web server.

Correlation from Mike Black, found at http://www.sans.org/y2k/101900.htm shows the attackers looking for various directories in which they can create their own "dot" directory (a directory with a preceeding '.' in its name). Depending on the operating system, the "dot" directory may be interpreted as a hidden or system directory. The ultimate goal for the attacker appears to be the creation a directory that may not be readily noticed by the system administrator or other users.

7. Evidence of active targeting

It is unlikely that this attack is directed specifically at this host. This host is serving as a public DNS and is listed in WHOIS; however, the connection is most likely just part of a larger-range network scan and not a focused attack. A sweep would be easier to detect if there were data for other IP addresses in the same block.

8. Severity

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

Criticality	4	This is an FTP probe sent to an FTP server
Lethality	1	The anonymous login was correctly denied by the FTP server
System	4	Server contains up-to-date kernel and system patches
Network	4	Firewall contains tight firewall rules with logging and up-to-date patches

9. Defensive recommendation

The attack was unsuccessful, because the FTP server was configured to not accept anonymous users. It is recommended that the FTP server continue to disallow anonymous users, especially since we do not need it. Also, as one correlation indicates, the attacker is looking to upload files and execute them via a web server that supports Active Server Pages. It has been verified that the web server on this machine does not support ASP.

10. Multiple choice test question

If you want to run an anonymous FTP server and also support downloads of the same content with a web server, which of the following would be a good idea to avoid the problems associated with this type of exploit?

A. Disallow anonymous users
B. Restrict FTP uploads from anonymous users to a directory or directories where the web server will not execute content
C. Set a rule on the firewall to prevent all ICMP packets from reaching the server
D. Set a rule on the firewall to prevent all TCP packets from reaching the server

Answer: B

Assignment 2 – Describe the State of Intrusion Detection

Attack Synopsis

The famous Ping of Death attack was able to get a lot of exposure with the IT industry, due to its combination of simplicity and effectiveness. By creating a situation that the TCP/IP stack was not able to properly handle, this malicious code was able to halt Windows computers. In time, Microsoft was able to provide a system patch that prevented this attack from occurring, however, other attacks shortly came out to provide the same combination of simplicity and lethality. One such attack method was dubbed the Kiss of Death.

Attack Technique

IGMP (Internet Group Management Protocol) is detailed in RFC 2263[1]. This protocol is used by hosts in the negotiation of IP Multicast sessions. The Kiss of Death exploits a weakness in the way the IP stack on Microsoft Windows handles fragmented IGMP packets. Windows 95, 98, 98SE, and NT are vulnerable, though security updates to have been made to address the problem. Further details on the issues and resolutions may be found on Security Bulleting MS99-034[2] at the Microsoft Tech Net site.

There are a number of tools (kod, pimp, kox, and igmpofdeath) developed to exploit this weakness. The exact nature of the payload differs a bit from one tool to the next, and some offer extra features, however, the end results are the same. One such extra feature is source IP address spoofing. This effectively enables an attacker to adversely affect the victim computer anonymously, because the attack will disrupt the victim computer without any handshaking or interaction.

Traces of the Attack

On a successful Kiss of Death attack, one of several things may occur on the victim host. The host may instantly reboot, it may hang and cease to respond to all input, or it might display a blue screen with a message similar to the following:

```
    windows core dump output
    An exception 0E has occurred at 0028:C14C9212 in VxD VIP (01) + 00006C72.
    This was called from 0028:C183FF54 in VcD PPPMAC(04) + 000079BR.
    It may be possible to continue normally.
```

In the latter case, the user may be able to press the space bar and continue using the system, locally, however, the TCP/IP stack will no longer function. When the user shuts down or reboots the system it will hang and not complete its shutdown, requiring a system reset or power off.

The underlying technique to the Kiss of Death is the fragmentation of IGMP (IP protocol 2) packets. Un-patched Windows TCP/IP stacks will not reassemble the packet fragments properly and will become corrupt. The following trace illustrates the packets sent by the tool, kod:

```
    04/04-23:49:48.655017 A.SPOOFED.IP.101 -> MY.NET.WORK.1
    IGMP TTL:64 TOS:0x0 ID:48648 IpLen:20 DgmLen:220
    Frag Offset: 0x73A   Frag Size: 0xC8
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    ------------------ 10 more lines of the same. -------------------
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    00 00 00 00 00 00 00 00                          ........

    =+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

    04/04-23:49:48.655418 A.SPOOFED.IP.101 -> MY.NET.WORK.1
    IGMP TTL:64 TOS:0x0 ID:48648 IpLen:20 DgmLen:1500 MF
    Frag Offset: 0x681   Frag Size: 0x5BA
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    ------------------ 39 more lines of the same. -------------------
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
    00 00 00 00 00 00 00 00 00 00                    ..........

    22 packets were sent in all, with the last 20 being identical to the 2nd.
```

Another Kiss of Death tool, kox, operates under the same premise as kod, with a couple of exceptions. The kox tool will start sending 1500-byte fragments from the beginning. It will also fill in “random” data, so that the fragment payloads will not be all 0x00 values. Unfortunately, for the attacker, the so-called random data on my traces happened to include useful information such as what would be found by running the Unix ‘uname’ command.

It is also worth noting that though a directed attack can cause a victim host to crash, completely legitimate IGMP packets that happen to be fragmented will cause the same problem. Microsoft had published a frequently asked question page[3] to address this particular bug in the TCP/IP stack. Microsoft is careful to mention that IGMP has no inherent security risks, and that the vulnerability lies within the way TCP/IP has been implemented on the affected operating systems.

Protection Against this Attack

First and foremost in the process of protecting vulnerable Windows computers would be to download and apply the most recent security patches for the affected versions of Windows. After applying the patches (available from Microsoft via the Security Bulleting MS99-034[2]), Windows should not only be protected against this attack, but the patches should address other known exploit or bug issues.

Perimeter firewall rules can also protect internal network hosts from being attacked by outside hosts. Disallowing all IGMP (IP protocol 2) traffic to the internal network, or at least restricting access to only those hosts that need to have such communications, will prevent this attack from ever reaching vulnerable hosts.

Additionally, an intrusion detection system could be able to send alerts on this attack's signature. An IDS rule, for example could trigger an alert on all IGMP (IP protocol 2) traffic from the outside. A more refined rule would be to alert on any fragmented IGMP packets, or any extremely large IGMP packets.

Conclusion

As vulnerabilities in a system are discovered and exploits are made and used against those vulnerabilities, the product vendors and security administrators need to react. A secure network does not begin and end with a strong firewall, nor does the newest system patch grant a system complete invulnerability to all attacks. The combination of maintaining systems at current patch levels and strong firewalls and firewall rules helps to prevent known attacks and attack types from creating problems. Furthermore, by adding the techniques of traffic capture and analysis, information technologists are able to better understand new attacks and attack types, as well as develop methods to protect against them.

