Global Information Assurance Certification Paper

SANS GIAC Certified Intrusion Analysts (GCIA)

Practical Assignment for Capitol SANS,

December 10-15, 2000, Washington D.C.

Submitted by:

TED FERRETTA

January 2001

---

1) NETWORK DETECTS

<> DETECT #1: SYN-FIN Scans With Same Datagram ID Numbers

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:07.715355 203.32.161.197:21 - MY.NET.1.4:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x4D641BCC   Ack: 0x2641A89   Win: 0x404
9C 00 88 87 2D 1E                                 ....-.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:07.736085 203.32.161.197:21 - MY.NET.1.5:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x4D641BCC   Ack: 0x2641A89   Win: 0x404
0A 4D 5B 4B 4D 51                                 .M[KMQ
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:08.533969 203.32.161.197:21 - MY.NET.1.45:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x4D641BCC   Ack: 0x2641A89   Win: 0x404
00 00 00 00 00 00                                 ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:08.676131 203.32.161.197:21 - MY.NET.1.52:21
TCP TTL:26 TOS:0x0 ID:39426
```

```
**SF**** Seq: 0x3AD1187B   Ack: 0x76B68378   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:08.696793 203.32.161.197:21 - MY.NET.1.53:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x3AD1187B   Ack: 0x76B68378   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

       .
.
.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/02-06:26:27.055885 208.61.4.207:9704 - MY.NET.1.6:9704
TCP TTL:28 TOS:0x0 ID:39426
**SF**** Seq: 0x4B34FDE8   Ack: 0x11550072   Win: 0x404
B7 CC C7 D8 E0 17                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/02-16:59:04.636915 212.177.241.101:21 - MY.NET.1.4:21
TCP TTL:27 TOS:0x0 ID:39426
**SF**** Seq: 0x4C60905D   Ack: 0x1820B92   Win: 0x404
24 4A 3B 22 9D A5                                  $J;"..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/03-08:41:23.592641 209.92.40.32:9704 - MY.NET.1.0:9704
TCP TTL:28 TOS:0x0 ID:39426
**SF**** Seq: 0x3E824A80   Ack: 0x4C4F249   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-00:49:16.135987 128.2.81.133:21 - MY.NET.1.21:21
TCP TTL:34 TOS:0x0 ID:39426
**SF**** Seq: 0x511AE364   Ack: 0x4CF340E0   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-11:28:13.371327 63.195.56.20:21 - MY.NET.1.19:21
TCP TTL:27 TOS:0x0 ID:39426
**SF**** Seq: 0x2733439A   Ack: 0x25170DEA   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-19:25:53.085552 202.153.112.222:21 - MY.NET.1.11:21
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x4AAB756B   Ack: 0x2281813E   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/07-11:19:49.767207 163.10.19.34:21 - MY.NET.4.4:21
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x2E23A391   Ack: 0x6B53C321   Win: 0x404
00 00 00 00 00 00                                  ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1. Source of Trace.
   From SANS GIAC Certified Intrusion Analysts (GCIA) Practical Assignment
   for Capitol SANS, December 10-15, 2000, Washington D.C.

2. Detect was generated by:
   Snort looking for SYN-FIN scans; this is a partial listing from a 7 day
   period extracted from the Capitol SANS GCIA Practical OOSche<#.txt files.
   (Note: This data represents a number of SYN-FIN scans over a number of
   days - we particularly chose this collection of packets as we have different
   source IPs with the same ID number. The first few packets are all from the
   same IP. Then we have a break and the remaining packets are all from different
   IPs, but still have same ID number.)

3. Probability the source address was spoofed:
   Unlikely, SYN-FIN scans are not normally useful unless a
   response is returned to the sender.

4. Description of attack:
   A TCP probe was sent with the SYN and FIN flags set. This does not occur normally
   and indicates an intentional probe, likely as part of a single-packet OS detection.

5. Attack mechanism:
   Sending a crafted packet with the SYN and FIN flags both set, will sneak past some
   firewalls which are attempting to block outside traffic. Also, some logging mechanisms
   will not log such a packet as it sees the FIN as tearing down a connection and does
   not log such an event. SYN-FIN packets can also be used in operating system
   fingerprinting (linux systems are known to respond with a SYN-FIN-ACK.

6. Correlations:
   http://www.securityfocus.com - numerous references here

7. Evidence of active targeting:
   Yes, the beginning packets are part of a bigger picture, showing one IP, 203.32.161.197,
   scanning through a range of different 4512 IPs, all to port 21.

8. Severity:

   ```
   Criticality             = 4,  the scan, if successful will map a significant part of the
                                 network, and identify some linux operating systems.
   Lethality               = 4,  because there are many known FTP (port 21) vulnerabilities
   System countermeasures  = 2,  if we assume all systems running latest patches, but
                                 some are listening on the FTP port
   Network countermeasures = 0,  assuming that's why you are entertaining hiring us
   ```

   Severity = (Criticality + Lethality) - (System + Net Countermeasures)
            = (4+4) - (2+0)
            = 6

9. Defensive recommendation:

Can be blocked by a well designed firewall.

10. Multiple choice test question:
    The same ID number on these packets indicates:
    a) They all passed through the same router.
    b) The different IP addresses are spoofed and
       the packets all come from the same host.
    c) The different IP addresses are not spoofed but each
       is using the same tool for there scans, and this
       tool happens to have the ID number hard coded into
       the crafted SYN-FIN packets.
    d) The packets all came from the same fragmented
       datagram.

    Answer: c

<> DETECT #2: Insecure TIMBUKTU Password

```
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:03.982386 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x3D
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:26116  DF
*****PA* Seq: 0x198040   Ack: 0xC609A1   Win: 0x1FB3
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:04.349692 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x44
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:26628  DF
*****PA* Seq: 0x198047   Ack: 0xC609AD   Win: 0x1FA7
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:04.651210 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x44
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:27140  DF
*****PA* Seq: 0x198055   Ack: 0xC609E5   Win: 0x1F6F
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:04.956150 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x4B
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:27652  DF
*****PA* Seq: 0x198063   Ack: 0xC60A13   Win: 0x1F41
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:05.247455 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x44
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:28164  DF
*****PA* Seq: 0x198078   Ack: 0xC60A41   Win: 0x1F13
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:05.548249 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x3D
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:28676  DF
*****PA* Seq: 0x198086   Ack: 0xC60A76   Win: 0x1EDE
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:05.850208 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x3D
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:29188  DF
*****PA* Seq: 0x19808D   Ack: 0xC60AA4   Win: 0x1EB0
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:06.151273 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x4B
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:29700  DF
*****PA* Seq: 0x198094   Ack: 0xC60AD2   Win: 0x1E82
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:06.280689 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x3D
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:29956  DF
*****PA* Seq: 0x1980A9   Ack: 0xC60ADE   Win: 0x1E76
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Insecure TIMBUKTU Password [**]
12/22-06:02:07.393765 0:0:A5:13:BF:0 - 0:D0:6:93:CC:1 type:0x800 len:0x3D
OUTSIDE.NET.246.13:1157 - INSIDE.NET.79.161:1417 TCP TTL:127 TOS:0x0 ID:30724  DF
*****PA* Seq: 0x1980B0   Ack: 0xC60B3A   Win: 0x1E1A
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1. Source of Trace.
   my network

2. Detect was generated by:
   Snort with the following rule:
   ```
   alert TCP any any - any 1417 (msg:"Insecure TIMBUKTU Password"; flags: PA; content: "|0500 3E|"; depth: 16; )
   ```

3. Probability the source address was spoofed:
   Unlikely

4. Description of attack:
   Insecure traffic to Timbuktu remote control software, passwords are passed in plaintext and can be sniffed.
   What we detect here is not an attack but a vulnerability.

5. Attack mechanism:
   Netopia's Timbuktu Pro is a remote administration software package which runs on Microsoft
   Windows NT (among other platforms). When a user of a Windows NT host logs into their machine
   remotely via Timbuktu Pro, the username and password of the user are sent to the host for
   authentication in cleartext (unencrypted). This allows for anyone who is sniffing network
   traffic to retrieve the username and password pair, exactly as were typed in by the user, and
   access the host being logged into as the user logging in (and possibly compromise the entire
   machine). This affects Netopia Timbuktu Pro 2.0 and 3.0.
   To exploit this, an attacker would wait for someone on your shared LAN to access a target host

with Timbuktu. Sniff the traffic going from user to target host, tcp destination port 1417.
The packets containing the characters typed will have (in the data segment) an initial hex sequence
of "05 00 3E" each (followed by the uppercased character).

6. Correlations:
http://www.securityfocus.com BugtraqID 935
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0086
http://www.whitehats.com/info/IDS229

7. Evidence of active targeting:
No; it turns out the traffic was normal.

8. Severity:

```
Criticality             = 2,  presuming these are not critical servers
Lethality               = 5,  egads!!!, passwords in clear text over the network
System countermeasures  = 2,  if we assume all systems running latest patches, but
                              this won't help with cleat text passwords
Network countermeasures = 5,  using a virtual private network; server behind very restictive firewall

Severity = (Criticality + Lethality) - (System + Net Countermeasures)
         = (2+5) - (2+5)
         = 0
```

9. Defensive recommendation:
Netopia suggests installing a VPN. http://www.netopia.com/software/tb2/index.html

10. Multiple choice test question:

Virtual Private Networks (VPNs) are useful in network security because:
a) Usernames and passwords are encrypted as the travel over the network.
b) Packet headers are encrypted as the travel across the network
c) Packet payloads are encrypted as the travel across the network
d) All except (b).
Answer: d

<> DETECT #3: HTTP Directory Traversal

```
01/08-18:58:27.521447 OUTSIDE.NET.230.48:1656 - INSIDE.NET.130:80 TCP TTL:125 TOS:0x0 ID:62745  DF
*****PA* Seq: 0x29CF9B0   Ack: 0x9302676D   Win: 0x2238
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 69 77 6E  GET /cgi-bin/iwn
32 3F 2E 2E 2F 68 74 64 6F 63 73 2F 63 61 6C 69  2?../htdocs/cali
66 32 37 2E 74 65 6D 70 20 32 37 20 46 72 65 6D  f27.temp 27 Frem
6F 6E 74 20 48 54 54 50 2F 31 2E 30 0D 0A 43 6F  ont HTTP/1.0..Co
01/08-19:00:29.150368 OUTSIDE.NET.230.48:1657 - INSIDE.NET.130:80 TCP TTL:125 TOS:0x0 ID:65049  DF
*****PA* Seq: 0x29ED106   Ack: 0x11B0462A   Win: 0x2238
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 69 77 6E  GET /cgi-bin/iwn
32 3F 2E 2E 2F 68 74 64 6F 63 73 2F 63 61 6C 69  2?../htdocs/cali
66 32 37 2E 74 65 6D 70 20 32 37 20 46 72 65 6D  f27.temp 27 Frem
6F 6E 74 20 48 54 54 50 2F 31 2E 30 0D 0A 43 6F  ont HTTP/1.0..Co
01/08-19:02:34.466729 OUTSIDE.NET.230.48:1658 - INSIDE.NET.130:80 TCP TTL:125 TOS:0x0 ID:1562  DF
*****PA* Seq: 0x2A0BC3F   Ack: 0xBD8D1E3F   Win: 0x2238
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 69 77 6E  GET /cgi-bin/iwn
32 3F 2E 2E 2F 68 74 64 6F 63 73 2F 63 61 6C 69  2?../htdocs/cali
66 32 37 2E 74 65 6D 70 20 32 37 20 46 72 65 6D  f27.temp 27 Frem
6F 6E 74 20 48 54 54 50 2F 31 2E 30 0D 0A 43 6F  ont HTTP/1.0..Co
01/08-19:04:36.316824 OUTSIDE.NET.230.48:1659 - INSIDE.NET.130:80 TCP TTL:125 TOS:0x0 ID:4122  DF
*****PA* Seq: 0x2A295CA   Ack: 0x1B6F8E2C   Win: 0x2238
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 69 77 6E  GET /cgi-bin/iwn
32 3F 2E 2E 2F 68 74 64 6F 63 73 2F 63 61 6C 69  2?../htdocs/cali
66 32 37 2E 74 65 6D 70 20 32 37 20 46 72 65 6D  f27.temp 27 Frem
6F 6E 74 20 48 54 54 50 2F 31 2E 30 0D 0A 43 6F  ont HTTP/1.0..Co
```

1. Source of Trace.
my network

2. Detect was generated by:
Snort with the following rule:
alert TCP any any - any 80 (msg:"http-directory-traversal 1"; flags: PA; content: "../";)

3. Probability the source address was spoofed:
Unlikely, the source is most likely trying to access data at a web site.

4. Description of attack:
This signature may indicate an attempt to traverse directory limitations through a vulnerable
web server daemon or CGI script. This alert could be caused by several different attacks based
on ".." directory traversal.

5. Attack mechanism:
Numerous web servers and CGI scripts are vulnerable to directory traversal attacks. In many
cases the web application may intend to allow access to a particular portion of the filesystem.
Without proper checking of user input, a user could often add ".." directories to the path
allowing access to parent directories, possibly climbing to the root directory and being able
to access the entire filesystem.

6. Correlations:
CVE entries: CVE-1999-0842, CVE-1999-0887, CVE-2000-0436, CAN-2000-0443

7. Evidence of active targeting:
Yes, the user is going to a specific port on a specific host.

```
8. Severity:

   Criticality             = 3,  fairly important web server
   Lethality               = 4,  attacker could gain access to entire filesystem
   System countermeasures  = 3,  system running latest patches, but
                                 some are listening on the FTP port
   Network countermeasures = 4,  IDS/firewall system detects and blocks this traffic

   Severity = (Criticality + Lethality) - (System + Net Countermeasures)
            = (3+4) - (3+4)
            = 0
```

9. Defensive recommendation:
   Update web server to most recent version. Block traffic to web site that triggers such an alert.

10. Multiple choice test question:

    Allowing web site users to have relative paths in their URLs is poor practice because:
    a) If the root directory for web site is moved the old reference will still be valid and you may not want the user access to the old directories.
    b) Relative paths are resolved before absolute paths and can be used for a web site denial of service attack.
    c) It may allow a user to access the entire file system of a web server system.
    d) It is less efficient than using absolute paths.

    Answer: c

<> DETECT 4: WinGate-1080-Attempt

```
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:28.396979 OUTSIDE.NET.232.40:3925 - INSIDE.NET.133.1:1080 TCP TTL:117 TOS:0x0 ID:2547
**S***** Seq: 0x3E33F61   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:28.476037 OUTSIDE.NET.232.40:3926 - INSIDE.NET.133.2:1080 TCP TTL:117 TOS:0x0 ID:2803
**S***** Seq: 0x3E33FAE   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:28.546359 OUTSIDE.NET.232.40:3927 - INSIDE.NET.133.3:1080 TCP TTL:117 TOS:0x0 ID:3571
**S***** Seq: 0x3E33FFD   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:28.660521 OUTSIDE.NET.232.40:3928 - INSIDE.NET.133.4:1080 TCP TTL:117 TOS:0x0 ID:3827
**S***** Seq: 0x3E3406B   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:28.881097 OUTSIDE.NET.232.40:3929 - INSIDE.NET.133.5:1080 TCP TTL:117 TOS:0x0 ID:4339
**S***** Seq: 0x3E34146   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:29.015532 OUTSIDE.NET.232.40:3930 - INSIDE.NET.133.6:1080 TCP TTL:117 TOS:0x0 ID:4595
**S***** Seq: 0x3E341CB   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:29.334514 OUTSIDE.NET.232.40:3931 - INSIDE.NET.133.7:1080 TCP TTL:117 TOS:0x0 ID:5619
**S***** Seq: 0x3E34308   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:29.455072 OUTSIDE.NET.232.40:3932 - INSIDE.NET.133.8:1080 TCP TTL:117 TOS:0x0 ID:6643
**S***** Seq: 0x3E34376   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] WinGate-1080-Attempt [**]
01/08-05:02:29.555490 OUTSIDE.NET.232.40:3933 - INSIDE.NET.133.9:1080 TCP TTL:117 TOS:0x0 ID:6899
**S***** Seq: 0x3E343E9   Ack: 0x0   Win: 0x2800
TCP Options = MSS: 1460 NOP NOP SackOK
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1. Source of Trace.
   my network

2. Detect was generated by:
   Snort with the following rules:
   `alert TCP any any - any 1080 (msg:"WinGate-1080-Attempt"; flags: S; )`

3. Probability the source address was spoofed:
   Unlikely, the scanner wants to get responses indicating the presence of open WinGate ports.

4. Description of attack:
   These probes are very common, as many home and small-business users have vulnerable Socks or Wingates. An attacker is usually interested in this service because they can use it to bounce their connections through the server, and make other connections that will then seem to come from the victim IP address.

5. Attack mechanism:
   SOCKS is a system that allows multiple machines to share a common Internet connection. Many products support SOCKS. A typical product for home users is WinGate. WinGate is installed on a single machine that contains the actual Internet connection. All the other machines within the home connect to the Internet through the machine running WinGate. The problem with SOCKS and products like WinGate is that it isn't picky about the source and destination. Just as it allows internal machines access to the Internet, it possibly will allow Internet machines access the internal home network. Most importantly, it may allow a hacker access to other Internet machines through your system. This allows the hacker to hide his/her true location. The attacks against the victim appear to come from your machine, not from the real hacker. The ability to hide their tracks like this is important to hackers. Therefore, hackers scour the Internet religiously looking for systems they can bounce their attacks through. This intrusion signature indicates that somebody scanned your system looking for SOCKS, but probably did not find it. Confirm by watching for a corresponding socks-active signature.

6. Correlations:
   http://www.whitehats.com/info/IDS175

7. Evidence of active targeting:
   Yes, the attacker is attempting to scan an entire class C network.

8. Severity:

```
Criticality             = 3,  these are not critical servers
Lethality               = 1,  because there are no open 1080 ports on this subnet
System countermeasures  = 5,  all systems running latest patches, and port 1080 is disabled
Network countermeasures = 5,  the firewall blocks this traffic all traffic to port 1080

Severity = (Criticality + Lethality) - (System + Net Countermeasures)
         = (3+1) - (5+5)
         = -6
```

9. Defensive recommendation:
   Deny incoming port 1080 connections at your firewall.

10. Multiple choice test question:

    SOCKS give rise to security issues because:
    a) Just as it allows internal machines access to the Internet, it possibly will allow Internet machines access to the internal home network.
    b) It may allow a hacker access to other Internet machines through your system. This allows the hacker to hide his/her true location. The attacks against the victim appear to come from your machine, not from the real hacker.
    c) It is hard to block with most firewalls.
    d) (a) and (b)

    Answer: d

---

2) "ANALYZE THIS" SCENARIO

<> INTRODUCTION

We have been asked to provide you, GIAC Enterprises (an e-business that sells electronic fortune cookie sayings), with a basic analysis of some network-based intrusion detection data you provided us, as part of a bid to provide you with security services.

Before we begin our analysis, we would like to briefly mention our view of how intrusion detection fits into a comprehensive strategy for systems and networks security. Intrusion detection is only one component of that strategy. It also requires protective measures on systems and networks to slow the attackers down, and reactive protocols and methods to respond to attacks as they occur. The principle is that your protective methods (such as a minimal set of open ports on your systems) need to sufficiently slow attackers, so that your detection methods (such as Snort) and reactions to attacks (such as blocking an intruder at your firewall) are fast enough to stop an intruder, before they overcome your defenses. We will return to this idea at the end of the analysis, where we give some recommendations for improving your systems and networks security.

Here is an overview of the details which follow. First, a description of the 3 data file types is given. We follow with frequency distributions of the types of alerts and the types of scans that were found in your files. This tells us the types of attacks with which your systems are most frequently targeted. We also discuss the significance of each type of alert. In addition, we discuss the different types of scans and the significance of these scans. This is followed with frequency distributions of source IPs, destination IPs, and destination ports to show which hosts are the most active attackers, and which hosts and ports are the most frequently targeted. Finally, we conclude with a summary analysis and some recommendations for making your site more secure.

In performing our analysis we wrote a special purpose Perl script, called AnalyzeALL (described in the "Analysis Process" section), which can process all 3 data types, which we sometimes refer to in our analysis.

Our analysis shows that between Sep 27, 2000 and Nov 24, 2000, the time period for which we were provided data, traffic was reported in your 3 different types of Snort-related files from 2,625 unique source IPs, coming from 18,081 unique source ports, to 35,946 unique destination IPs and 16,647 unique destination ports. The total number of events recorded was 486,956. Two of the three

data file types (SnortS<#.txt and OOSche<#.txt) contained only data related to scans. The other data file type (SnortA<#.txt) contained data related to scans, but also data related to other types of events.

We have laid out our analysis in the following order:

- INTRODUCTION
- EXAMINATION OF THE RAW DATA FILES
- FREQUENCY DISTRIBUTION AND DESCRIPTION OF ALERT TYPES
- FREQUENCY DISTRIBUTION AND DESCRIPTION OF SCAN TYPES
- OBSERVATIONS ON ABNORMAL FLAG SCANS
- FREQUENCY DISTRIBUTIONS OF SOURCE IPs, DESTINATION IPs, AND DESTINATION PORTS
- SUMMARY ANALYSIS AND RECOMMENDATIONS

You may want to skip over the details to our SUMMARY ANALYSIS AND RECOMMENDATIONS section, and then return to the details.

<> EXAMINATION OF THE RAW DATA FILES

The process began with an examination of the data files. The data consisted of 113 unique files (3 pairs of files were duplicates even though the file names were different) containing a total of 844,363 lines of ascii text (54,479,653 bytes).

There were three types of files:

1) OOSche<#.txt files (example: OOSche6.txt), which we will refer to as LOG FILES, appeared to be standard Snort log files containing packet headers and some payload in Snort format. There were 17 such files, containing 377,682 lines and 16,974,318 bytes. Each such file contained a subject line, such as:

```
Subject: OOS check /usr/LOG/packets/Oct.1.2000.packets.de0.gz
```

Each file contained many records, where each record was multi-lined and was delimited by a line of alternating "+" and "=", such as:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-01:19:43.355584 203.32.161.197:21 - MY.NET.254.247:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x5AEBC36E   Ack: 0x3A70D29D   Win: 0x404
00 00 00 00 00 00                                   ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-01:19:43.395652 203.32.161.197:21 - MY.NET.254.249:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x5AEBC36E   Ack: 0x3A70D29D   Win: 0x404
00 00 00 00 00 00                                   ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-02:21:05.647359 24.20.202.103:8311 - MY.NET.206.54:1196
TCP TTL:45 TOS:0x0 ID:47542
21SF*P** Seq: 0xFA02C1   Ack: 0xCA530137   Win: 0x5010
TCP Options = EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-02:28:37.858491 24.20.202.103:8311 - MY.NET.206.54:1196
TCP TTL:45 TOS:0x0 ID:10003
21SF*P** Seq: 0x460371   Ack: 0xBA530137   Win: 0x5010
TCP Options = EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-11:19:14.085426 24.108.122.172:8311 - MY.NET.203.62:1348
TCP TTL:113 TOS:0x0 ID:8240  DF
2*SFR*** Seq: 0xFF0069   Ack: 0xC000000F   Win: 0x5010
20 77 05 44 00 FF 00 69 C0 00 00 0F 08 47 50 10   w.D...i.....GP.
21 C8 8B 49 00 00 89 6C B1 B5 3E D3 10 A1 E4 5B  !..I...l......[
66 9E                                            f.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

2) SnortA<#.txt files (example: SnortA10.txt), which we will refer to as ALERT FILES, appeared to be processed Snort alert files containing an alert message, timestamp, and source and destination, on one line. There were 54 such files, containing 151,963 lines and 15,550,184 bytes. Each such file contained a subject line, such as:

```
Subject: Snort Alert Report at Wed Oct 11 00:05:11 2000
```

Each file contained many records, where each record record was one line, such as:

```
10/10-09:51:01.696780  [**] WinGate 1080 Attempt [**] 204.117.70.5:2974 - MY.NET.212.214:1080
10/10-10:24:36.504626  [**] spp_portscan: PORTSCAN DETECTED from 216.123.62.32 (STEALTH) [**]
10/10-10:24:38.763443  [**] spp_portscan: portscan status from 216.123.62.32: 1 connections across 1 hosts: TCP(1), UDP(0) STEALTH [**]
10/10-10:24:41.758747  [**] spp_portscan: End of portscan from 216.123.62.32 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]
10/10-10:23:41.754369  [**] WinGate 1080 Attempt [**] 212.78.153.242:3992 - MY.NET.53.142:1080
10/10-10:58:33.278242  [**] WinGate 1080 Attempt [**] 193.252.63.9:60807 - MY.NET.222.102:1080
10/10-11:07:40.113289  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.16:6699 - MY.NET.214.46:1167
10/10-11:07:43.132251  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.16:6699 - MY.NET.214.46:1167
10/10-11:07:47.357771  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.16:6699 - MY.NET.214.46:1167
10/10-11:40:04.616744  [**] SMB Name Wildcard [**] MY.NET.101.160:137 - MY.NET.101.192:137
10/10-11:40:08.341002  [**] SNMP public access [**] MY.NET.97.159:1059 - MY.NET.101.192:161
10/10-11:40:11.137565  [**] SNMP public access [**] MY.NET.97.159:1062 - MY.NET.101.192:161
10/10-11:41:10.870134  [**] SNMP public access [**] MY.NET.97.159:1069 - MY.NET.101.192:161
```

3) SnortS<#.txt files (example: SnortS10.txt), which we will refer to as SCAN FILES, appeared to be files generated by the Snort portscan preprocessor. There were 42 such files, containing 314,718 lines and 21,955,151 bytes. Each such file contained a subject line, such as:

```
Subject: Snort Scan Report at Sun Oct  1 00:10:06 2000
```

Each file contained many records, where each record was one line, such as:

```
Sep 30 14:27:12 195.149.21.65:27025 - MY.NET.217.202:4877 UDP
Sep 30 14:27:12 195.149.21.65:27015 - MY.NET.217.202:4878 UDP
Sep 30 14:27:12 195.149.21.65:27045 - MY.NET.217.202:4875 UDP
Sep 30 14:29:59 24.22.255.16:6688 - MY.NET.202.222:1255 NOACK *1*FRP** RESERVEDBITS
Sep 30 14:30:49 207.218.236.252:37244 - MY.NET.203.178:8572 INVALIDACK ***FR*A*
Sep 30 14:32:15 24.22.255.16:141 - MY.NET.202.222:6688 SYNFIN 21SF**** RESERVEDBITS
Sep 30 15:29:11 24.7.211.58:6699 - MY.NET.221.62:1512 NOACK 2*S****U RESERVEDBITS
Sep 30 17:08:17 213.4.14.254:65068 - MY.NET.205.134:6699 XMAS 2**F*P*U RESERVEDBITS
Sep 30 17:36:42 194.239.155.193:55582 - MY.NET.202.206:4711 NULL ********
Sep 30 17:50:57 24.141.214.186:6688 - MY.NET.205.102:2172 INVALIDACK 2*SF*PA* RESERVEDBITS
Sep 30 18:21:14 24.201.72.26:1080 - MY.NET.219.214:6699 NULL ********
Sep 30 19:06:13 151.202.17.228:1735 - MY.NET.223.5:21 SYN **S*****
Sep 30 19:06:13 151.202.17.228:1747 - MY.NET.223.37:21 SYN **S*****
Sep 30 19:06:13 151.202.17.228:1754 - MY.NET.223.149:21 SYN **S*****
Sep 30 19:06:13 151.202.17.228:1775 - MY.NET.223.157:445 SYN **S*****
```

Though most filenames contained numbers (i.e SnortA42.txt, SnortS10.txt, OOSche25.txt), there seemed to be no relationship between that number and the data it contained. Each file did contain data relating to only one day and the entire data set spanned Sep 27, 2000 through Nov 24, 2000 with some holes.

<> FREQUENCY DISTRIBUTION AND DESCRIPTION OF ALERT TYPES

From the output of AnalyzeALL, we can extract a frequency distribution of all alert types reported. Table 1A shows this distribution. This provides with the type of attacks with which your systems are most frequently targeted.

Table 1A: Frequency of Alerts Reported in SnortA<#.txt files (in order of greatest frequency):

from ALERT Files:

total number alerts	fraction of all alerts	alert message
56250	0.48119	SYN-FIN scan!
30997	0.26517	Watchlist 000220 IL-ISDNNET-990517
8134	0.06958	Watchlist 000222 NET-NCFC
6440	0.05509	PORTSCAN DETECTED
4764	0.04075	WinGate 1080 Attempt
2893	0.02475	TCP SMTP Source Port traffic
2542	0.02175	Attempted Sun RPC high port access
1813	0.01551	Broadcast Ping to subnet 70
1697	0.01452	Back Orifice
468	0.00400	SNMP public access
277	0.00237	Null scan!
218	0.00186	SMB Name Wildcard
142	0.00121	Queso fingerprint
96	0.00082	NMAP TCP ping!
60	0.00051	SUNRPC highport access!
56	0.00048	connect to 515 from inside
15	0.00013	Probable NMAP fingerprint attempt
13	0.00011	External RPC call
7	0.00006	SITE EXEC - Possible wu-ftpd exploit - GIAC000623
7	0.00006	Tiny Fragments - Possible Hostile Activity
6	0.00005	site exec - Possible wu-ftpd exploit - GIAC000623
2	0.00002	Happy 99 Virus

We will examine a few of the most frequently occurring alerts.