References

1. RFC 2263, Internet Group Management Protocol, Version 2. Internet Engineering Task Force (IETF). http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2236.html.
2. Microsoft Security Program: Microsoft Security Bulletin (MS99-034). Microsoft Tech Net. http://www.microsoft.com/technet/security/bulletin/MS99-034.asp.
3. Microsoft Security Program: Frequently Asked Questions: Microsoft Security Bulletin (MS99-034). Microsoft Tech Net. http://www.microsoft.com/technet/security/bulletin/fq99-034.asp.

Assignment 3 – "Analyze This" Scenario

Executive Summary

Overview

The administrators of MY.NET were able to collect a good amount of IDS (Intrusion Detection System) data of their site for the two-week period, from January 30 through February 12. Most of the activity flagged by these IDS alerts is probe scans by remote hosts trying to learn more about the topology of and services running on hosts within the network. In addition to reconnaissance scans, there was evidence of internal systems running services that may be of questionable value to the productivity and security of the overall site.

Scans

Typically, a scan of one's network by remote systems is not an immediate threat to network security, however, it could provide those remote scanners sufficient information about the internal site so that they could attempt to exploit any weaknesses they find. (It is worth noting that, in sufficient volume, scans could result in a denial of service to the network or specific hosts, or could overload the IDS's making them less effective.) Though scans are not usually damaging they can serve as a good early-warning mechanism, indicating such things as the source(s) an attack might come from, the type of attack that might come, and the systems that might come under attack. These pieces of information could greatly assist administrators in determining what steps to take in order to protect against these potential threats.

Among other, small-scale scans, MY.NET experienced a relatively large number of SYN-FIN Scans (the name given to packets that are sent with both the SYN and FIN flags turned on to avoid detection by firewalls) alerts. Over 98% of the SYN-FIN detects were from the activity of one IP source address, 211.248.112.67, which is registered to APNIC (Asia Pacific Network Information Center). Refer to the "SYN-FIN Scan!" section, below, for more details.

Potential Exploits

The four connections to Sun RPC services from outside addresses are of interest. An attacker may or may not have been able to exploit these systems, but the fact that those services were globally available should be evaluated. Refer to the "SUNRPC highport access" section, below, for more details.

Questionable Services

Evidence of Gnutella and Napster activity has been found on several hosts within MY.NET. The use of network resources for the sharing of music and other files (typically multimedia), should be checked with the network use policy for MY.NET. Refer to the following online document for more information on how these peer-to-peer services can affect network performance and security, http://www.sans.org/infosecFAQ/threats/napster.htm.

Conclusions

Given the volume of detected scan packets originating from one IP address within APNIC, it is strongly recommended that a report of the scanning activity from this address should be sent to them. Additionally, it is recommended that Sun RPC services not be available to external hosts at all, therefore, the perimeter firewall should prevent those connection from coming into MY.NET.

Analysis of Alerts

The data provided contains a log of 205,319 unique alerts from data captured on MY.NET between January 30 and February 12. The alerts were separated into three categories for easier analysis. The analysis details are provided in the Analysis of Alerts section, below. The unique alerts, listed by category, are as follows:

• Multicast Traffic	144,609
• Traffic Outside of MY.NET	3,716
• Remaining Traffic	56,994

There were a good number of duplicate alerts, due to overlapping data in the alert files provided. The 40,487 duplicate alerts were discarded from the detailed analysis, to avoid the skewing of the results.

Multicast Traffic

Alert Summary

Alerts generated by traffic to/from mulitcast addresses (224.0.0.0 – 239.255.255.255) was distributed, by protocol, as follows:

• ICMP:	5
• UDP	144,604

Alert Analysis

```
-------------------------
Distribution of ICMP destinations:
     224.2.127.254:             5
-------------------------


-------------------------
```

```
Distribution of UDP destinations:
     224.0.1.1:123:               201         Network Time Protocol
     224.0.1.41:1718:             1133        gatekeeper
     224.2.127.254:9875:          139195      SAPv1 Announcements
     224.2.127.254:9880:          4075        SAPv1 Announcements
-------------------------
```

Though there are a large number of alerts generated by these multicast packets, most, if not all, of them can be regarded as false positives. All of the addresses fit into defined assignments by IANA and most originate from educational networks (where MBONE use is more common).

Traffic Outside of MY.NET

Alert Summary

Alerts generated by traffic with both source and destination addresses outside of MY.NET were distributed, by protocol, as follows:

• ICMP:	14
• TCP:	60
• UDP:	3,642

Alert Analysis

In general, the IDS's in MY.NET shouldn't be seeing any of this traffic. It is possible that some ISP and/or extranet network equipment is sharing our network segment with others. For the most part, this poses no threat, however, it might not be a bad idea to investigate the problem further to cut-down on false positives and clean-up the network perimeter for MY.NET.

Remaining Traffic

Alert Summary

The remaining alerts generated we distributed, by alert type, as follows:

• Attempted Sun RPC high port access:	507
• NMAP TCP ping!:	12
• Null scan!:	72
• Possible RAMEN server activity:	3,779
• Queso fingerprint:	210
• Russia Dynamo - SANS Flash 28-jul-00:	1
• SNMP public access:	5
• SUNRPC highport access:	4
• SYN-FIN scan!:	1,112
• TCP SMTP Source Port traffic:	4
• Tiny Fragments - Possible Hostile Activity:	111
• Watchlist IDs:	9,090
• WinGate 1080 Attempt:	191
• connect to 515 from inside:	590
• spp_portscan: Alerts:	41,306

Alert Analysis

Attempted Sun RPC high port access

```
-------------------------
Distribution of 'Attempted Sun RPC high port access' sources:
     205.188.153.107:4000:         5
     205.188.153.108:4000:         6
     205.188.153.97:4000:          134
     64.244.10.40:7777:            362
-------------------------
```

```
-------------------------
Distribution of 'Attempted Sun RPC high port access' destinations:
     MY.NET.105.115:32771:        6
     MY.NET.221.246:32771:        134
     MY.NET.223.254:32771:        362
     MY.NET.97.217:32771:         5
-------------------------
```

The 205.188.153.x addresses resolve to ICQ servers in AOL's domain. Most likely these alerts represent legitimate ICQ traffic and are, therefore, false positives.

The 64.224.10.40 address, however, seems to be a little more interesting. The address resolves to 'y0u.g0t.sh0t.sh00ting.0n.d0t.net' and is a whois at ARIN shows the address to be registered to Interland. Interland (http://www.interland.net/) provides web and application hosting services. Most of the alerts were triggered by traffic between this address and MY.NET.223.25, so it 1might be worth investigating further. Though 7777 is not an IANA assigned port, Napster is known to use ports 4444, 5555, 6666, 7777, 8888, and 8875, as well as some Internet games, such as Unreal.