From Table 1A we see that the most frequent alert (48.1% of all alerts) are from "SYN-FIN" scans. This alert indicates that a TCP probe was sent with the SYN and FIN flags set. This does not occur normally and indicates an intentional probe, likely as part of a single-packet OS detection. We then ran our special purpose Perl script, AnalyzeALL searching only for SYN-FIN scans. For the output see: Appendix 7: Output From Running Modified AnalyzeALL - Looking For SYN-FIN Scans.
The results indicate that over the approximately 2 month period 56 different source IPs using 41 different source ports were used to scan 27,440 different IPs and 28 different destination ports in the MY.NET network, using a "SYN-FIN" scan.

The second and third most frequent alerts were "Watchlist 000220 IL-ISDNNET-990517" (26.5%) and "Watchlist 000222 NET-NCFC" (7.0%). These both appear to be alerts which are generated by snort rules which watch for incoming traffic from "suspicious" networks, namely from subnets 212.79 and 159.226, respectively. Using Whois we find that the 212.79 network is probably from an ISDN provider from Israel and the 159.226 network is from the Computer Network Center Chinese Academy of Sciences (Appendix 9: Results of Whois 212.79 and Appendix 10: Results of Whois 159.226).
Again, we ran AnalyzeALL, this time to examine the activities of these two networks in detail.
See the following output from AnalyzeALL:
Appendix 4: Output From Running Modified AnalyzeALL - Looking For Source Net 159.226

Appendix 5: Output From Running Modified AnalyzeALL - Looking For Source Net 212.179
The results indicate that, from the 159.226 network, 45 different source IPs over 337 different ports had traffic going to 27 different IPs and 52 different ports on the MY.NET network, and from the 212.179 network, 63 different source IPs over 219 different ports had traffic going to 110 different IPs and 97 different port on the MY.NET network.

The forth most frequent alert was "PORTSCAN DETECTED". This alert was generated by the Snort Portscan Preprocessor and indicates a portscan is in progress. I did not count "portscan status" and "End of portscan" messages which indicate intermediate status and end of scan, respectively. Here is another, redundancy as some of these alerts are also counted by the "SYN-FIN" alert, "Null scan", "Queso fingerprint", and "NMAP TCP ping", in the Alert (SnortA<#.txt) files, as well as in the Scan files (SnortS<#.txt) files and the Log (OOSche<#.txt) files. This generic portscan alert was generated by 1486 unique source IPs.

The fifth most frequent alert was "Wingate 1080 Attempt". These probes are very common, as many home and small-business users have vulnerable socks or wingates. An attacker is usually interested in this service because they can use it to bounce their connections through the server, and make other connections that will then seem to come from the victim IP address. 570 different source IPs using 2861 different source ports were used to scan 2655 different IPs on port 1080 in the MY.NET network, using this probe.

Table 1B provides a description of each of the alerts from Table 1A, and includes a possible snort rule that might have generated the alert and, in some cases, web site references, where further information is available.

Table 1B: Descriptions of Alerts Reported in SnortA<#.txt files (in order of greatest frequency):

Alert Message: SYN-FIN scan!
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET any (msg:"IDS198 - SCAN-SYN FIN";flags:SF;)
Description: A TCP probe was sent with the SYN and FIN flags set. This does not occur normally and indicates an intentional probe, likely as part of a single-packet OS detection.
Reference: http://whitehats.com/info/IDS198

Alert Message: Watchlist 000220 IL-ISDNNET-990517
Possible Snort Rule: alert TCP 212.179.0.0/16 any - MY.NET.0.0/16 any (msg:"Watchlist 000220 IL-ISDNNET-990517";)
Description: Looking for attempted connections from Israel.

Alert Message: Watchlist 000222 NET-NCFC
Possible Snort Rule: alert TCP 159.226.0.0/16 any - MY.NET.0.0/16 any (msg:"Watchlist 000222 NET-NCFC";)
Description: Looking for attempted connections from China.

Alert Message: PORTSCAN DETECTED from . . .
Possible Snort Rule: from Portscan Preprocessor
Description: Indicates that a either 7 IP/port combinations were targeted within 2 seconds from one source or one IP/port was hit with a "stealth" scan packet (such as NULL, FIN, XMAS, SYNFIN, etc.).

Alert Message: WinGate 1080 Attempt
Possible Snort Rule: alert TCP any !53 - any 1080 (msg:"MISC-WinGate-1080-Attempt"; flags: S;)
Description: Someone is scanning your system to see if it is running SOCKS. This may be a hacker that desires to bounce traffic through your system at other systems. It may also be a chat server trying to determine if someone is indeed bouncing through your system to chat anonymously.
Reference: http://whitehats.com/info/IDS175

Alert Message: TCP SMTP Source Port traffic
Possible Snort Rule: alert TCP any 25 - any any (msg:"TCP SMTP Source Port traffic";)
Description: This alert indicates an unsuccessful attempt to use an internal mail server for relaying mail to a third party.
Reference: http://whitehats.com/info/IDS249
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0512

Alert Message: Attempted Sun RPC high port access
Possible Snort Rule: alert TCP any any - any 32771 (msg:"MISC-Attempted Sun RPC high port access";)
Description: Attemped exploit of the rpc.ttdbservd process. Success could allow execution of arbitrary commands.
Reference: http://whitehats.com/info/IDS241
http://whitehats.com/info/IDS242
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0003

Alert Message: Broadcast Ping to subnet 70
Possible Snort Rule: alert ICMP any any - MY.NET.70.255 any (msg:"Broadcast Ping to subnet 70";)
Description: Attempting to get subnet MY.NET.70 to respond to a number of (probably spoofed) IP addresses, thus employing that subnet for a denial of service attack.

Alert Message: Back Orifice
Possible Snort Rule: alert udp any any - any 31337 (msg:"Back Orifice";)
Description: A remote attacker is sending a probe to see if the Back Orifice trojan is running on the server.
Reference: http://whitehats.com/info/IDS188
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0660

Alert Message: SNMP public access
Possible Snort Rule: alert udp any any - any 161 (msg:"SNMP public access";)
Description: This alert may indicate an SNMP probe was attempted to determine a list of NT usernames from the server.
Reference: http://whitehats.com/info/IDS333
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0499

Alert Message: Null scan!
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET any (msg:"IDS04 - SCAN-NULL Scan";flags:0; seq:0; ack:0;)
Description: A TCP frame has been sent with a sequence number of zero and all control bits are set to zero. This frame should never be seen in normal operation. An attacker may be scanning your system to see what services are available.

Reference: http://whitehats.com/info/IDS4

Alert Message: SMB Name Wildcard
Possible Snort Rule: alert udp any 137 - any 137 (msg:"SMB Name Wildcard";)
Description: This is a standard netbios name table retrieval query. An attacker could use this to extract useful information such as workstation name, domain, and users currently logged in.
Reference: http://whitehats.com/info/IDS177
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0621

Alert Message: Queso fingerprint
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET any (msg:"IDS29 - SCAN-Possible Queso Fingerprint attempt";flags:S12;)
Description: A remote user has used the Queso tool to determine the OS fingerprint of the server.
Reference: http://whitehats.com/info/IDS29
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0454

Alert Message: NMAP TCP ping!
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET any (msg:"IDS28 - PING NMAP TCP";flags:A;ack:0;)
Description: A remote user has used the NMAP portscanning tool to probe the server.
Reference: http://whitehats.com/info/IDS28
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0523

Alert Message: SUNRPC highport access!
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET 32771 (msg:"SUNRPC highport access!";)
Description: Attemped exploit of the rpc.ttdbservd process. Success could allow execution of arbitrary commands.
Reference: http://whitehats.com/info/IDS241
http://whitehats.com/info/IDS242
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0003

Alert Message: connect to 515 from inside
Possible Snort Rule: alert tcp $HOME_NET any - $HOME_NET 515 (msg:"connect to 515 from inside";)
Description: Attempt to connect to printer spooler port from inside.

Alert Message: Probable NMAP fingerprint attempt
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET any (msg:"IDS05 - SCAN-Possible NMAP Fingerprint attempt";flags:SFPU;)
Description: Attempted to determine the server OS using the nmap tool.
Reference: http://whitehats.com/info/IDS5
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0454

Alert Message: External RPC call
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET 111 (msg:"External RPC call";)
Description: A query was sent to the portmap daemon.
Reference: http://whitehats.com/info/IDS428
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0632

Alert Message: SITE EXEC - Possible wu-ftpd exploit - GIAC000623
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET 21 (msg:"Possible wu-ftpd exploit";)
Description: A portion of the remote ftpd attack against wu-2.6.0.
Reference: http://whitehats.com/info/IDS286
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0574

Alert Message: Tiny Fragments - Possible Hostile Activity
Possible Snort Rule: preprocessor minfrag: 128
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET 21 (msg:"Possible wu-ftpd exploit";)
Description: Indicates presence of fragmented IP packets. Such fragments can pass through a stateless firewall and can contain malicious intent.

Alert Message: site exec - Possible wu-ftpd exploit - GIAC000623
Possible Snort Rule: alert tcp !$HOME_NET any - $HOME_NET 21 (msg:"Possible wu-ftpd exploit";)
Description: A portion of the remote ftpd attack against wu-2.6.0.
Reference: http://whitehats.com/info/IDS286
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0574

Alert Message: Happy 99 Virus
Possible Snort Rule: alert tcp $HOME_NET any - any 25 (msg:"MCAFEE ID 10144 - Virus - Possible Outgoing Happy99 Virus"; content:"X-Spanska\:Yes

---

<> FREQUENCY DISTRIBUTION AND DESCRIPTION OF SCAN TYPES

From the output of AnalyzeALL, we can extract a frequency distribution of all scan types reported. Table 2 shows a truncated distribution showing the 20 most frequent scan types. As we said before, with the alerts, this provides with the type of attacks (in this case, scans) with which your systems are most frequently targeted.

Table 2: Frequency of Top 20 Scans Reported in SnortS<#.txt files

from SCAN Files:

total number scans	fraction of all scans	scan message
235361	0.75806	SYN **S*****

```
 50523  0.16273   SYNFIN **SF****
 21585  0.06952   UDP
   454  0.00146   FIN ***F****
   351  0.00113   VECNA *****P**
   281  0.00091   INVALIDACK **S*R*A*
   221  0.00071   NULL ********
   104  0.00033   SYN 21S***** RESERVEDBITS
    57  0.00018   INVALIDACK ***FR*A*
    29  0.00009   NOACK *1SF*P** RESERVEDBITS
    28  0.00009   FULLXMAS 21SFRPAU RESERVEDBITS
    16  0.00005   SYNFIN 21SF**** RESERVEDBITS
    15  0.00005   FIN *1*F**** RESERVEDBITS
    14  0.00005   UNKNOWN 2*S***A* RESERVEDBITS
    14  0.00005   NOACK *1**RP** RESERVEDBITS
    14  0.00005   NOACK *1SFRP** RESERVEDBITS
    13  0.00004   NOACK *1S**P** RESERVEDBITS
    13  0.00004   NOACK **S**P**
    13  0.00004   NOACK *1*FRP** RESERVEDBITS
    13  0.00004   NOACK **SF***U
```

The vast majority of scans (235361 - 76%) had only the SYN flag set. This type of flag configuration occurs normally in the first packet at the beginning of a normal TCP connection. The third most frequent scan type was a UDP scan (21585 - 7%). These 2 scan types generate packets that are "normal". What causes Snort to record these as a scans is that it counts too many such packets over too small a time interval from the same host. It appears from the ALERTS files that the threshold of the Snort portscan preprocessor was set at 7 connections in 2 seconds. Like many scans, SYN-only and UDP scans can be used for reconnaisance to determine host/port vulnerabilities, and to actually connect to open ports (where trojans or vulnerable services might exist).

The second most frequent scan type was a SYN-FIN scan (50523 - 16%). The SYN-FIN scans as well as the other 0.9% remaining scans involve "abnormal" TCP packets ("abnormal" because their flag configurations do not occur with normal traffic). Abnormal flag combinations occur in crafted packets, which are frequently used to determine operating system types and to sneak through poorly designed firewalls where a normal packet (like a SYN-only) would be detected. For this reason, such scans are sometimes referred to as "stealth" scans. The Snort portscan preprocessor only requires one such packet to record this as a scan.

SYN-only scan alerts can also be indicative of SYN-flood denial of service attacks. To test for such an attack, I ran a modified AnalyzeALL looking for SYN-only scans in only the SCAN files. I examined the 3 most frequent destination IPs. Indeed all 3 of these IPs appeared to have been under SYN-flood denial of service attacks. Here is some sample data from the 3 SYN-floods:

1) The following data indicates that on Nov 4, starting at 03:53:09 and lasting until 04:02:46 (less than 10 minutes) a total of 11,904 SYN packets were sent from 194.244.78.145 to MY.NET.220.2. A sample of the data follows:

```
Nov  4 03:53:09 194.244.78.145:14066 - MY.NET.220.2:1 SYN **S*****
Nov  4 03:53:06 194.244.78.145:14073 - MY.NET.220.2:8 SYN **S*****
Nov  4 03:53:07 194.244.78.145:14105 - MY.NET.220.2:40 SYN **S*****
 .
 .
 .
Nov  4 04:02:46 194.244.78.145:36293 - MY.NET.220.2:22214 SYN **S*****
Nov  4 04:02:46 194.244.78.145:36277 - MY.NET.220.2:22198 SYN **S*****
Nov  4 04:02:46 194.244.78.145:36285 - MY.NET.220.2:22206 SYN **S*****
```

2) The following data indicates that on Nov 17, starting at 05:59:57 and lasting until 06:01:44 (less than 2 minutes) a total of 1,751 SYN-only packets were sent from 24.23.51.218 to MY.NET.162.77. A sample of the data follows:

```
Nov 17 05:59:57 24.23.51.218:64524 - MY.NET.162.77:6 SYN **S*****
Nov 17 05:59:57 24.23.51.218:64524 - MY.NET.162.77:7 SYN **S*****
Nov 17 05:59:57 24.23.51.218:64524 - MY.NET.162.77:9 SYN **S*****
 .
 .
 .
Nov 17 06:01:44 24.23.51.218:64524 - MY.NET.162.77:7969 SYN **S*****
Nov 17 06:01:44 24.23.51.218:64524 - MY.NET.162.77:7970 SYN **S*****
Nov 17 06:01:44 24.23.51.218:64524 - MY.NET.162.77:8000 SYN **S*****
```

3) The following data indicates that on Nov 17, starting at 16:58:31 and lasting until 17:01:01 (less than 3 minutes) a total of 224 SYN-only packets were sent from 209.102.105.64 to MY.NET.60.16. A sample of the data follows:

```
Nov 17 16:58:31 209.102.105.64:20526 - MY.NET.60.16:23285 SYN **S*****
Nov 17 16:58:32 209.102.105.64:20539 - MY.NET.60.16:23290 SYN **S*****
Nov 17 16:58:32 209.102.105.64:20540 - MY.NET.60.16:23291 SYN **S*****
 .
 .
 .
Nov 17 17:01:00 209.102.105.64:20600 - MY.NET.60.16:24800 SYN **S*****
Nov 17 17:01:01 209.102.105.64:20617 - MY.NET.60.16:24809 SYN **S*****
Nov 17 17:01:01 209.102.105.64:20761 - MY.NET.60.16:24816 SYN **S*****
```

The remaining 24% of the scans all involved abnormal flags being set (such as SYN and FIN together), and were probably attempts to probe for OS types.