NMAP TCP ping!

```
-------------------------
Distribution of 'NMAP TCP ping' sources:
     12.40.36.194:80:              1
     192.102.197.234:53:           1
     192.102.197.234:80:           3
     194.133.58.129:80:            1
     2.2.2.2:80:                   1
     208.5.219.131:53:             1
     63.119.91.2:80:               4
-------------------------
```

```
-------------------------
Distribution of 'NMAP TCP ping' destinations:
     MY.NET.1.3:53:               3
     MY.NET.1.5:53:               3
     MY.NET.1.8:53:               5
     MY.NET.110.39:25:            1
-------------------------
```

NMAP uses a "TCP ping" to probe for select services. The "TCP ping" is actually a TCP packet with the ACK bit set. The packet is intended to penetrate a firewall by emulating a step of the three-way handshake. If the firewall lets the packet go through then the destination host may send a TCP reset if the host is listening on that port. The reset packet then tips off the attacker that the destination is listening on that port.

These probes appear to be looking for typical DNS and SMTP servers. Further investigation of traffic by these outside IP addresses is warranted, as it could indicate if they attempted or, even worse, if there were successful at exploiting the services they were probing for. These addresses should be added to the list of IP addresses to watch in the future.

Null scan!

```
-------------------------
Distribution of 'Null scan' sources:
     128.40.224.18:4141:           2
     128.61.39.84:6699:            1
     129.98.118.190:3342:          1
     130.111.152.76:6699:          1
     130.83.217.180:4051:          1
     131.155.227.132:3054:         1
     131.155.227.236:4783:         1
     195.242.112.99:12288:         1
     195.38.204.151:6700:          1
     195.77.212.71:3592:           1
     202.92.71.227:1500:           1
     203.106.87.77:18245:          1
     209.156.50.124:0:             1
     209.156.50.57:65531:          1
     209.156.50.86:0:              1
     209.252.95.40:0:              1
     209.254.238.109:0:            1
     209.255.160.185:0:            1
     209.255.181.63:0:             1
     209.255.181.76:0:             1
     209.255.213.217:12288:        1
     210.50.36.147:18245:          1
     212.139.34.136:18245:         1
     212.232.32.94:0:              1
     212.47.211.11:13430:          1
     213.204.138.158:12288:        1
     213.47.184.236:1083:          1
     213.64.56.185:2619:           1
     216.50.249.154:1024:          1
     216.51.105.10:12288:          1
     217.80.83.127:1025:           1
     24.10.1.67:1184:              1
     24.141.128.226:411:           1
     24.167.72.249:2766:           1
     24.17.73.154:1592:            2
     24.180.66.185:1119:           1
     24.180.66.185:1121:           1
     24.185.223.19:3912:           1
     24.201.127.80:1135:           1
     24.21.31.206:1561:            1
     24.23.120.18:4021:            1
     24.67.220.137:1772:           1
     24.9.203.188:63602:           2
     62.180.210.55:0:              1
     62.29.70.109:12849:           1
     62.59.138.146:18245:          1
     63.252.119.17:65531:          1
     63.252.93.183:65532:          1
     63.252.93.186:65533:          1
     63.252.95.34:65531:           1
     63.253.104.172:0:             1
     63.253.105.248:65531:         1
     63.253.106.27:0:              1
     63.253.106.51:0:              1
     63.253.106.8:0:               1
     63.253.136.41:65532:          1
     63.253.226.133:12288:         1
     63.255.0.30:18245:            1
     63.91.222.118:0:              1
     63.91.234.62:0:               1
     63.91.237.227:21843:          1
     63.91.244.71:21843:           1
     64.48.221.224:0:              1
     64.48.239.17:12544:           1
     64.48.75.1:17217:             1
     64.48.75.35:17217:            1
     65.0.74.188:4161:             1
     65.2.140.248:1450:            1
     66.27.9.70:3216:              1
-------------------------


-------------------------
Distribution of 'Null scan' destinations:
     MY.NET.165.129:427:          2
     MY.NET.178.42:17746:         1
     MY.NET.179.50:0:             1
     MY.NET.182.40:1527:          1
     MY.NET.201.234:0:            1
     MY.NET.201.234:900:          2
     MY.NET.201.242:76:           1
     MY.NET.201.254:6688:         1
     MY.NET.201.70:0:             1
     MY.NET.202.14:6699:          1
     MY.NET.202.94:6699:          1
     MY.NET.203.170:4924:         1
     MY.NET.203.6:0:              1
     MY.NET.204.102:6688:         1
     MY.NET.205.214:6688:         1
     MY.NET.206.54:4374:          1
     MY.NET.207.42:21504:         1
     MY.NET.208.218:1083:         1
     MY.NET.209.138:2340:         1
     MY.NET.209.210:21504:        1
     MY.NET.210.118:0:            1
     MY.NET.210.178:21504:        1
     MY.NET.210.66:0:             1
     MY.NET.211.122:0:            1
     MY.NET.211.74:6346:          9
     MY.NET.212.42:1794:          1
     MY.NET.214.22:21504:         1
     MY.NET.218.190:21504:        1
     MY.NET.219.238:6688:         1
     MY.NET.219.250:0:            1
     MY.NET.219.62:0:             1
     MY.NET.220.14:2514:          1
     MY.NET.220.14:4999:          1
     MY.NET.221.50:13105:         1
     MY.NET.221.70:0:             1
     MY.NET.221.82:0:             1
     MY.NET.222.86:0:             1
     MY.NET.223.14:6688:          1
     MY.NET.223.210:17746:        1
     MY.NET.224.102:6346:         3
     MY.NET.225.150:0:            1
     MY.NET.5.29:0:               3
     MY.NET.6.39:20545:           1
     MY.NET.6.44:20545:           1
     MY.NET.60.11:0:              2
     MY.NET.60.11:6144:           1
     MY.NET.60.11:8960:           1
     MY.NET.60.38:0:              1
     MY.NET.60.38:256:            1
     MY.NET.60.38:8960:          1
     MY.NET.60.8:0:              2
     MY.NET.60.8:6144:           3
     MY.NET.98.109:0:            1
     MY.NET.98.114:0:            1
-------------------------
```

A "Null scan" packet has none of the TCP flag bits set. As with TCP pings in NMAP, these packet are intended to penetrate a firewall. If the firewall lets the packet go through then the destination host may send a TCP reset if the host is listening on that port. The reset packet then tips off the attacker that the destination is listening on that port.

These probes appear to be looking for a good variety of servers. Destination ports of most interest are 0, 427, and 1527 (reserved, Server Location, and Oracle listener, respectively). Also, the repetition of destination ports 21504 and 20545 across multiple hosts is interesting – perhaps the attacker is trolling for trojans. Additionally, the destination ports 6699 and 6688 are also known for use by Napster services.

Further investigation of traffic by these outside IP addresses is warranted, as it could indicate if they attempted or, even worse, if there were successful at exploiting the services they were probing for. These addresses should be added to the list of IP addresses to watch in the future. Due to the larger volume of IP addresses originating these probes than in the NMAP scans, priority should be given to those more interesting alerts mentioned, above.