<> OBSERVATIONS ON "ABNORMAL FLAG" SCANS

On examining the LOG (OOSche<#.txt) files, we found that all of this data appeared to be crafted packets that were part of "abnormal flag" TCP scans. Certain TCP flag configuration, such as SYN and FIN together, never occur in normal traffic. This type of packet is used solely for scanning. The unusual flags allow these packets to pass through some poorly designed firewalls (where a normal SYN-only packet

might be blocked) and also are used to identify the operating systems of the scanned hosts based on their responses. Since all of the packets in these files contained these type of "crafted" packets, it is reasonable to assume that the source IPs in all of these packets represent systems that are up to no good. The source IPs from outside your site should all be blocked. Also, unless someone from your systems/security team is scanning for valid protective reasons, the source IPs from inside your network are also up to no good, and probably represent compromised systems which are being used to scan systems outside your site. These systems should all be taken off line and further analysis performed. Here are some samples of crafted packets coming from MY.NET systems:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-01:58:39.857584 MY.NET.220.142:1 - 208.39.14.157:1842
TCP TTL:126 TOS:0x0 ID:6468  DF
**SF**** Seq: 0x500051   Ack: 0x376E15A9   Win: 0x5010
00 01 07 32 00 50 00 51 37 6E 15 A9 04 03 50 10  ...2.P.Q7n....P.
22 38 F7 06 20 20 20 20 20 00                    "8..      .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-02:10:31.993445 MY.NET.220.142:1079 - 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:33768  DF
2*SFR*A* Seq: 0x8EEED   Ack: 0x4161   Win: 0x5010
00 08 EE ED 00 00 41 61 13 57 50 10 22 38 13 82  ......Aa.WP."8..
20 20 20 20 20 00                                     .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-08:35:35.582649 MY.NET.203.198:1870 - 205.188.3.194:5190
TCP TTL:126 TOS:0x0 ID:59444  DF
21SF**AU Seq: 0x13F9   Ack: 0x9CF83C54   Win: 0x5011
TCP Options = Opt 32 (32): 2020 2000 E43D 16FF 4313 0103 0000 0000 0000 0000 0000 0000 0000 0000 0000
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-11:10:24.607489 MY.NET.203.150:8311 - 128.205.218.221:2158
TCP TTL:126 TOS:0x0 ID:45969  DF
*1SF**AU Seq: 0x4202325   Ack: 0x5B430FB   Win: 0x5010
20 77 08 6E 04 20 23 25 05 B4 30 FB 00 B3 50 10   w.n. #%..0...P.
22 38 5D 2C 20 20 20 20 20 00                    "8],      .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-11:10:53.806235 MY.NET.203.150:1851 - 206.167.181.162:6688
TCP TTL:126 TOS:0x0 ID:33949  DF
21SF*PAU Seq: 0x425F353   Ack: 0x7858127   Win: 0x8010
07 3B 1A 20 04 25 F3 53 07 85 81 27 00 FB 80 10  .;. .%.S...'....
1D A0 B4 C1 00 00 01 01 05 0A 07 85 8B 73 07 85  ............s..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-11:41:48.898267 MY.NET.203.150:179 - 134.126.193.61:1841
TCP TTL:126 TOS:0x0 ID:34368  DF
*1SF*P** Seq: 0x2077041B   Ack: 0xF95201DC   Win: 0x5010
20 20 20 20 20 00                                     .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-11:44:22.432712 MY.NET.203.150:1841 - 134.126.193.61:8311
TCP TTL:126 TOS:0x0 ID:53575  DF
*1SFRPA* Seq: 0x41B   Ack: 0xF95201F7   Win: 0x8010
00 00 01 01 05 0A 01 F7 65 53 01 F7              ........eS..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-13:06:14.670875 MY.NET.227.150:1842 - 64.12.15.17:5190
TCP TTL:126 TOS:0x0 ID:34593  DF
*1SF*PAU Seq: 0x5B0   Ack: 0x30E87D07   Win: 0x5010
30 BB 50 10 22 26 D8 D2 20 20 20 20 20 00        0.P."&..      .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-13:07:44.901506 MY.NET.227.150:1842 - 64.12.15.17:5190
TCP TTL:126 TOS:0x0 ID:54581  DF
2*SF**AU Seq: 0x5B0   Ack: 0x81CC7D7C   Win: 0x5010
22 26 72 C1 20 20 20 20 20 00                    "&r.      .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/04-15:20:01.788474 MY.NET.213.138:0 - 147.188.152.131:1516
TCP TTL:126 TOS:0x0 ID:26684  DF
*1SFRPAU Seq: 0x1A200435   Ack: 0x5E2500D6   Win: 0x5010
20 00                                            .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

In all the OOSche<#.txt files together, there were 59,582 packets, all of which had both the SYN and FIN flags set. 59,080 (99.1 %) of these packets had only the SYN and FIN flags set (SYN-FIN scans, as described earlier). It is of interest to note that of all these SYN-FIN packets, all but 8 had the same datagram ID number (ID:39426). The identification field uniquely identifies each datagram sent by a host. It normally increments by one each time a datagram is sent. The only time two packets would normally have the same ID number if they were part of the same fragmented IP datagram, in which case they would come from one unique IP address and have a destination of one unique IP address. The identical ID number serves to underscore the fact that we are dealing with "crafted" packets. The remaining 369 (0.6 %) packets included other flags as well as SYN and FIN and also different packet ID numbers. These also are crafted packets. Here is a sample of the crafted packets with the same ID numbers:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:09.671627 203.32.161.197:21 - MY.NET.1.102:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x2A0B0777   Ack: 0x2D213622   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:09.738783 203.32.161.197:21 - MY.NET.1.105:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x2A0B0777   Ack: 0x2D213622   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-00:58:09.755989 203.32.161.197:21 - MY.NET.1.106:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x2A0B0777   Ack: 0x2D213622   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
.
.
.
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/14-05:53:55.149839 MY.NET.218.106:1086 - 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:26460  DF
21SF**A* Seq: 0x460018   Ack: 0xF9D43F58   Win: 0x5010
TCP Options = Opt 32 (32): 2020 2000 8C09 A64A 82BB 0014 0000 0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL EOL EOL
EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/14-05:54:01.309640 MY.NET.218.106:1086 - 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:45920  DF
2*SF**** Seq: 0x18FA4B   Ack: 0xA3F7B   Win: 0x5010
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/14-06:01:57.768582 MY.NET.218.106:70 - 207.172.3.46:1086
TCP TTL:126 TOS:0x0 ID:15260  DF
**SF*PAU Seq: 0x770019   Ack: 0x1DB0496B   Win: 0x5010
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/14-06:09:30.853175 MY.NET.218.106:1090 - 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:30373  DF
*1SFRP*U Seq: 0x29   Ack: 0x40CD596E   Win: 0x5010
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

<> FREQUENCY DISTRIBUTIONS OF SOURCE IPs, DESTINATION IPs, AND DESTINATION PORTS

SOURCE IPs

From the output of AnalyzeALL, we can extract frequency distributions for all source IPs, all MY.NET source IPs, all MY.NET source IPs generating crafted packets, all destination IPs, and all destination ports. Tables 3A, 3B, 3C, 3D, and 3E show truncated results (top 20) for these, respectively.

By performing a frequency analysis of source IPs, we can obtain a list of what possibly may be the most active attackers of your site. Similarly, by performing frequency analyses of both destination IPs and destination ports, we can can obtain lists of potentially the most active targets of your site. We have limited our lists to the top 20 of each distribution, for ease of illustration.

Table 3A: Top 20 Most Active Source IPs

SOURCE IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL	SOURCE NAME
208.61.4.207	21725	0.04461	6660	6634	8431	adsl-61-4-207.mia.bellsouth.net
66.9.27.254	20649	0.04240	0	20649	0	
209.92.40.32	15699	0.03224	4993	4956	5750	dslcv1-32.fast.net
160.78.49.191	14418	0.02961	7226	7192	0	ema.chim.unipr.it
130.89.229.48	13297	0.02731	3886	3860	5551	cal032044.student.utwente.nl
62.252.21.241	13290	0.02729	233	13057	0	pc241-gui4.cable.ntl.com
194.244.78.145	11906	0.02445	2	11904	0	
63.88.175.201	11753	0.02414	35	11718	0	www.multilateral.com
203.32.161.197	11644	0.02391	3571	3562	4511	adnet.imgserv.com
210.113.89.200	11388	0.02339	3598	3566	4224	
193.64.114.10	10934	0.02245	3321	3321	4292	net10.printeq.fi
195.103.69.159	10581	0.02173	3319	3294	3968	
62.157.23.237	9664	0.01985	23	9641	0	p3E9D17ED.dip.t-dialin.net
63.248.55.245	9083	0.01865	10	9073	0	3ff837f5.dsl.flashcom.net
62.96.169.86	9062	0.01861	123	8939	0	m-dialin-86.addcom.de
24.23.151.112	8795	0.01806	32	8763	0	cx673530-a.vbch1.va.home.com
63.195.56.20	8670	0.01780	3921	0	4749	adsl-63-195-56-20.dsl.snfc21.pacbell.net
64.50.161.162	8653	0.01777	18	8635	0	public.washingtonhomes.com
210.101.101.110	8442	0.01734	2610	2578	3254	
212.0.107.107	7807	0.01603	2364	2340	3103	

We can further explore the details of these most active source IPs, by running AnalyzeALL on each IP individually. Some results from the top 10 most active are shown here:

```
1) 208.61.4.207  -  21725 events; all SYN-FIN scans to 8431 destination IPs
                    from source port 9704 to destination  port 9704
2) 66.9.27.254   -  20649 events; all SYN-only scans to 19322 destination IPs
                    from 3958 source ports to destination port 515
3) 209.92.40.32  -  15699 events; all SYN-FIN scans to 5750 destination IPs
                    from source port 9704 to destination  port 9704
4) 160.78.49.191 -  14418 events; almost all SYN-FIN scans to 7206 destination IPs
                    from 11 source ports to destination  port 53
5) 130.89.229.48 -  13297 events; all SYN-FIN scans to 5551 destination IPs
```

from source port 53 to destination port 53
6) 62.252.21.241 - 13290 events; all SYN-only scans to 8267 destination IPs
from 3748 source ports to destination port 21
7) 194.244.78.145 - 11906 events; all SYN-only scans to one destination IP, MY.NET.220.2,
from 10441 source ports to 10441 destination ports
8) 63.88.175.201 - 11753 events; almost all SYN-only scans to 10647 destination IPs
from 3769 source ports to destination port 21
9) 203.32.161.197 - 11644 events; almost all SYN-only scans to 4525 destination IPs
from 18 source ports to destination port 21
10) 212.179.15.122 - 564 events; all "Israel" events to one destination IP, MY.NET.227.190,
from source port 2100 to destination port 6699

From this limited picture of the top 10 most active source IPs, it is most likely that they are all up to no good and should be blocked from your site. If we had looked further down this list, I am sure we would find other bad guys, but again this is for illustration purposes. Also, simply because an IP appears at the top of such a frequency distribution that it is a bad guy, only that it is highly suspicious and should be examined further.

We also ran AnalyzeALL restricting our attention to only source IPs from the MY.NET network. The idea here is that there is a good chance that some of the more active IPs represent compromised systems that are being used to attack other systems. Doing this we found 11284 total events with 112 source IPs from 3182 source ports going to 6181 destination IPs and 1902 destination ports. The top 30 most active source IPs from MY.NET are shown in Table 3B. The most used source ports were 67 (bootps), 123 (ntp), 53 (DNS), and 137 (NETBIOS name service). The most used destination ports were 139 (NETBIOS session service), 67 (bootps), 161 (snmp), 119 (nntp), and 137 (NETBIOS name service).

Table 3B: Top 20 Most Active Source IPs from the MY.NET network

SOURCE IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL	SOURCE NAME
MY.NET.224.150	2981	0.26418	0	2981	0	
MY.NET.221.82	2680	0.23750	12	2668	0	
MY.NET.5.25	2313	0.20498	2	2311	0	
MY.NET.1.3	627	0.05557	50	577	0	
MY.NET.110.111	271	0.02402	1	270	0	
MY.NET.110.16	268	0.02375	1	267	0	
MY.NET.109.41	253	0.02242	1	252	0	
MY.NET.110.105	216	0.01914	1	215	0	
MY.NET.110.108	161	0.01427	1	160	0	
MY.NET.110.109	121	0.01072	1	120	0	
MY.NET.109.40	110	0.00975	1	109	0	
MY.NET.110.110	101	0.00895	1	100	0	
MY.NET.109.38	94	0.00833	1	93	0	
MY.NET.213.58	94	0.00833	0	94	0	
MY.NET.101.160	93	0.00824	93	0	0	
MY.NET.218.106	92	0.00815	0	0	92	
MY.NET.98.106	58	0.00514	58	0	0	
MY.NET.101.142	54	0.00479	54	0	0	
MY.NET.98.174	49	0.00434	49	0	0	
MY.NET.97.185	44	0.00390	44	0	0	

As we did before, We can further explore the details of these most active MY.NET source IPs, by running AnalyzeALL on each IP individually. Some results from the top 10 most active are shown here:

1) MY.NET.224.150 - 2981 events; all SYN-only scans to 2981 destination IPs
from 2100 source ports to destination port 139
2) MY.NET.221.82 - 2680 events; all SYN-only scans to 2668 destination IPs
from 1980 source ports to destination port 139
3) MY.NET.5.25 - 2313 events; all UDP scans to 559 destination IPs
from source port 67 to destination ports 67 or 68
4) MY.NET.1.3 - 627 events; all UDP scans to 4 destination IPs
from source port 53 to 576 destination ports
5) MY.NET.110.111 - 271 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 270 destination ports
6) MY.NET.110.16 - 268 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 267 destination ports
7) MY.NET.109.41 - 253 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 252 destination ports
8) MY.NET.110.105 - 216 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 215 destination ports
9) MY.NET.110.108 - 161 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 160 destination ports
10) MY.NET.110.109 - 121 events; all UDP scans to 1 destination IP, MY.NET.120.36,
from source port 123 to 120 destination ports

Unfortunately this analysis of the MY.NET source IPs has not produced any obvious compromised systems. Almost all activity were to destination IPs in the MY.NET network. Also, The source ports mostly used, 67 (bootps), 123 (ntp), 53 (DNS), and 137 (NETBIOS name service), and the destination ports mostly used, 139 (NETBIOS session service), 67 (bootps), 161 (snmp), 119 (nntp), and 137 (NETBIOS name service). These indications alone, does not indicate anything clearly abnormal at your site.