Queso fingerprint

```
-------------------------
Distribution of 'Queso fingerprint' sources:
     134.109.185.77:1214:         1
     134.109.185.77:2109:         1
     134.109.185.77:2138:         1
     134.109.185.77:2823:         1
     134.109.185.77:3089:         1
     134.109.185.77:3662:         1
     134.109.185.77:4718:         1
     141.100.77.52:2292:          1
     141.30.228.115:1323:         1
     141.30.228.115:1865:         1
     141.30.228.115:2314:         1
     141.30.228.115:2673:         1
     141.30.228.115:2857:         1
     141.30.228.115:3254:         1
     141.30.228.115:4145:         1
     141.30.228.115:4536:         1
     141.30.228.120:1030:         1
     141.30.228.122:1039:         1
     141.30.228.122:1530:         1
     141.30.228.122:1558:         1
     141.30.228.122:1984:         1
     141.30.228.122:2122:         1
     141.30.228.122:2210:         1
     141.30.228.122:2239:         1
     141.30.228.122:2709:         1
     141.30.228.122:3031:         1
     141.30.228.122:3099:         1
     141.30.228.122:3559:         1
     141.30.228.122:3638:         1
     141.30.228.122:4037:         1
     141.30.228.122:4200:         1
     141.30.228.122:4452:         1
     141.30.228.122:4720:         2
```

```
141.30.228.122:4732:         1
141.30.228.122:4763:         1
141.30.228.134:1065:         1
141.30.228.134:1154:         1
141.30.228.134:1265:         1
141.30.228.134:1792:         1
141.30.228.134:1808:         1
141.30.228.134:1868:         1
141.30.228.134:2150:         1
141.30.228.134:2287:         1
141.30.228.134:2409:         1
141.30.228.134:2436:         1
141.30.228.134:2616:         1
141.30.228.134:2759:         1
141.30.228.134:2800:         1
141.30.228.134:2826:         1
141.30.228.134:2933:         1
141.30.228.134:3062:         1
141.30.228.134:3106:         1
141.30.228.134:3364:         1
141.30.228.134:3489:         1
141.30.228.134:3519:         1
141.30.228.134:3554:         1
141.30.228.134:3625:         1
141.30.228.134:3840:         1
141.30.228.134:4143:         1
141.30.228.134:4198:         1
141.30.228.134:4374:         1
141.30.228.134:4437:         1
141.30.228.134:4576:         1
141.30.228.134:4628:         1
141.30.228.155:2998:         1
141.30.228.161:1030:         1
141.30.228.161:1445:         1
141.30.228.161:1974:         1
141.30.228.161:2362:         1
141.30.228.161:2426:         1
141.30.228.161:2571:         1
141.30.228.161:3366:         1
141.30.228.161:3528:         1
141.30.228.161:3559:         1
141.30.228.161:3594:         1
141.30.228.161:4273:         1
141.30.228.161:4508:         1
141.30.228.161:4681:         1
141.30.228.161:4717:         1
141.30.228.161:4940:         1
141.30.228.165:1032:         1
141.30.228.165:2730:         1
141.30.228.165:2812:         1
141.30.228.165:2814:         1
141.30.228.165:3207:         1
141.30.228.165:3256:         1
141.30.228.175:3442:         1
141.30.228.178:1507:         1
141.30.228.178:4781:         1
141.30.228.182:1376:         1
141.30.228.182:1678:         1
141.30.228.182:1725:         1
141.30.228.182:1869:         1
141.30.228.182:2787:         1
141.30.228.182:3254:         1
141.30.228.182:3403:         1
```

```
141.30.228.182:3652:        1
141.30.228.182:3830:        1
141.30.228.182:4715:        1
141.30.228.182:4943:        1
141.30.228.189:1193:        1
141.30.228.189:1472:        1
141.30.228.189:1973:        1
141.30.228.189:1999:        1
141.30.228.189:2130:        1
141.30.228.189:2232:        1
141.30.228.189:2289:        1
141.30.228.189:2409:        1
141.30.228.189:2570:        1
141.30.228.189:2737:        1
141.30.228.189:3156:        1
141.30.228.189:3315:        2
141.30.228.189:3534:        1
141.30.228.189:3583:        1
141.30.228.189:3646:        1
141.30.228.189:3847:        1
141.30.228.189:4215:        1
141.30.228.189:4388:        1
141.30.228.199:1303:        1
141.30.228.199:1578:        2
141.30.228.199:2438:        1
141.30.228.199:2450:        1
141.30.228.199:3435:        1
141.30.228.199:3627:        1
141.30.228.199:4043:        1
141.30.228.199:4528:        1
141.30.228.199:4832:        1
141.30.228.221:2150:        1
141.30.228.221:2483:        1
141.30.228.221:3261:        1
141.30.228.221:3778:        1
141.30.228.221:3978:        1
141.30.228.221:4410:        1
141.30.228.222:1569:        1
141.30.228.222:1851:        1
141.30.228.222:2455:        1
141.30.228.222:2515:        1
141.30.228.222:2614:        1
141.30.228.222:2914:        1
141.30.228.222:3776:        1
141.30.228.43:1104:         1
141.30.228.43:1196:         1
141.30.228.43:1236:         1
141.30.228.43:1354:         1
141.30.228.43:1476:         1
141.30.228.43:1785:         1
141.30.228.43:1999:         1
141.30.228.43:2049:         1
141.30.228.43:2266:         1
141.30.228.43:2270:         1
141.30.228.43:2346:         1
141.30.228.43:2778:         1
141.30.228.43:2821:         1
141.30.228.43:2975:         1
141.30.228.43:3173:         1
141.30.228.43:3207:         1
141.30.228.43:3917:         1
141.30.228.43:3969:         1
141.30.228.43:4227:         1
```

```
     141.30.228.43:4317:           1
     141.30.228.43:4410:           1
     141.30.228.43:4493:           1
     141.30.228.43:4637:           1
     141.30.228.58:1031:           1
     141.30.228.58:1108:           1
     141.30.228.58:1374:           1
     141.30.228.58:2504:           1
     141.30.228.58:3520:           1
     141.30.228.58:3738:           1
     141.30.228.58:3984:           1
     141.30.228.58:4116:           1
     141.30.228.58:4652:           1
     194.154.201.2:63264:          1
     194.154.201.2:63705:          1
     194.249.91.190:2792:          1
     194.87.39.73:42413:           1
     194.87.39.73:42419:           1
     194.87.39.73:42424:           1
     204.42.254.5:33204:           1
     204.42.254.5:39357:           1
     204.42.254.5:44726:           1
     204.42.254.5:45615:           1
     204.42.254.5:45789:           1
     204.42.254.5:60397:           1
     207.96.122.8:20:              3
     207.96.122.8:51690:           1
     209.85.37.60:2027:            1
     209.85.37.60:3478:            1
     209.85.37.60:4034:            1
     209.85.37.60:4901:            1
     209.85.60.179:1978:           10
     24.66.70.156:1228:            1
     4.35.4.244:1837:              1
     62.155.143.10:3333:           1
     63.208.2.34:46739:            1
     64.108.199.136:37287:         1
-------------------------



-------------------------
Distribution of 'Queso fingerprint' destinations:
     MY.NET.110.249:6346:         1
     MY.NET.178.42:1974:          1
     MY.NET.201.146:6355:         2
     MY.NET.202.158:6355:         9
     MY.NET.202.234:6346:         1
     MY.NET.203.50:6346:          25
     MY.NET.204.102:6688:         1
     MY.NET.205.10:5500:          2
     MY.NET.205.174:6355:         1
     MY.NET.206.198:6346:         1
     MY.NET.206.30:5581:          1
     MY.NET.206.30:6346:          19
     MY.NET.206.42:6346:          1
     MY.NET.207.98:5858:          1
     MY.NET.208.46:6346:          1
     MY.NET.208.54:6355:          4
     MY.NET.208.90:6355:          10
     MY.NET.211.230:6355:         1
     MY.NET.211.250:6346:         1
     MY.NET.211.38:6346:          2
     MY.NET.211.74:1:             1
     MY.NET.211.74:6346:          18
     MY.NET.212.66:6346:          1
     MY.NET.213.194:6346:         2
     MY.NET.214.14:6346:          5
     MY.NET.217.242:6346:         4
     MY.NET.217.34:6355:          3
     MY.NET.217.58:6355:          6
     MY.NET.220.130:6355:         4
     MY.NET.220.14:2033:          1
     MY.NET.220.14:2136:          1
     MY.NET.220.14:2151:          1
     MY.NET.220.14:2153:          1
     MY.NET.220.14:2276:          1
     MY.NET.220.14:2355:          1
     MY.NET.220.14:2374:          1
     MY.NET.220.14:2463:          1
     MY.NET.220.14:2481:          1
     MY.NET.220.14:4858:          1
     MY.NET.220.6:6355:           7
     MY.NET.222.178:113:          1
     MY.NET.222.222:6346:         2
     MY.NET.222.230:6346:         2
     MY.NET.223.242:113:          1
     MY.NET.224.102:6346:         1
     MY.NET.224.242:6355:         6
     MY.NET.224.30:6346:          6
     MY.NET.224.90:6346:          2
     MY.NET.225.106:6346:         4
     MY.NET.225.198:6346:         1
     MY.NET.225.42:4964:          1
     MY.NET.225.98:6346:          1
     MY.NET.227.146:12506:        2
     MY.NET.229.22:6346:          15
     MY.NET.253.105:113:          1
     MY.NET.253.105:25:           1
     MY.NET.253.105:6000:         1
     MY.NET.253.41:25:            1
     MY.NET.253.43:25:            6
     MY.NET.53.152:3273:          1
     MY.NET.53.152:3297:          1
     MY.NET.53.152:3312:          1
     MY.NET.6.35:25:              1
     MY.NET.97.159:6346:          2
     MY.NET.97.79:113:            1
     MY.NET.98.118:113:           1
     MY.NET.98.166:6346:          1
-------------------------
```

Queso is tool that specializes in the identification of a remote operating system. Queso sends various test packets compares the responses against a list of known responses for various operating systems.

Russia Dynamo - SANS Flash 28-jul-00

```
02/03-20:46:15.618252  [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.203.50:6346 -> 194.87.6.79:1791
```

Despite this being a Snort alert with the tag ‘SANS Flash 28-jul-00’ I was unable to find much information on this attack, by name, from the SANS or Snort sites. I was able to discern that the 194.87.6.0/24 network is the cause of this alert.

Also of interest may be use of port 6346, as it is common for Gnutella services. This in only important if it and/or other peer-to-peer services, such as Napster are against network policy.

SNMP public access

```
01/30-00:01:03.208289  [**] SNMP public access [**] MY.NET.70.42:2155 ->
MY.NET.50.154:161
02/03-00:01:04.845994  [**] SNMP public access [**] MY.NET.70.42:1156 ->
MY.NET.50.154:161
02/03-00:01:05.046691  [**] SNMP public access [**] MY.NET.70.42:1156 ->
MY.NET.50.154:161
02/03-00:04:29.598072  [**] SNMP public access [**] MY.NET.111.156:1737 ->
MY.NET.50.154:161
02/03-00:04:30.898906  [**] SNMP public access [**] MY.NET.111.156:1737 ->
MY.NET.50.154:161
```

Depending on the nature of the machine providing the SNMP data, MY.NET.50.154, this might be completely legitimate traffic. It might be work investigating what type of system MY.NET.50.154 is. As a best practices guideline, the use of the "public" community string should be avoided. It is suggested that the community string be changed and/or password protected, if possible.

SUNRPC highport access

```
01/30-14:34:29.280204  [**] SUNRPC highport access! [**] 200.233.81.13:13765
-> MY.NET.60.17:32771
01/30-19:19:16.387947  [**] SUNRPC highport access! [**] 24.9.203.188:61207
-> MY.NET.165.129:32771
02/03-22:17:09.957552  [**] SUNRPC highport access! [**] 205.188.5.157:5190
-> MY.NET.98.227:32771
02/03-22:17:10.679807  [**] SUNRPC highport access! [**] 205.188.5.157:5190
-> MY.NET.98.227:32771
```

The 205.188.5.157 address doesn't resolve though it does lie within the addresses registered to AOL by ARIN. Most likely these alerts represent legitimate AOL Instant Messenger traffic and are, therefore, false positives.

The 200.233.81.13 and 24.9.203.188 addresses, however, don't seem to have such a correlation to AOL. Therefore, they are worth investigating further. Internet addresses should not be sucessfully connecting to these port numbers.

SYN-FIN scan!

```
-------------------------
Distribution of 'SYN-FIN scan' sources:
     209.255.180.130:32808:       1
     211.248.112.67:53:           1108
     24.50.25.5:6699:             1
     4.35.4.244:1837:             1
     63.252.15.242:2754:          1
-------------------------
```

Due to its size, the distribution of destinations has not been included. In summary, the 1,108 scan packets from 211.248.112.67 were all directed at port 53 and ranged across more than 1,000 hosts. The remaining four alerts were directed at other ports:

```
02/03-16:41:50.481325  [**] SYN-FIN scan! [**] 209.255.180.130:32808 ->
MY.NET.5.29:259
02/04-10:16:07.886629  [**] SYN-FIN scan! [**] 24.50.25.5:6699 ->
MY.NET.211.122:1415
```

```
02/06-16:49:34.770262  [**] SYN-FIN scan! [**] 63.252.15.242:2754 ->
MY.NET.5.29:443
02/11-02:49:26.226895  [**] SYN-FIN scan! [**] 4.35.4.244:1837 ->
MY.NET.211.74:6346
```

Researching 211.248.112.67 lead to (http://www.apnic.net/apnic-bin/whois.pl?search=211.248.112.67) at APNIC. The whois search results show that the range of IP addresses this address falls into is registered to the Korea Network Information Center. I'm not sure why this national organization would be scanning MY.NET, but I strongly recommend that they be notified of the activity.