However, if we run AnalyzeALL again, but this time restricting our attention to only the "crafted" packet (OOSche<#.txt) files and source IPs in the MY.NET network, we will obtain a list of systems at your site

that are definitely involved in scanning other hosts. The results from running AnalyzeALL show us that 299 events were recorded where crafted packets traveled from 51 different source IPs on the MY.NET network to 79 different destination IPs (all outside your site), and 81 different destination ports. See Appendix 8: Output From Running Modified AnalyzeALL - Looking For Crafted Packets From MY.NET.

Table 3C: Top 20 Most Active Source IPs From the MY.NET Network Generating "Crafted" Packets

SOURCE IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.218.106	92	0.30769	0	0	92
MY.NET.217.194	33	0.11037	0	0	33
MY.NET.224.2	32	0.10702	0	0	32
MY.NET.220.142	24	0.08027	0	0	24
MY.NET.219.2	16	0.05351	0	0	16
MY.NET.203.150	14	0.04682	0	0	14
MY.NET.203.198	8	0.02676	0	0	8
MY.NET.211.130	7	0.02341	0	0	7
MY.NET.213.138	6	0.02007	0	0	6
MY.NET.201.14	5	0.01672	0	0	5
MY.NET.209.110	5	0.01672	0	0	5
MY.NET.208.82	4	0.01338	0	0	4
MY.NET.181.131	4	0.01338	0	0	4
MY.NET.214.142	3	0.01003	0	0	3
MY.NET.202.66	3	0.01003	0	0	3
MY.NET.217.222	3	0.01003	0	0	3
MY.NET.227.186	2	0.00669	0	0	2
MY.NET.219.18	2	0.00669	0	0	2
MY.NET.227.150	2	0.00669	0	0	2
MY.NET.218.182	2	0.00669	0	0	2

All of these IPs from your site are guilty of sending out crafted packets to hosts outside your site. They should all be considered compromised and investigated further to determine if there were valid reasons for this traffic (such as systems/security administrators running appropriate scans).

DESTINATION IPs

From the output of AnalyzeALL, we can extract frequency distributions for destination IPs and destination ports. This data can point us in the direction of the most active targets at your site. Table 3D shows truncated results (top 20) for the most active destination IPs.

Table 3D: Top 20 Most Active Destination IPs

DEST IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.220.2	11932	0.02450	6	11926	0
MY.NET.6.7	5816	0.01194	5800	14	2
MY.NET.211.146	4876	0.01001	4814	51	11
MY.NET.223.98	3953	0.00812	3940	12	1
MY.NET.206.90	3934	0.00808	3918	13	3
MY.NET.218.50	2372	0.00487	9	2359	4
MY.NET.253.114	1987	0.00408	9	1976	2
MY.NET.70.255	1814	0.00373	1813	0	1
MY.NET.206.94	1806	0.00371	4	1799	3
MY.NET.162.77	1763	0.00362	3	1759	1
MY.NET.203.142	1661	0.00341	1640	18	3
MY.NET.205.214	1595	0.00328	3	1589	3
MY.NET.120.36	1591	0.00327	0	1591	0
MY.NET.218.142	1480	0.00304	1463	13	4
MY.NET.214.170	1387	0.00285	1371	14	2
MY.NET.215.210	1373	0.00282	3	1367	3
MY.NET.60.16	1348	0.00277	41	1306	1
MY.NET.100.230	1304	0.00268	1289	15	0
MY.NET.140.57	1222	0.00251	1	1220	1

MY.NET.70.121	1220	0.00251	9	1206	5

Running AnalyzeALL individually on the 10 most active destination IPs we get:

1) MY.NET.220.2 - 11932 events; almost all, 99.9%, were SYN-only scans from 19 source IPs, but mostly (99.8%) from 194.244.78.145, from 10459 source ports to 10454 destination ports
2) MY.NET.6.7 - 5816 events; almost all, 99.6%, were "Watchlist 000222 NET-NCFC" alerts from 25 source IPs, and 99.0% from 159.226.45.3, from 111 source ports to 17 destination ports
3) MY.NET.211.146 - 4876 events; almost all activities, 98.9%, were "Watchlist 000220 IL-ISDNNET-990517" alerts from 18 source IPs, and 98.6% from 212.179.95.5, from 38 source ports to 15 destination ports, 99.3% to port 4922
4) MY.NET.223.98 - 3953 events; almost all activities, 99.7%, were "Watchlist 000220 IL-ISDNNET-990517" alerts from 12 source IPs, from 13 source ports to 7 destination ports, and 99.6% to port 3953
5) MY.NET.206.90 - 3934 events; almost all activities, 99.6%, were "Watchlist 000220 IL-ISDNNET-990517" alerts from 13 source IPs, from 17 source ports to 6 destination ports, and 99.6% to port 3934
6) MY.NET.218.50 - 2372 events; almost all activities, 99%, were UDP scans from 13 source IPs, and 99.2% from 24.9.152.152, from 13 source ports to 1252 destination ports
7) MY.NET.253.114 - 1987 events; almost all activities equally split between SYN-only and UDP scans from 16 source IPs, from 908 source ports to 1157 destination ports
8) MY.NET.253.114 - 1987 events; almost all activities equally split between SYN-only and UDP scans from 16 source IPs, from 908 source ports to 1157 destination ports
9) MY.NET.206.94 - 1806 events; almost all activities were UDP scans from 17 source IPs, from 15 source ports to 63 destination ports
10) MY.NET.162.77 - 1763 events; almost all were SYN-only scans from 13 source IPs, 99.3% from 24.23.51.218, from 9 source ports to 1754 destination ports

This data shows the most actively targeted system at your site.

DESTINATION PORTS

From the output of AnalyzeALL, we can extract frequency distributions for destination ports. This information give us a good indication of what type of trojans and service vulnerabilities your attackers are looking for. Table 3E shows truncated results (top 30) for these.

Table 3E: Top 20 Most Active Destination Ports And Known Trojan Use

DEST PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL	KNOWN USES
21	159399	0.32734	19639	117678	22082	FTP control, back construction, blade runner, doly trojan, fore, ftp t
53	52646	0.10811	18341	19513	14792	dns
9704	45787	0.09403	14184	14168	17435	
27374	44015	0.09039	3577	36214	4224	subseven21
515	25853	0.05309	56	25797	0	
25	11122	0.02284	11034	88	0	SMTP, ajan, antigen, email password sender, promail trojan, terminator
6699	10124	0.02079	9762	318	44	
98	9467	0.01944	0	9467	0	
9088	8763	0.01800	0	8763	0	
110	8728	0.01792	43	8685	0	POP3, promail trojan
1080	6669	0.01370	4774	1895	0	SOCKS
4619	5738	0.01178	5734	4	0	
139	5648	0.01160	0	5648	0	NETBIOS session service
4922	4845	0.00995	4813	26	6	
113	4353	0.00894	109	4244	0	AUTHENTICATION service, kazimas
23	3574	0.00734	343	3044	187	TELNET, tiny telnet server
6688	3513	0.00721	3293	190	30	
31337	2914	0.00598	1697	1217	0	back orifice and others
32771	2607	0.00535	2602	5	0	SUN-RPC
67	2295	0.00471	0	2295	0	BOOTPS

<> SUMMARY ANALYSIS AND RECOMMENDATIONS

Our approach was to perform a frequency analysis of your data, keying on various parameters, such as alert types, scan types, source IP, destination IP, or destination port. We then focused our attention on the alerts, scans, IPs and ports that occurred most frequently.

As we have already stated, our analysis shows that between Sep 27, 2000 and Nov 24, 2000, traffic was reported from your 3 different types of Snort-related files, from 2,625 unique source IPs, coming from 18,081 unique source ports, going to 35,946 unique destination IPs and 16,647 unique destination ports. Two of the three data file types (SnortS<#.txt and OOSche<#.txt) contained only data related to scans. The other data file type (SnortA<#.txt) contained data related to scans, but also data related to other types of events.

Your site is constantly being scanned. The data reveals that the majority of all attacks against your systems are scans. In fact of all the 486,956 events provided us from your data, 433,264 (89%) of the events were various types of scans (SYN-only, SYN-FIN, UDP, Null, Queso Fingerprint, NMAP TCP Ping, and other "abnormal TCP flag" scans). Roughly 99% of all your scans fall into 3 types: SYN-only (75.8%), SYN-FIN (16.3%), and UDP (7.0%). The SYN-FIN scans as well as the other 0.9% remaining scans involve TCP packets with abnormal flag combinations.

Scanning is often the first step, or reconnaisance phase, to compromising a site. All types of scans can be used to determine what hosts are active and which service ports (where vulnerable services or trojans might reside) are open. In addition, "abnormal TCP flag" scans can be used to determine the operating system types of scanned hosts and can some times pass through poorly designed firewalls, where SYN-only scans might be blocked. The information collected by scanning helps an intruder determine where vulnerabilities might exist to determine what method of attack might best be used to compromise your site. Events registered as SYN-only scans, can also be indicative of SYN-flood denial of service attacks, which we have seen in your data.

We have shown that a number of your own hosts are sending crafted packets to hosts outside your network. You should consider all of these hosts compromised and taken off line until you can determine the cause of their suspicious activities. The top 10 offenders include:
MY.NET.218.106 MY.NET.217.194 MY.NET.224.2 MY.NET.220.142 MY.NET.219.2,
MY.NET.203.150 MY.NET.203.198 MY.NET.211.130 MY.NET.213.138 MY.NET.201.14.

We have shown that the top 20 destination ports from your alerts, in order of greatest activity, are: 21 (FTP control, possible trojans: back construction, blade runner, doly trojan, fore, ftp trojan, and others), 53 (DNS), 9704, 27374 (possible subseven21 trojan), 515, 25 (SMTP), 6699, 98, 9088, 110 (POP3), 1080 (SOCKS), 4619, 139 (NETBIOS), 4922, 113 (AUTHENTICATION service), 23 (TELNET, possible tiny telnet server trojan), 6688, 31337 (possible back orifice and others), 32771 (Sun RPC), 67 (BOOTPS). Some of these ports are targeted because they are default ports for some well-known trojans. The fact that you have so many showing up in your most active destination ports indicates that a lot of activity is focused on searching for and exploiting (if they are found) these trojans on your systems. Other frequented ports include 53-DNS (which is on SANS Ten Most Critical Internet Security Threats List, because 50% of all DNS servers on the Internet are running vulnerable versions of BIND on this port), 110-POP3 (also on SANS top 10 list, because attackers who can exploit flaws in this service can often gain root-level control), 139-NETBIOS (also on SANS top 10 list, because, if configured incorrectly, can give full file system access to any party on the network), and 32771-SunRPC (also on SANS top 10, because of possible root compromise). In addition, 25-SMTP and 1080-SOCKS are listed by SANS (Perimeter Protection For An Added Layer of Defense Depth) as ports which should be blocked if not required for a specific use. In other words 10 of the 20 most frequented ports are well known for often having vulnerabilities. Of course the other 10 port may be just as vulnerable at your site, but are not well known ports. It is fairly simple to take a trojan whose default is a certain port and, given the source code, modify it to run on an unknown port.

We have also shown that, the top most active source IPs from your data are up to no good and you need to be particularly defensive against them. The top 10 offenders here include:
208.61.4.207 66.9.27.254 209.92.40.32 160.78.49.191 130.89.229.48,
62.252.21.241 194.244.78.145 63.88.175.201 203.32.161.197 210.113.89.200

Likewise, the most active destination IPs and destination ports from your data show us your most targeted systems and ports and, hence those in most need of defense. Your top 10 targeted systems include:
MY.NET.220.2 MY.NET.6.7 MY.NET.211.146 MY.NET.223.98 MY.NET.206.90
MY.NET.218.50 MY.NET.253.114 MY.NET.70.255 MY.NET.206.94 MY.NET.162.77

Aside from scans, the next most frequent detected events are traffic coming from networks in Israel and China (perhaps your afraid your electronic fortunes are of interest to a real Chinese fortune cookie factory). I assume you have created Snort rules to detect any activity from these sites because you consider them to be suspicious or hostile.

From the Israeli network, 212.179, we counted 31,034 different alerts, from 63 different IPs and 219 different source ports to 110 different MY.NET destination IPs and 97 destination ports.
The destinations of most frequency, which made up 65% of all the Israel activity, included:
MY.NET.211.146 (15%) MY.NET.223.98 (13%) MY.NET.206.90 (13%) MY.NET.203.142 (5%) MY.NET.218.142 (5%)
MY.NET.214.170 (4%) MY.NET.202.22 (3%) MY.NET.201.174 (3%) MY.NET.214.74 (2%) MY.NET.209.106 (2%)
The destination ports of most frequency included:
6699 (31%) 4619 (18%) 4922(16%) 6688(10%) 4990(5%)
1069 (2%) 1255 (2%) 1476(2%) 6346(1%) 4968(1%)
What is disturbing here (assuming that you consider them bad guys) is that the destination ports are not well known, either for services or for trojans. This could indicate that the destination IPs have been compromised by the Israeli network and they have installed there own services at these destination ports. We recommend you take a much closer look at these systems and block all traffic from the Israel network.

From the Chinese network, 159.226, we counted 8,148 different alerts, from 45 different IPs and 337 different source ports to 27 different MY.NET destination IPs and 52 destination ports. The distributions for destination IPs and ports were significantly different than from the Israeli network, with 3 destination IPs accounting for 93% of the traffic and 1 destination port accounting for 96% of the traffic.
The destinations of most frequency included:
MY.NET.6.7 (71%) MY.NET.100.230 (16%) MY.NET.253.43 (6%)
The destination ports of most frequency included:
25 (smtp - 96%) 113 (authentication service - 1%).
This may be indicative of an exploit of sendmail by this Chinese network. As with the Israeli network, we recommend you take a much closer look at these systems and block all traffic from the Chinese network.

Following the Israeli and Chinese network events, the next most frequent events were "Wingate 1080 Attempt" alerts. This is a response to a common probe, as many home and small-business users have vulnerable socks or wingates. An attacker is usually interested in this service because they can use it to bounce their connections through the server, and make other connections that will then seem to come from the victim IP address. 4764 events were recorded, from 570 different source IPs using 2861 different source ports were used to scan 2655 different IPs on port 1080 in the MY.NET network, using this probe.

In the main body of our analysis we have provide you with descriptions of all the remaining alerts types that we found in your data. We have only commented on the most frequently occurring here, but the entire

list deserves examination by you.

In closing, We would like to point out that we are providing you with an overview analysis and certainly not an exhaustive one. We have omitted doing any time based analysis of your data (that is, looking for patterns that have evolved over time. We have also not performed a source-destination correlation study (where you look for IPs in your network that are both source IPs at one time and destination IPs at another time - this sometimes shows IPs that were initially attacked, compromised, and then used as attackers). We have also not done a sort on the source IPs (which sometimes shows distributed attacks coming from the same network). Our goal was to provide you with an introduction to what we are capable of.