The other four scan alerts indicate selective probing. I recommend checking those hosts in MY.NET for services and/or trojans running on the targeted ports. I also recommend adding those source addresses to the list of IP addresses to watch and see if there is more activity, indicate an exploit attempt or, even worse, a successful exploit.

TCP SMTP Source Port traffic

```
01/30-14:31:36.054897  [**] TCP SMTP Source Port traffic [**]
11.125.218.156:25 -> MY.NET.60.17:274
01/30-14:34:09.165435  [**] TCP SMTP Source Port traffic [**]
17.135.218.56:25 -> MY.NET.60.17:979
02/03-05:46:31.726285  [**] TCP SMTP Source Port traffic [**]
195.211.49.18:25 -> MY.NET.139.54:1007
02/04-05:37:48.374429  [**] TCP SMTP Source Port traffic [**]
200.251.185.30:25 -> MY.NET.158.238:399
```

There are reports of a network scanner tool that uses a source port of 25 for its scans. A quick check of these outside IP addresses shows that none of them have generated any other alerts. If one were to have free time, a check of the full packet log data might turn up some new type of scanner or exploit signature. Most likely, however, these are simply false positives.

Tiny Fragments - Possible Hostile Activity

```
-------------------------
Distribution of 'Tiny Fragments - Possible Hostile Activity' sources:
     111.111.111.111:              2
     127.0.0.1:                    1
     202.101.43.220:               2
     202.205.5.10:                 6
     202.96.96.3:                  5
     210.12.160.130:               1
     61.134.9.133:                 2
     61.134.9.134:                 1
     61.136.61.68:                 2
     61.140.75.3:                  1
     61.140.75.5:                  2
     61.155.13.3:                  1
     64.80.88.99:                  5
     64.80.89.149:                 2
     64.80.90.36:                  73
     64.80.90.55:                  2
     64.80.90.84:                  3
-------------------------
```

```
-------------------------
Distribution of 'Tiny Fragments - Possible Hostile Activity' destinations:
     MY.NET.1.10:                 7
     MY.NET.1.8:                  16
     MY.NET.160.109:              5
     MY.NET.20.10:               3
     MY.NET.206.254:             5
     MY.NET.206.58:              1
     MY.NET.228.10:              1
     MY.NET.97.231:              20
     MY.NET.98.117:              53
-------------------------
```

Tiny fragments could indicate an attempt to penetrate a firewall or establish a denial of service attack on the firewall, itself. Furthermore, there are known system exploits (Ping of Death, Kiss of Death, etc.) which prey upon OS vulnerabilities resulting in a number of problems, including a system panic on the firewall or systems behind it. On the other hand, these fragmented packets could indicate a network problem such as failing/faulty equipment, network congestion, etc. Despite whether the packets are the result of an attack or indication of network issues, they signify a problem that needs to be addressed.

The source address with the highest count, 64.80.90.36, communicated exclusively with the destination addresses with the highest counts, MY.NET.98.117 and MY.NET.97.231. The packet dumps from these communications could indicate whether there are network issues (equipment problems, congestion, etc.) or an actual attack.

The packets from 111.111.111.111 and 127.0.0.1 are very interesting as the 96.0.0.0 - 126.255.255.255 address range is reserved by IANA and a legitimate localhost (127.0.0.0 - 127.255.255.255) packet should never be seen by a network interface. These are either spoofed or corrupted packets, and investigation of those packets could give insight into whether there are network issues or an actual attack.

Watchlist IDs

```
-------------------------
Distribution of Watchlist IDs:
     000220:                   3702
     000222:                   5388
-------------------------



-------------------------
Distribution of 'Various Watchlist alerts' sources:
     159.226.111.1:33357:        2
     159.226.112.195:6476:       1
     159.226.114.1:36720:        1
     159.226.114.1:36729:        3
     159.226.120.19:113:         1
     159.226.126.85:37529:       1
     159.226.126.85:54681:       1
     159.226.197.106:26160:      1
     159.226.215.205:15499:      1
     159.226.227.72:44450:       1
     159.226.39.4:2859:          4
     159.226.39.4:2862:          2
     159.226.45.3:2957:          1
     159.226.47.195:32888:       1
     159.226.47.217:33678:       1
     159.226.61.246:36683:       1
     159.226.63.107:9258:        1
     159.226.63.200:2046:        1
     159.226.81.1:1026:          3
--- The sequence is almost continuous from port 1026 through port 5000. ---
--- Multiples exist for almost all ports in the range. ---
--- Port 113 has the most alerts reported, 700. ---
--- The total alert count for source IP 159.226.81.1 is 5362. ---
```

```
     159.226.81.1:5000:            3
     159.226.92.10:113:            1
     212.179.125.114:63912:        2
     212.179.21.179:1172:          2186
     212.179.27.6:1024:            81
     212.179.28.66:16940:          133
     212.179.40.132:63255:         152
     212.179.41.220:1844:          15
     212.179.42.21:6699:           321
     212.179.42.76:2993:           1
     212.179.42.76:3105:           1
     212.179.47.83:1572:           272
     212.179.51.114:11562:         1
     212.179.58.193:2226:          260
     212.179.79.2:12693:           206
     212.179.79.2:15240:           1
     212.179.79.2:20812:           1
     212.179.79.2:25042:           13
     212.179.79.2:29459:           36
     212.179.79.2:30916:           1
     212.179.79.2:32746:           1
     212.179.79.2:34637:           1
     212.179.79.2:47172:           1
     212.179.79.2:48386:           4
     212.179.79.2:49441:           1
     212.179.79.2:49809:           7
     212.179.79.2:51654:           2
     212.179.79.2:56577:           2
-------------------------


-------------------------
Distribution of 'Various Watchlist alerts' destinations:
     MY.NET.100.230:113:          1
     MY.NET.100.230:25:           4
     MY.NET.145.9:58587:          1
     MY.NET.201.242:4939:         2
     MY.NET.204.22:6699:          272
     MY.NET.204.78:6699:          81
     MY.NET.206.94:6699:          15
     MY.NET.207.226:6699:         2186
     MY.NET.211.74:6346:          133
     MY.NET.217.98:4222:          207
     MY.NET.221.114:2340:         2
     MY.NET.221.162:4879:         2
     MY.NET.222.94:2609:          134
     MY.NET.222.94:2610:          187
     MY.NET.224.126:4879:         1
     MY.NET.224.34:6688:          260
     MY.NET.225.186:6688:         152
     MY.NET.253.42:57319:         1
     MY.NET.253.43:25:            23
     MY.NET.253.43:45482:         1
     MY.NET.253.43:45503:         1
     MY.NET.253.43:45527:         1
     MY.NET.253.43:45868:         1
     MY.NET.253.51:113:           1
     MY.NET.6.34:25:              2
     MY.NET.6.35:25:              5
     MY.NET.6.47:25:              4658
     MY.NET.6.47:33933:           1
--- The sequence is roughly continuous from port 33933 to 40850. ---
--- Multiples exist for no ports in the range. ---
--- The total alert count for destination IP MY.NET.6.47 is 5337. ---
     MY.NET.6.47:40850:           1
     MY.NET.6.7:113:              1
     MY.NET.60.17:156:            1
     MY.NET.60.17:39386:          1
     MY.NET.60.17:52051:          1
     MY.NET.60.17:5481:           1
     MY.NET.60.17:587:            1
     MY.NET.60.17:6586:           1
     MY.NET.60.17:6909:           1
     MY.NET.60.17:804:            1
     MY.NET.60.17:9157:           1
     MY.NET.97.30:4116:           55
     MY.NET.97.62:4511:           11
     MY.NET.98.185:4511:          1
-------------------------
```

Watchlist 000222 NET-NCFC is an alert triggered for any packets from NCFC (159.226.0.0 - 159.226.255.255), in China. This is in response to significant suspicious activity from that network in the past.

There are 4692 alerts in this format:

```
02/03-09:08:59.679272  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859
-> MY.NET.100.230:25
02/03-09:09:03.444937  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859
-> MY.NET.100.230:25
02/03-09:09:08.908327  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859
-> MY.NET.100.230:25
02/03-09:09:09.400820  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859
-> MY.NET.100.230:25
02/03-09:09:14.301649  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2862
-> MY.NET.253.43:25
```

All 4692 of these alerts were triggered from packets destined for the following hosts on MY.NET:

```
     MY.NET.100.230:              4
     MY.NET.253.43:               23
     MY.NET.6.34:                 2
     MY.NET.6.35:                 5
     MY.NET.6.47:                 4658
```

In summary, there appear to be a lot of SNMP probes from NCFC. I would suggest further investigation of the five targeted SMTP servers (MY.NET.100.230, MY.NET.253.43, MY.NET.6.34, MY.NET.6.35, and MY.NET.6.47). Especially, MY.NET.6.47, as it is the single biggest destination host for the NCFC traffic.

Watchlist 000220 IL-ISDNNET-990517 is an alert triggered for any packets from 212.179.0.0/17, in Israel. This is in response to suspicious activity from that network in the past.

Within this subset of Watchlist alerts, the source address with the highest count, 212.179.21.179, communicated exclusively with the destination address with the highest count, MY.NET.207.226. The use of port 6699, seems to indicate the use of Napster. I would suggest further investigation of that machine, with regard to the network policy regarding the use of peer-to-peer services such as this.