On a final note, we would like to offer you some recommendations and repeat a comment we made in our introduction. Intrusion detection is only one component of a comprehensive systems and networks security strategy. Intrusion detection alone is not enough. It also requires protective measures to slow the attackers down and reactive protocols and methods to respond to attacks as they occur. Your protective methods need to sufficiently slow attackers, so that your detection and reaction measures together are fast enough to stop an intruder, before they overcome your defenses.

Our recommendations for you include:

1) Installing appropriate network hardware to place your entire site behind one or a few choke points to the Internet.
2) Placing firewalls at these choke points and block all traffic except that going to known hosts and ports absolutely required for necessary access to the Internet. If you don't need them, definitely block your "friends" from Israel and China.
3) Harden your site's hosts by turning off all unnecessary services and keeping systems patched to current versions. Use tools such as tcp wrappers and checkpoint on your servers to further restrict and monitor use of your systems. Use encryption when transferring data across the network either for remote sessions (ssh) or remote copies (scp). Also use encryption on any web servers that contain sensitive data (ssl). Consider commercial host based intrusion detection systems for your key servers.
4) Install network-based intrusion detection systems both inside and outside your firewall.
5) Consider developing or purchasing an adaptive intrusion detection system, that can automatically detect and block the majority of the intrusive traffic to your site. This can dramatically increase you reaction time to an intrusion.

6) HIRE US, and we will provide you with all of this!!!

---

3) ANALYSIS PROCESS

We began by examining the 3 types of data files, and found 844,363 limes of ascii text, far too much data to analyze by visual examination. After determining the structure of each file type, we decided to write a special purpose Perl script to perform a frequency analysis of all the data, keying on such features as alert type, scan type, source IP, destination IP, source port, and destination port. Our idea was that the alert and scan type frequency distributions would show us the type of attacks that were most common, that the source IP and source port frequencies would show us where the most active attackers were coming from, and that the destination IP and destination port frequencies would show us the hosts and ports that were most under attack.

Before writing our special purpose frequency analysis script we did some preprocessing of the data. We wrote scripts for each of the 3 data file types that combined all of the data of one type into one large file, sorted sequentially by time (we used the "subject line" from each file which had a date stamp). This gave us 3 large files which we called ALL_Alerts (the SnortA<#.txt files), ALL_Scans (the SnortA<#.txt files), and ALL_Logs (the OOSche<#.txt files). The ALL_Scans files we further processed by placing all the data for one packet, which covered multiple lines, into one long line. This made it easier to use our frequency analysis script when searching for all the data related to one key (such as source IP).

Though the data sets did not contain mutually exclusive events (for example SYN-FIN scans show up in all 3 data file types), our method for weighting IPs with respect to level of activity is accomplished by summing occurrences in all 3 data types. This results in some events being counted more than once. We consider this acceptable as our goal was to determine a relative and not an absolute level of activity. For example, when looking at source IPs, the most active will be grouped in the top of the list and the least active grouped at the bottom of the list.

We have provided the Perl script we wrote, called AnalyzeALL (Appendix 2: Perl Code For Basic AnalyzeALL), When run with no input, AnalyzeALL generates statistics for all of the data. When run with an input parameter such as an IP address, network address, or particular alert type, the code generates only statistics for that IP address, network, or alert type. With slight modifications this code was used to get statistics on specific source IPs, destination IPs, and source subnets. It can also very easily be modified to look at only one of the 3 data file types. We provide the basic perl script in Appendix 2. Modifications, which are easily accomplished, are left to the reader.

For sample outputs see:
Appendix 1: Output From Running Basic AnalyzeALL
Appendix 3: Output From Running Modified AnalyzeALL - Looking For Source IP 211.46.110.81
Appendix 4: Output From Running Modified AnalyzeALL - Looking For Source Net 159.226
Appendix 5: Output From Running Modified AnalyzeALL - Looking For Source Net 212.179
Appendix 6: Output From Running Modified AnalyzeALL - Looking For Destination IP MY.NET.220.2
Appendix 7: Output From Running Modified AnalyzeALL - Looking For SYN-FIN Scans
Appendix 8: Output From Running Modified AnalyzeALL - Looking For Crafted Packets From MY.NET

After running AnalyzeALL on all the data we found the most common attack types (alerts and scans), most common likely attackers (source IPs) and most common likely targets (destination IPs and ports). We then narrowed our attention to items of special interest such as a particularly active source IP or destination IP, or an alert or scan that occurs with high frequency. This was accomplished by running a Modified AnalyzeALL, filtering out all but the area of interest, and drilling down further into the data.

Two examples of this activity follows:

-For each of the top 10 most active source IPs we ran our script, generating statistics only for that particular IP. This gave us a very good picture of what that particular IP was up to (alert types, scan types, target hosts and ports).

-For certain networks, such as the Chinese and Israeli networks which were on the watchlist alerts, we ran the script looking only for statistics relative to that network. Like the specific IP example above, this gave us a very good picture of the activities of these 2 networks.

A potential problem exists with performing frequency analysis an all the data and then focusing our attention on only where the most activity exists. We might miss the more quite and more subtle attacker. To solve this, once we understand the noisiest activities, we can then run our analysis script, filtering out the "noise", and focus on the more quite activities. By a successive iteration of this approach, even the most subtle activities will eventually stand out. This approach is demonstrated in how we discovered the crafted packets coming from the MY.NET network. We started by looking at source IPs from all the traffic. The noisiest activity here was from outside the MY.NET network. After developing an understanding of that traffic, we ran our script, filtering out all outside source IPs, to focus on only traffic from the MY.NET network. Most of this traffic looked normal (i.e. almost all destinations were within the MY.NET network to and from normally used service ports such as BOOTPS, NTP, DNS, NETBIOS, and SNMP), even though a lot of it went to and from service ports with known vulnerabilities. We then ran our script again, this time filtering out most of the MY.NET source traffic by looking only for traffic from MY.NET that had crafted packets. This yielded a list of probable compromised hosts that were involved in "stealth" scans.

As references we used:

W. Richard Stevens, "TCP/IP Illustrated, Volume 1".
Stephen Northcutt and Judy Novak, "Network Intrusion Detection, An Analyst's Handbook", Second Edition.
Winn Schwartau, "Time Based Security".

and the following web sites:

http://www.cve.mitre.org
http://www.whitehats.com
http://www.sans.org
http://www.securityfocus.com

//

Appendix 1: Output From Running Basic AnalyzeALL (truncated)

```
------------------------------------------------------------------
from ALERT Files:
     56250  0.48119  SYN-FIN scan!
     30997  0.26517  Watchlist 000220 IL-ISDNNET-990517
      8134  0.06958  Watchlist 000222 NET-NCFC
      6440  0.05509  PORTSCAN DETECTED
      4764  0.04075  WinGate 1080 Attempt
      2893  0.02475  TCP SMTP Source Port traffic
      2542  0.02175  Attempted Sun RPC high port access
      1813  0.01551  Broadcast Ping to subnet 70
      1697  0.01452  Back Orifice
       468  0.00400  SNMP public access
       277  0.00237  Null scan!
       218  0.00186  SMB Name Wildcard
       142  0.00121  Queso fingerprint
        96  0.00082  NMAP TCP ping!
        60  0.00051  SUNRPC highport access!
        56  0.00048  connect to 515 from inside
        15  0.00013  Probable NMAP fingerprint attempt
        13  0.00011  External RPC call
         7  0.00006  SITE EXEC - Possible wu-ftpd exploit - GIAC000623
         7  0.00006  Tiny Fragments - Possible Hostile Activity
         6  0.00005  site exec - Possible wu-ftpd exploit - GIAC000623
         2  0.00002  Happy 99 Virus
------------------------------------------------------------------
from SCAN Files:
    235361  0.75806   SYN **S*****
     50523  0.16273   SYNFIN **SF****
     21585  0.06952   UDP
       454  0.00146   FIN ***F****
       351  0.00113   VECNA *****P**
       281  0.00091   INVALIDACK **S*R*A*
       221  0.00071   NULL ********
       104  0.00033   SYN 21S***** RESERVEDBITS
        57  0.00018   INVALIDACK ***FR*A*
        29  0.00009   NOACK *1SF*P** RESERVEDBITS
        28  0.00009   FULLXMAS 21SFRPAU RESERVEDBITS
        16  0.00005   SYNFIN 21SF**** RESERVEDBITS
        15  0.00005   FIN *1*F**** RESERVEDBITS
        14  0.00005   UNKNOWN 2*S***A* RESERVEDBITS
        14  0.00005   NOACK *1**RP** RESERVEDBITS
        14  0.00005   NOACK *1SFRP** RESERVEDBITS
        13  0.00004   NOACK *1S**P** RESERVEDBITS
        13  0.00004   NOACK **S**P**
        13  0.00004   NOACK *1*FRP** RESERVEDBITS
        13  0.00004   NOACK **SF***U
        13  0.00004   INVALIDACK 2*SF**A* RESERVEDBITS
        13  0.00004   INVALIDACK *1SF*PA* RESERVEDBITS
```

12	0.00004	NOACK *1S**P*U RESERVEDBITS
12	0.00004	NOACK 2*SFR*** RESERVEDBITS
12	0.00004	NOACK **SFRP*U
12	0.00004	INVALIDACK 2*S*RPAU RESERVEDBITS
12	0.00004	NOACK **S*R***
11	0.00004	UNKNOWN 2*****A* RESERVEDBITS
11	0.00004	UNKNOWN *1S***A* RESERVEDBITS
11	0.00004	NOACK 21S*R*** RESERVEDBITS
11	0.00004	XMAS ***F*P*U
11	0.00004	UNKNOWN *1**R*** RESERVEDBITS
11	0.00004	NOACK *1S*R**U RESERVEDBITS
11	0.00004	INVALIDACK ****RPAU
11	0.00004	NOACK *1*FR**U RESERVEDBITS
11	0.00004	NOACK 2**FR**U RESERVEDBITS
10	0.00003	INVALIDACK 21*FRPAU RESERVEDBITS
10	0.00003	VECNA 2**F*P** RESERVEDBITS
10	0.00003	NOACK 21**RP** RESERVEDBITS
10	0.00003	UNKNOWN 21***PAU RESERVEDBITS
10	0.00003	NOACK *1S*R*** RESERVEDBITS
10	0.00003	NOACK 21S**P** RESERVEDBITS
10	0.00003	INVALIDACK *1SF*PAU RESERVEDBITS
10	0.00003	INVALIDACK 2**FRPA* RESERVEDBITS
10	0.00003	INVALIDACK 21SF*PA* RESERVEDBITS
10	0.00003	INVALIDACK ***FRPA*
10	0.00003	INVALIDACK *1S**PA* RESERVEDBITS
10	0.00003	INVALIDACK 2**FR*AU RESERVEDBITS
10	0.00003	INVALIDACK 2**FR*A* RESERVEDBITS

SOURCE IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL	SOURCE NAME
208.61.4.207	21725	0.04461	6660	6634	8431	adsl-61-4-207.mia.bellsouth.net
66.9.27.254	20649	0.04240	0	20649	0	
209.92.40.32	15699	0.03224	4993	4956	5750	dslcv1-32.fast.net
160.78.49.191	14418	0.02961	7226	7192	0	ema.chim.unipr.it
130.89.229.48	13297	0.02731	3886	3860	5551	cal032044.student.utwente.nl
62.252.21.241	13290	0.02729	233	13057	0	pc241-gui4.cable.ntl.com
194.244.78.145	11906	0.02445	2	11904	0	
63.88.175.201	11753	0.02414	35	11718	0	www.multilateral.com
203.32.161.197	11644	0.02391	3571	3562	4511	adnet.imgserv.com
210.113.89.200	11388	0.02339	3598	3566	4224	
193.64.114.10	10934	0.02245	3321	3321	4292	net10.printeq.fi
195.103.69.159	10581	0.02173	3319	3294	3968	
62.157.23.237	9664	0.01985	23	9641	0	p3E9D17ED.dip.t-dialin.net
63.248.55.245	9083	0.01865	10	9073	0	3ff837f5.dsl.flashcom.net
62.96.169.86	9062	0.01861	123	8939	0	m-dialin-86.addcom.de
24.23.151.112	8795	0.01806	32	8763	0	cx673530-a.vbch1.va.home.com
63.195.56.20	8670	0.01780	3921	0	4749	adsl-63-195-56-20.dsl.snfc21.pacbell.net
64.50.161.162	8653	0.01777	18	8635	0	public.washingtonhomes.com
210.101.101.110	8442	0.01734	2610	2578	3254	
212.0.107.107	7807	0.01603	2364	2340	3103	
128.211.237.11	7035	0.01445	32	7003	0	cary-b-011.resnet.purdue.edu
211.49.165.9	6927	0.01423	8	6919	0	
213.41.69.52	6831	0.01403	3425	3406	0	hosting-52.69.rev.fr.colt.net
62.155.244.68	6520	0.01339	119	6401	0	p3E9BF444.dip.t-dialin.net
159.226.45.3	6295	0.01293	6295	0	0	aphy.iphy.ac.cn
216.191.162.145	6131	0.01259	38	6093	0	win-mb52-161.netcom.ca
212.179.95.5	6117	0.01256	6117	0	0	cable-95005.bezeqint.net
63.198.207.51	6062	0.01245	29	6033	0	adsl-63-198-207-51.dsl.snfc21.pacbell.net
63.167.58.13	5842	0.01200	1557	1546	2739	
143.89.13.3	5343	0.01097	1586	1587	2170	ustlnx6.ust.hk
208.214.247.60	4907	0.01008	26	4881	0	host60.djgrp.com
146.101.147.251	4875	0.01001	20	4855	0	g-f6.tsq.stores.easyeverything.com
199.239.94.98	4836	0.00993	0	4836	0	dsl98.9healthfair.org
130.225.136.39	4257	0.00874	26	4231	0	obelix.bmb.sdu.dk
163.10.19.34	4251	0.00873	1106	1105	2040	decanato.exactas.unlp.edu.ar
211.46.110.81	4125	0.00847	2664	1342	119	
195.247.65.216	4103	0.00843	38	4065	0	port216.duesseldorf.ivm.de
212.179.27.6	4015	0.00825	4013	2	0	clnt-27006.bezeqint.net
212.179.79.2	3950	0.00811	3950	0	0	
212.179.44.115	3938	0.00809	3938	0	0	bzq-44-115.bezeqint.net
63.193.210.208	3757	0.00772	1893	1864	0	adsl-63-193-210-208.dsl.snfc21.pacbell.net
128.2.81.133	3666	0.00753	1594	0	2072	
198.11.17.157	3350	0.00688	0	3350	0	home-dhcp3-157.Colorado.EDU
212.187.21.156	3330	0.00684	1112	1082	1136	c21156.upc-c.chello.nl
128.100.201.133	3059	0.00628	72	2987	0	storm.utias.utoronto.ca
MY.NET.224.150	2981	0.00612	0	2981	0	
130.237.34.161	2940	0.00604	39	2901	0	
24.43.30.182	2891	0.00594	6	2885	0	cr283564-a.brntfd1.on.wave.home.com
63.206.212.112	2809	0.00577	128	2681	0	adsl-63-206-212-112.dsl.snfc21.pacbell.net
4.40.0.91	2782	0.00571	49	2733	0	crtntx1-ar4-000-091.dsl.gtei.net

DEST IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.220.2	11932	0.02450	6	11926	0
MY.NET.6.7	5816	0.01194	5800	14	2
MY.NET.211.146	4876	0.01001	4814	51	11
MY.NET.223.98	3953	0.00812	3940	12	1
MY.NET.206.90	3934	0.00808	3918	13	3
MY.NET.218.50	2372	0.00487	9	2359	4
MY.NET.253.114	1987	0.00408	9	1976	2
MY.NET.70.255	1814	0.00373	1813	0	1
MY.NET.206.94	1806	0.00371	4	1799	3
MY.NET.162.77	1763	0.00362	3	1759	1
MY.NET.203.142	1661	0.00341	1640	18	3

MY.NET.205.214	1595	0.00328	3	1589	3
MY.NET.120.36	1591	0.00327	0	1591	0
MY.NET.218.142	1480	0.00304	1463	13	4
MY.NET.214.170	1387	0.00285	1371	14	2
MY.NET.215.210	1373	0.00282	3	1367	3
MY.NET.60.16	1348	0.00277	41	1306	1
MY.NET.100.230	1304	0.00268	1289	15	0
MY.NET.140.57	1222	0.00251	1	1220	1
MY.NET.70.121	1220	0.00251	9	1206	5
MY.NET.204.26	1174	0.00241	3	1169	2
MY.NET.204.218	1131	0.00232	3	1127	1
MY.NET.205.246	1097	0.00225	16	1076	5
MY.NET.212.114	1083	0.00222	0	1083	0
MY.NET.97.59	1006	0.00207	9	996	1
MY.NET.98.168	988	0.00203	11	973	4
MY.NET.202.22	974	0.00200	952	19	3
MY.NET.98.171	907	0.00186	6	900	1
MY.NET.162.36	874	0.00179	6	867	1
MY.NET.206.106	864	0.00177	295	565	4
MY.NET.201.174	826	0.00170	803	22	1
MY.NET.207.58	726	0.00149	6	716	4
MY.NET.211.254	719	0.00148	0	719	0
MY.NET.214.74	679	0.00139	669	8	2
MY.NET.209.106	665	0.00137	655	9	1
MY.NET.221.146	659	0.00135	639	16	4
MY.NET.223.254	636	0.00131	627	8	1
MY.NET.211.178	619	0.00127	610	8	1
MY.NET.253.43	600	0.00123	589	11	0
MY.NET.15.215	591	0.00121	582	6	3
MY.NET.227.190	576	0.00118	565	11	0
MY.NET.217.34	571	0.00117	0	571	0
MY.NET.101.192	561	0.00115	561	0	0
MY.NET.101.89	546	0.00112	4	542	0
MY.NET.223.6	532	0.00109	2	529	1
MY.NET.203.206	527	0.00108	508	17	2
MY.NET.98.181	510	0.00105	501	8	1
MY.NET.221.246	499	0.00102	490	7	2
MY.NET.225.58	489	0.00100	477	10	2
MY.NET.60.11	466	0.00096	70	395	1

SOURCE PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
21	55912	0.11482	19619	14213	22080
53	52355	0.10751	18307	19256	14792
9704	45787	0.09403	14184	14168	17435
27374	11362	0.02333	3572	3566	4224
7777	10632	0.02183	0	10632	0
25	2895	0.00595	2893	2	0
1067	2753	0.00565	2701	51	1
4000	2587	0.00531	2537	50	0
67	2312	0.00475	0	2311	1
6699	2114	0.00434	1903	184	27
1498	1896	0.00389	1823	73	0
0	1835	0.00377	1820	0	15
1574	1770	0.00363	1727	43	0
64524	1751	0.00360	0	1751	0
20	1700	0.00349	23	1676	1
123	1586	0.00326	0	1586	0
36203	1517	0.00312	0	1517	0
13270	1459	0.00300	1459	0	0
1031	1421	0.00292	1355	66	0
32685	1409	0.00289	1409	0	0
1192	1399	0.00287	1347	52	0
1057	1304	0.00268	1242	62	0
34997	1294	0.00266	2	1292	0
2078	1179	0.00242	1121	58	0
23	1107	0.00227	123	983	1
34996	1060	0.00218	0	1060	0
31338	1031	0.00212	642	389	0
1167	1016	0.00209	955	61	0
4	845	0.00174	327	330	188
1263	840	0.00173	787	53	0
1271	837	0.00172	784	53	0
2118	733	0.00151	674	59	0
4092	730	0.00150	684	46	0
1090	721	0.00148	671	47	3
4103	690	0.00142	640	50	0
2009	641	0.00132	578	63	0
1254	630	0.00129	594	36	0
109	626	0.00129	267	0	359
4112	622	0.00128	564	58	0
2100	612	0.00126	566	46	0
10120	609	0.00125	609	0	0
4094	594	0.00122	544	50	0
1220	533	0.00109	480	53	0
55021	505	0.00104	505	0	0
7281	500	0.00103	500	0	0
4101	498	0.00102	450	48	0
4121	486	0.00100	435	51	0
4107	463	0.00095	401	62	0
14293	458	0.00094	0	458	0
2637	454	0.00093	403	51	0

DEST PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL

```
21                  159399  0.32734      19639     117678      22082
53                   52646  0.10811      18341      19513      14792
9704                 45787  0.09403      14184      14168      17435
27374                44015  0.09039       3577      36214       4224
515                  25853  0.05309         56      25797          0
25                   11122  0.02284      11034         88          0
6699                 10124  0.02079       9762        318         44
98                    9467  0.01944          0       9467          0
9088                  8763  0.01800          0       8763          0
110                   8728  0.01792         43       8685          0
1080                  6669  0.01370       4774       1895          0
4619                  5738  0.01178       5734          4          0
139                   5648  0.01160          0       5648          0
4922                  4845  0.00995       4813         26          6
113                   4353  0.00894        109       4244          0
23                    3574  0.00734        343       3044        187
6688                  3513  0.00721       3293        190         30
31337                 2914  0.00598       1697       1217          0
32771                 2607  0.00535       2602          5          0
67                    2295  0.00471          0       2295          0
19000                 2081  0.00427          0       2081          0
0                     1835  0.00377       1820          0         15
4990                  1460  0.00300       1459          1          0
5232                   944  0.00194          0        944          0
1069                   652  0.00134        648          4          0
109                    641  0.00132        267         15        359
1255                   627  0.00129        625          1          1
1476                   590  0.00121        579         11          0
6346                   528  0.00108        474         53          1
161                    473  0.00097        468          5          0
4968                   437  0.00090        420         17          0
6700                   378  0.00078        368          9          1
443                    373  0.00077         14        356          3
1057                   333  0.00068          0        333          0
1041                   317  0.00065          0        317          0
2781                   317  0.00065          0        317          0
1162                   316  0.00065          0        316          0
4410                   290  0.00060        290          0          0
1103                   284  0.00058          0        284          0
3083                   261  0.00054          0        261          0
4752                   260  0.00053        260          0          0
4722                   258  0.00053        257          1          0
2183                   247  0.00051          0        247          0
4545                   243  0.00050        243          0          0
8311                   242  0.00050        148         73         21
2184                   239  0.00049          0        239          0
2981                   238  0.00049          0        238          0
137                    232  0.00048        218         14          0
3111                   229  0.00047          0        229          0
4191                   218  0.00045        217          1          0
-------------------------------------------------------------------------
-------------------------------------------------------------------------
total number of events from all 3 data file types = 486956
total number of unique source IPs                 = 2625
total number of unique source ports               = 18081
total number of unique destination IPs            = 35946
total number of unique destination ports          = 16647
```

Appendix 2: Perl Code For Basic AnalyzeALL

```
#!/usr/local/bin/perl
$input = $ARGV[0];
$cutoff = 100;
print "string = $input\n";
#
# ---processing ALERTS (SnortA<#.txt files combined)---
#
$inalerts = 0;
$inscans = 0;
$inlogs = 0;
require "flush.pl";
open(ALERTFILE,"< ALL_Alerts");
while()
{
 if(/\[\*\*\]/ && !/spp_portscan/ && /$input/)
 {
  $inalerts = 1;
  @spl = split(/ \[\*\*\] /, $_);
  $alert = $spl[1];
  $srcanddst = $spl[2];
  chop $srcanddst;
  @spl2 = split(/\s+/, $srcanddst);
  $srcandport = $spl2[0];
  $dstandport = $spl2[2];
  @spl3 = split(/:/, $srcandport);
  $src = $spl3[0];
  $srcport = $spl3[1];
  @spl4 = split(/:/, $dstandport);
  $dst = $spl4[0];
  $dstport = $spl4[1];
  # print;
```

```
  # print "\t-$alert-$src-$srcport-$dst-$dstport\n";
  $srccount_a{$src} += 1;
  $dstcount_a{$dst} += 1;
  $srcportcount_a{$srcport} += 1;
  $dstportcount_a{$dstport} += 1;
  $alertcount_a{$alert} += 1;
  $total_a += 1;
  $total += 1;
  $srccount{$src} += 1;
  $dstcount{$dst} += 1;
  $srcportcount{$srcport} += 1;
  $dstportcount{$dstport} += 1;
 }
 if(/PORTSCAN DETECTED/ && /$input/)
 {
  @spl = split(/from /, $_);
  @spl2 = split(/ \(/, $spl[1]);
  $scanip = $spl2[0];
  $countscan_a{$scanip} += 1;
  $totalscans_a += 1;
  $srccount_a{$scanip} += 1;
  $srccount{$scanip} += 1;
  $alert = "PORTSCAN DETECTED";
  $alertcount_a{$alert} += 1;
  $total_a += 1;
  $total += 1;
 }
}
close(ALERTFILE);
if ($inalerts == 0)
{
        print "\t$input NOT in ALERTS files\n";
}
else
{
 print "\t$input IS present in ALERTS files\n";
}


#
# ---processing SCANS (SnortS<#.txt files combined)---
#
require "flush.pl";

open(SCANFILE,"< ALL_Scans");
while()
{
 if (/MY\.NET/ && /$input/)
 {
                $inscans = 1;
  chop $_;
  @spl = split(/\s+/, $_);
  $srcandport = $spl[3];
  @spl2 = split(/:/, $srcandport);
  $src = $spl2[0];
  $srcport = $spl2[1];
  $dstandport = $spl[5];
  @spl2 = split(/:/, $dstandport);
  $dst = $spl2[0];
  $dstport = $spl2[1];
  # $scantype = $spl[6];
  @spl = split(/$dstandport/, $_);
                $scantype = $spl[1];
  $srccount_s{$src} += 1;
  $dstcount_s{$dst} += 1;
  $srcportcount_s{$srcport} += 1;
  $dstportcount_s{$dstport} += 1;
  $scantypecount_s{$scantype} += 1;
  $total_s += 1;
  $total += 1;
  # $src_dst = "${srcip}_${dstip}";
  # $linkcount_s{$src_dst} += 1;
  $srccount{$src} += 1;
  $dstcount{$dst} += 1;
  $srcportcount{$srcport} += 1;
  $dstportcount{$dstport} += 1;
 }
}
close(SCANFILE);




if ($inscans == 0)
{
        print "\t$input NOT in SCANS files\n";
}
else
{
 print "\t$input IS present in SCANS files\n";
}

#
# ---processing LOGS (OOSche<#.txt files combined)---
#
# NOTE: The OOSche files were modified so that all the data for
# one packet was on one line with the word "LINE" placed where
# a line break used to be -- this makes it easy]ier to search
```

```
# for a particular string and get the entire packet
#
open(LOGFILE,"< ALL_Logs");
while()
{
   if(/$input/)
   {
 $inlogs = 1;
 @spl = split(/ LINE /, $_);
 @spl2 = split(/\s+/, $spl[1]);
 $srcandport = @spl2[1];
 $dstandport = @spl2[3];
 @spl3 = split(/:/, $srcandport);
 $src = $spl3[0];
 $srcport = $spl3[1];
 @spl3 = split(/:/, $dstandport);
 $dst = $spl3[0];
 $dstport = $spl3[1];
 $srccount_l{$src} += 1;
 $dstcount_l{$dst} += 1;
 $srcportcount_l{$srcport} += 1;
 $dstportcount_l{$dstport} += 1;
 # $src_dst = "${src}_${dst}";
 # $linkcount_l{$src_dst} += 1;
 $total_l += 1;
 $total += 1;
 $srccount{$src} += 1;
 $dstcount{$dst} += 1;
 $srcportcount{$srcport} += 1;
 $dstportcount{$dstport} += 1;
   }
}
close(LOGFILE);
if ($inlogs == 0)
{
        print "\t$input NOT in LOGS files\n";
}
else
{
 print "\t$input IS present in LOGS files\n";
}
print "--------------------------------------------------------------------------\n";
print "from ALERT Files:\n";
flush(STDOUT);
$linecount = 0;
foreach $alert(sort {$alertcount_a{$b} <= $alertcount_a{$a}} keys(%alertcount_a))
{
        $linecount += 1;
        if($linecount <= $cutoff)
        {
  $fraction = $alertcount_a{$alert}/$total_a;
                printf("%10d  %6.5f  %s\n", $alertcount_a{$alert}, $fraction, $alert);
                flush(STDOUT);
        }
}


print "--------------------------------------------------------------------------\n";
print "from SCAN Files:\n";
flush(STDOUT);
$linecount = 0;
foreach $scantype(sort {$scantypecount_s{$b} <= $scantypecount_s{$a}} keys(%scantypecount_s))
{
        $linecount += 1;
        if($linecount <= $cutoff)
        {
  $fraction = $scantypecount_s{$scantype}/$total_s;
                printf("%10d  %6.5f  %s\n", $scantypecount_s{$scantype}, $fraction, $scantype);
                flush(STDOUT);
        }
}


print "--------------------------------------------------------------------------\n";
printf("SOURCE IP             ALL   FRACTION      ALERTS     SCANS      LOGS     SOURCE NAME\n");
printf("                     FILES   OF ALL       FILES      FILES      FILES                    \n");
printf("                     TOTAL   FILES        TOTAL      TOTAL      TOTAL                    \n");
printf("\n");
$linecount = 0;
$sum_src = 0;
foreach $srcip(sort {$srccount{$b} <= $srccount{$a}} keys(%srccount))
{
        $linecount += 1;
 $sum_src += 1;
        if($linecount <= $cutoff)
        {
             $percent = $srccount{$srcip}/$total;
     $srcname{$srcip} = &GetHostName($srcip);
             printf("%-15s %10d %8.5f %10d %10d %10d     %s\n", $srcip, $srccount{$srcip}, $percent, $srccount_a{$srcip},$srccount_s{$srcip},$s
            flush(STDOUT);
        }
}

print "--------------------------------------------------------------------------\n";
printf("DEST IP               ALL   FRACTION      ALERTS     SCANS      LOGS     \n");
printf("                     FILES   OF ALL       FILES      FILES      FILES                    \n");
printf("                     TOTAL   FILES        TOTAL      TOTAL      TOTAL                    \n");
printf("\n");
```

```
$linecount = 0;
$sum_dest = 0;
foreach $dstip(sort {$dstcount{$b} <= $dstcount{$a}} keys(%dstcount))
{
        $linecount += 1;
        $sum_dest += 1;
        if($linecount <= $cutoff)
        {
             $percent = $dstcount{$dstip}/$total;
             printf("%-15s %10d %8.5f %10d %10d %10d\n", $dstip, $dstcount{$dstip}, $percent, $dstcount_a{$dstip},$dstcount_s{$dstip},$dstcount_
            flush(STDOUT);
        }
}

print "------------------------------------------------------------------------\n";
printf("SOURCE PORT           ALL   FRACTION      ALERTS     SCANS      LOGS     \n");
printf("                     FILES   OF ALL       FILES      FILES      FILES                    \n");
printf("                     TOTAL   FILES        TOTAL      TOTAL      TOTAL                    \n");
printf("\n");

$linecount = 0;
$sum_srcport = 0;
foreach $srcport(sort {$srcportcount{$b} <= $srcportcount{$a}} keys(%srcportcount))
{
        $linecount += 1;
        $sum_srcport += 1;
        if($linecount <= $cutoff)
        {
             $percent = $srcportcount{$srcport}/$total;
             printf("%-15d %10d %8.5f %10d %10d %10d\n", $srcport, $srcportcount{$srcport}, $percent, $srcportcount_a{$srcport},$srcportcount_s
            flush(STDOUT);
        }
}

print "------------------------------------------------------------------------\n";
printf("DEST PORT             ALL   FRACTION      ALERTS     SCANS      LOGS     \n");
printf("                     FILES   OF ALL       FILES      FILES      FILES                    \n");
printf("                     TOTAL   FILES        TOTAL      TOTAL      TOTAL                    \n");
printf("\n");

$linecount = 0;
$sum_dstport = 0;
foreach $dstport(sort {$dstportcount{$b} <= $dstportcount{$a}} keys(%dstportcount))
{
        $linecount += 1;
        $sum_dstport += 1;
        if($linecount <= $cutoff)
        {
             $percent = $dstportcount{$dstport}/$total;
             printf("%-15d %10d %8.5f %10d %10d %10d\n", $dstport, $dstportcount{$dstport}, $percent, $dstportcount_a{$dstport},$dstportcount_s
            flush(STDOUT);
        }
}
print "------------------------------------------------------------------------\n";
print "------------------------------------------------------------------------\n";
printf("total number of events from all 3 data file types = %d\n", $total);
printf("total number of unique source IPs                 = %d\n", $sum_src);
printf("total number of unique source ports               = %d\n", $sum_srcport);
printf("total number of unique destination IPs            = %d\n", $sum_dest);
printf("total number of unique destination ports          = %d\n", $sum_dstport);

sub GetHostName
{
        $ip = $_[0];
        @ipoctets = split(/\./, $ip);
         $binip = pack "c4",$ipoctets[0],$ipoctets[1],$ipoctets[2],$ipoctets[3];
        @info = gethostbyaddr($binip,2);
        $name = $info[0];
        return $name;
}
```