WinGate 1080 Attempt

```
-------------------------
Distribution of 'WinGate 1080 Attempt' sources:
```

```
128.121.244.217:1205:         1
128.121.244.217:1632:         1
128.121.244.217:1746:         1
128.121.244.217:1781:         1
128.121.244.217:1954:         1
128.121.244.217:2149:         1
128.121.244.217:2295:         1
128.121.244.217:2574:         1
128.121.244.217:2819:         1
128.121.244.217:2901:         1
128.121.244.217:3118:         1
128.121.244.217:3178:         1
128.121.244.217:3250:         1
128.121.244.217:3310:         1
128.121.244.217:3516:         1
128.121.244.217:3645:         1
128.121.244.217:3827:         1
128.121.244.217:4080:         1
128.121.244.217:4393:         1
128.121.244.217:4508:         1
128.121.244.217:4737:         1
128.220.101.100:20:           1
148.233.219.106:1272:         1
154.5.207.52:3619:            1
161.58.8.77:20:               1
172.145.180.190:1531:         1
172.145.180.190:1825:         1
195.152.235.159:14955:        1
199.173.178.2:1361:           1
199.173.178.2:1418:           2
199.173.178.2:2472:           1
199.173.178.2:2679:           1
199.173.178.2:2817:           1
199.173.178.2:2892:           1
199.173.178.2:3330:           1
199.173.178.2:3366:           1
199.173.178.2:3865:           1
199.173.178.2:3895:           1
199.173.178.2:4085:           1
199.173.178.2:4562:           1
199.173.178.2:4569:           1
199.173.178.2:4762:           1
199.173.178.2:4837:           1
199.173.178.2:4873:           1
199.173.178.2:4931:           1
202.169.133.164:11237:        1
203.128.252.44:2873:          1
203.164.81.35:2283:           1
203.168.0.12:1372:            2
203.45.154.120:4411:          1
204.117.70.5:1098:            1
204.117.70.5:1265:            1
204.117.70.5:1657:            1
204.117.70.5:2638:            1
204.117.70.5:3235:            1
204.117.70.5:3507:            1
204.117.70.5:3549:            1
204.117.70.5:3674:            1
204.117.70.5:3700:            1
204.117.70.5:4372:            1
204.117.70.5:4834:            1
204.117.70.5:4949:            1
205.136.57.121:1470:          1
```

```
205.136.57.121:4440:          1
205.136.57.121:4549:          1
205.245.78.188:63219:         1
205.252.89.115:1411:          1
206.105.43.5:1611:            1
206.204.3.253:20:             1
207.126.106.118:3453:         1
207.126.106.118:4240:         1
208.191.171.235:1374:         1
208.191.171.235:2036:         1
209.1.233.136:2326:           1
209.1.233.136:2861:           1
209.10.77.201:3697:           1
209.210.178.105:48956:        1
209.212.128.41:2027:          1
209.212.128.47:1420:          1
209.212.128.47:2306:          1
209.212.128.47:3559:          1
209.212.128.47:4283:          1
209.212.128.47:4783:          1
209.222.114.225:3874:         1
209.222.114.225:4223:         2
209.49.141.9:42670:           1
210.107.195.13:1447:          1
210.107.195.13:2107:          1
212.17.106.32:4023:           1
212.73.162.30:34138:          1
212.73.162.30:34657:          1
212.73.162.30:39154:          1
212.73.162.30:43029:          1
212.73.162.30:45027:          2
212.73.162.30:47549:          1
212.73.162.30:51533:          1
212.73.162.30:54558:          1
212.73.162.30:56849:          1
212.73.162.30:60764:          1
213.61.112.10:1037:           1
213.61.112.10:4972:           1
216.120.76.195:2351:          1
216.120.76.195:3197:          1
216.179.0.32:1221:            1
216.179.0.32:1272:            2
216.179.0.32:1311:            1
216.179.0.32:1800:            1
216.179.0.32:1847:            1
216.179.0.32:2020:            1
216.179.0.32:2031:            1
216.179.0.32:2329:            1
216.179.0.32:2441:            1
216.179.0.32:3780:            1
216.179.0.32:4467:            1
216.179.0.32:4862:            1
216.179.0.32:4878:            2
216.234.161.197:2298:         1
216.234.161.197:2313:         1
216.234.161.197:2779:         1
216.234.161.197:3728:         1
216.35.103.80:58673:          1
216.35.217.66:20:             1
216.54.223.198:9474:          1
237.70.255.190:62558:         1
24.1.201.200:1137:            1
24.1.201.200:1256:            1
```

```
     24.1.201.200:1284:            1
     24.1.201.200:1323:            1
     24.1.201.200:1606:            1
     24.1.201.200:1736:            1
     24.1.201.200:2153:            1
     24.1.201.200:2493:            1
     24.1.201.200:2563:            1
     24.1.201.200:2638:            1
     24.1.201.200:2748:            1
     24.1.201.200:2792:            1
     24.1.201.200:2859:            1
     24.1.201.200:3239:            1
     24.1.201.200:3381:            1
     24.1.201.200:3548:            1
     24.1.201.200:3643:            1
     24.1.201.200:3803:            1
     24.1.201.200:3827:            1
     24.1.201.200:4031:            1
     24.1.201.200:4148:            1
     24.1.201.200:4153:            1
     24.1.201.200:4508:            1
     24.1.201.200:4602:            1
     24.1.201.200:4607:            1
     24.1.201.200:4693:            1
     24.1.201.200:4730:            1
     24.1.201.200:4836:            1
     24.1.201.200:4906:            1
     24.114.232.44:1534:           1
     24.114.232.44:3307:           1
     24.18.15.120:1517:            1
     24.202.82.28:2408:            1
     24.9.203.188:64450:           1
     24.93.200.116:4586:           1
     55.84.106.246:31937:          1
     63.151.165.130:1106:          1
     63.151.165.130:1161:          1
     63.151.165.130:1256:          1
     63.151.165.130:1331:          1
     63.151.165.130:1336:          1
     63.151.165.130:1364:          1
     63.151.165.130:1457:          1
     63.151.165.130:1689:          1
     63.151.165.130:1776:          1
     63.151.165.130:2081:          1
     63.151.165.130:2125:          1
     63.151.165.130:4473:          1
     63.151.165.130:4680:          1
     63.151.165.130:4860:          1
     63.165.90.113:4837:           1
     63.248.65.53:2570:            1
     64.154.61.232:2171:           1
     64.229.12.51:1449:            1
     64.229.12.51:1919:            1
     64.65.0.178:4264:             1
     64.84.40.12:1979:             1
     64.84.40.12:3884:             1
     66.20.176.104:1749:           1
     66.44.11.2:1506:              1
     66.44.15.92:2874:             1
-------------------------


-------------------------
```

```
Distribution of 'WinGate 1080 Attempt' destinations:
     MY.NET.100.203:1080:          2
     MY.NET.15.178:1080:           21
     MY.NET.165.129:1080:          1
     MY.NET.178.42:1080:           1
     MY.NET.201.102:1080:          1
     MY.NET.201.170:1080:          1
     MY.NET.202.138:1080:          7
     MY.NET.202.158:1080:          1
     MY.NET.203.234:1080:          9
     MY.NET.203.82:1080:           2
     MY.NET.203.94:1080:           1
     MY.NET.204.102:1080:          1
     MY.NET.204.22:1080:           1
     MY.NET.204.38:1080:           1
     MY.NET.205.126:1080:          2
     MY.NET.205.174:1080:          1
     MY.NET.205.234:1080:          2
     MY.NET.207.98:1080:           1
     MY.NET.208.222:1080:          2
     MY.NET.209.234:1080:          1
     MY.NET.209.26:1080:           1
     MY.NET.209.98:1080:           1
     MY.NET.210.138:1080:          1
     MY.NET.210.38:1080:           2
     MY.NET.210.74:1080:           1
     MY.NET.211.154:1080:          1
     MY.NET.214.58:1080:           2
     MY.NET.214.62:1080:           1
     MY.NET.217.122:1080:          1
     MY.NET.217.130:1080:          1
     MY.NET.217.202:1080:          1
     MY.NET.218.114:1080:          3
     MY.NET.218.230:1080:          1
     MY.NET.218.86:1080:           5
     MY.NET.220.14:1080:           1
     MY.NET.220.74:1080:           1
     MY.NET.221.234:1080:          1
     MY.NET.221.30:1080:           29
     MY.NET.222.178:1080:          2
     MY.NET.222.54:1080:           1
     MY.NET.223.114:1080:          1
     MY.NET.223.242:1080:          2
     MY.NET.224.166:1080:          2
     MY.NET.224.190:1080:          1
     MY.NET.225.66:1080:           3
     MY.NET.225.74:1080:           2
     MY.NET.226.238:1080:          1
     MY.NET.226.34:1080:           1
     MY.NET.227.218:1080:          1
     MY.NET.227.70:1080:           1
     MY.NET.229.162:1080:          1
     MY.NET.60.11:1080:            1
     MY.NET.60.17:1080:            4
     MY.NET.60.38:1080:            2
     MY.NET.60.8:1080:             6
     MY.NET.97.121:1080:           1
     MY.NET.97.13:1080:            1
     MY.NET.97.194:1080:           1
     MY.NET.97.200:1080:           1
     MY.NET.97.229:1080:           1
     MY.NET.97.38:1080:            1
     MY.NET.97.40:1080:            1
     MY.NET.97.62:1080:           2
     MY.NET.97.69:1080:           2
     MY.NET.97.72:1080:           1
     MY.NET.97.87:1080:           1
     MY.NET.98.110:1080:          1
     MY.NET.98.112:1080:          1
     MY.NET.98.118:1080:          14
     MY.NET.98.120:1080:          1
     MY.NET.98.132:1080:          1
     MY.NET.98.150:1080:          1
     MY.NET.98.156:1080:          4
     MY.NET.98.167:1080:          1
     MY.NET.98.185:1080:          1
     MY.NET.98.187:1080:          1
     MY.NET.98.189:1080:          2
     MY.NET.98.197:1080:          1
     MY.NET.98.198:1080:          1
     MY.NET.98.22:1080:           1
     MY.NET.98.241:1080:          1
     MY.NET.98.248:1080:          1
-------------------------
```

These alerts could represent probes or exploits associated with the WinGate or SOCKS proxies running on port 1080. Most likely these are false positives, however, one might want to check any such proxies in MY.NET that correspond to the destination list, above.

connect to 515 from inside

```
-------------------------
Distribution of 'connect to 515 from inside' sources:
     MY.NET.162.71:2878:           1
     MY.NET.201.170:2697:          1
     MY.NET.7.20:22:               15
     MY.NET.97.88:1025:            59
     MY.NET.98.190:1025:           514
-------------------------
```

```
-------------------------
Distribution of 'connect to 515 from inside' destinations:
     209.249.182.79:515:          1
     209.50.66.2:515:             1
     216.181.129.185:515:         573
     216.88.97.58:515:            15
-------------------------
```

The source addresses with the highest counts, MY.NET.97.88 and MY.NET.98.190, communicated exclusively with the destination address with the highest count, 216.181.129.185.

In general, hosts on MY.NET should not need to connect to lpd or spooler services (port 515) on outside machines. No other alerts were generated for these IP addresses. This is suspicious activity, however, and given the limited set of "offenders" further investigation of these IP addresses might be worthwhile. On one hand, a host might be compromised and spooling print jobs to outside systems, on the other hand, a user might be sending a print to their home.