Appendix 3: Output From Running Modified AnalyzeALL - Looking For Source IP 211.46.110.81

```
string = 211.46.110.81
 211.46.110.81 IS present in ALERTS files
 211.46.110.81 IS present in SCANS files
 211.46.110.81 IS present in LOGS files
------------------------------------------------------------------------
from ALERT Files:
      1789 TCP SMTP Source Port traffic
       596 PORTSCAN DETECTED
       276 SYN-FIN scan!
         2 External RPC call
         1 SUNRPC highport access!
------------------------------------------------------------------------
from SCAN Files:
       494  SYN **S*****
       301  VECNA *****P**
       276  SYNFIN **SF****
       271  FIN ***F****
------------------------------------------------------------------------
SOURCE IP             ALL   FRACTION      ALERTS     SCANS      LOGS     SOURCE NAME
```

	FILES TOTAL	OF ALL FILES	FILES TOTAL	FILES TOTAL	FILES TOTAL
211.46.110.81	4125	1.00000	2664	1342	119

DEST IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.109.40	5	0.00121	1	3	1
MY.NET.204.42	5	0.00121	1	3	1
MY.NET.188.18	5	0.00121	2	2	1
MY.NET.157.106	5	0.00121	2	2	1
MY.NET.204.110	4	0.00097	1	2	1
MY.NET.227.249	4	0.00097	2	2	0
MY.NET.231.177	4	0.00097	2	2	0
MY.NET.202.145	4	0.00097	1	2	1
MY.NET.204.53	4	0.00097	1	2	1
MY.NET.21.29	4	0.00097	1	2	1
MY.NET.203.201	4	0.00097	1	2	1
MY.NET.153.1	4	0.00097	2	1	1
MY.NET.21.21	4	0.00097	1	2	1
MY.NET.232.165	4	0.00097	2	2	0
MY.NET.75.28	4	0.00097	1	2	1
MY.NET.232.121	4	0.00097	1	3	0
MY.NET.200.83	4	0.00097	1	2	1
MY.NET.203.189	4	0.00097	1	2	1
MY.NET.205.110	4	0.00097	2	1	1
MY.NET.138.1	4	0.00097	1	2	1
MY.NET.202.93	4	0.00097	1	2	1
MY.NET.115.178	4	0.00097	2	1	1
MY.NET.228.155	4	0.00097	1	3	0
MY.NET.69.216	4	0.00097	1	2	1
MY.NET.1.1	4	0.00097	1	2	1
MY.NET.217.175	4	0.00097	1	3	0
MY.NET.219.135	4	0.00097	2	2	0
MY.NET.228.121	4	0.00097	1	3	0
MY.NET.228.120	4	0.00097	1	3	0
MY.NET.161.10	4	0.00097	1	2	1
MY.NET.60.20	4	0.00097	1	2	1
MY.NET.15.127	3	0.00073	1	1	1
MY.NET.217.131	3	0.00073	0	3	0
MY.NET.217.113	3	0.00073	1	2	0
MY.NET.213.5	3	0.00073	1	2	0
MY.NET.208.101	3	0.00073	1	2	0
MY.NET.211.49	3	0.00073	1	2	0
MY.NET.211.13	3	0.00073	2	1	0
MY.NET.121.13	3	0.00073	1	1	1
MY.NET.228.64	3	0.00073	1	2	0
MY.NET.215.101	3	0.00073	1	2	0
MY.NET.204.186	3	0.00073	1	1	1
MY.NET.222.160	3	0.00073	1	2	0
MY.NET.228.40	3	0.00073	1	2	0
MY.NET.228.35	3	0.00073	1	2	0
MY.NET.204.169	3	0.00073	1	1	1
MY.NET.222.140	3	0.00073	1	2	0
MY.NET.222.136	3	0.00073	1	2	0
MY.NET.1.203	3	0.00073	1	1	1
MY.NET.228.11	3	0.00073	1	2	0

SOURCE PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
25	1789	0.43370	1789	0	0
4	671	0.16267	276	276	119
5	301	0.07297	0	301	0
2	271	0.06570	0	271	0
4362	3	0.00073	0	3	0
1071	2	0.00048	0	2	0
2200	2	0.00048	0	2	0
3772	2	0.00048	0	2	0
1266	2	0.00048	0	2	0
4019	2	0.00048	0	2	0
2458	2	0.00048	0	2	0
3418	2	0.00048	0	2	0
2145	2	0.00048	0	2	0
3371	2	0.00048	0	2	0
4972	2	0.00048	0	2	0
4402	2	0.00048	0	2	0
1505	2	0.00048	0	2	0
3304	2	0.00048	0	2	0
1967	2	0.00048	0	2	0
2868	2	0.00048	0	2	0
1320	2	0.00048	0	2	0
4866	2	0.00048	0	2	0
2525	2	0.00048	0	2	0
1618	2	0.00048	0	2	0
4009	2	0.00048	0	2	0
2646	2	0.00048	0	2	0
1336	2	0.00048	0	2	0
4263	2	0.00048	0	2	0
2854	2	0.00048	0	2	0
3421	2	0.00048	0	2	0
4052	2	0.00048	0	2	0
3878	2	0.00048	0	2	0
1088	2	0.00048	0	2	0
2772	2	0.00048	0	2	0

```
3540                    2  0.00048          0          2          0
1933                    2  0.00048          0          2          0
2175                    2  0.00048          0          2          0
4551                    1  0.00024          0          1          0
1087                    1  0.00024          0          1          0
3663                    1  0.00024          0          1          0
3744                    1  0.00024          0          1          0
1089                    1  0.00024          0          1          0
1326                    1  0.00024          0          1          0
1246                    1  0.00024          0          1          0
4719                    1  0.00024          0          1          0
3747                    1  0.00024          0          1          0
1070                    1  0.00024          0          1          0
1408                    1  0.00024          0          1          0
4700                    1  0.00024          0          1          0
3108                    1  0.00024          0          1          0
-------------------------------------------------------------------------
DEST PORT             ALL   FRACTION      ALERTS      SCANS       LOGS
                     FILES   OF ALL       FILES      FILES       FILES
                     TOTAL   FILES        TOTAL      TOTAL       TOTAL

25                    1789  0.43370       1789          0           0
23                    1624  0.39370        276       1229         119
1                      113  0.02739          0        113           0
111                      2  0.00048          2          0           0
32771                    1  0.00024          1          0           0
-------------------------------------------------------------------------
-------------------------------------------------------------------------
total number of events from all 3 data file types = 4125
total number of unique source IPs                 = 1
total number of unique source ports               = 467
total number of unique destination IPs            = 2886
total number of unique destination ports          = 5
```

Appendix 4: Output From Running Modified AnalyzeALL - Looking For Source Net 159.226

```
string = 159.226
 159.226 IS present in ALERTS files
 159.226 IS present in SCANS files
 159.226 IS present in LOGS files
-------------------------------------------------------------------------
from ALERT Files:
      8134 Watchlist 000222 NET-NCFC
         2 SYN-FIN scan!
-------------------------------------------------------------------------
from SCAN Files:
         9  SYN **S*****
         2  SYNFIN **SF****
-------------------------------------------------------------------------
SOURCE IP             TOTAL  FRACTION      ALERTS      SCANS      LOGS     SOURCE NAME
                       ALL    OF ALL       FILES      FILES      FILES
                      FILES   FILES        TOTAL      TOTAL      TOTAL

159.226.45.3           6295  0.77258       6295          0          0     aphy.iphy.ac.cn
159.226.91.20          1209  0.14838       1209          0          0
159.226.41.166          123  0.01510        123          0          0
159.226.5.77             87  0.01068         87          0          0
159.226.228.1            58  0.00712         58          0          0
159.226.157.1            38  0.00466         38          0          0
159.226.66.130           33  0.00405         33          0          0
159.226.92.10            29  0.00356         29          0          0     netlib.amss.ac.cn
159.226.114.1            21  0.00258         21          0          0
159.226.63.200           20  0.00245         20          0          0
159.226.159.1            19  0.00233         19          0          0
159.226.118.9            18  0.00221         18          0          0     moon.ibp.ac.cn
159.226.21.3             18  0.00221         18          0          0
159.226.5.222            16  0.00196         16          0          0
159.226.6.5              14  0.00172         14          0          0     search.cnnic.net.cn
159.226.39.1             13  0.00160         13          0          0
159.226.49.157           12  0.00147         12          0          0
159.226.115.1            12  0.00147         12          0          0
159.226.5.83              9  0.00110          9          0          0
159.226.172.136           8  0.00098          8          0          0
159.226.41.188            7  0.00086          7          0          0
159.226.45.204            6  0.00074          6          0          0     dos204.iphy.ac.cn
159.226.224.1             6  0.00074          6          0          0
159.226.144.130           6  0.00074          6          0          0
159.226.120.14            6  0.00074          6          0          0
159.226.63.190            5  0.00061          5          0          0     lcc.icm.ac.cn
159.226.42.9              5  0.00061          5          0          0
159.226.120.19            4  0.00049          4          0          0
159.226.159.146           3  0.00037          3          0          0
159.226.128.1             3  0.00037          3          0          0     server.shcnc.ac.cn
159.226.61.62             3  0.00037          3          0          0
159.226.45.60             3  0.00037          3          0          0     ssc.iphy.ac.cn
159.226.22.55             3  0.00037          3          0          0
159.226.113.1             3  0.00037          3          0          0
159.226.158.188           3  0.00037          3          0          0
159.226.5.65              2  0.00025          2          0          0
159.226.2.20              2  0.00025          2          0          0     fruits.cnc.ac.cn
159.226.23.3              2  0.00025          2          0          0
159.226.111.1             2  0.00025          2          0          0
```

159.226.218.3	2	0.00025	2	0	0	
159.226.209.2	2	0.00025	2	0	0	apple.cast.ac.cn
159.226.247.60	1	0.00012	1	0	0	
159.226.64.152	1	0.00012	1	0	0	
159.226.22.59	1	0.00012	1	0	0	
159.226.5.207	1	0.00012	1	0	0	

DEST IP	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.6.7	5793	0.71097	5793	0	0
MY.NET.100.230	1286	0.15783	1286	0	0
MY.NET.253.43	461	0.05658	461	0	0
MY.NET.253.41	179	0.02197	179	0	0
MY.NET.253.42	151	0.01853	151	0	0
MY.NET.99.51	70	0.00859	70	0	0
MY.NET.100.81	53	0.00650	53	0	0
MY.NET.145.9	41	0.00503	41	0	0
MY.NET.159.226	14	0.00172	2	11	1
MY.NET.6.34	13	0.00160	13	0	0
MY.NET.145.18	13	0.00160	13	0	0
MY.NET.6.47	12	0.00147	12	0	0
MY.NET.253.24	9	0.00110	9	0	0
MY.NET.253.53	8	0.00098	8	0	0
MY.NET.1.2	8	0.00098	8	0	0
MY.NET.75.3	6	0.00074	6	0	0
MY.NET.100.165	5	0.00061	5	0	0
MY.NET.253.51	4	0.00049	4	0	0
MY.NET.60.17	4	0.00049	4	0	0
MY.NET.130.185	3	0.00037	3	0	0
MY.NET.154.27	3	0.00037	3	0	0
MY.NET.70.33	3	0.00037	3	0	0
MY.NET.253.52	2	0.00025	2	0	0
MY.NET.6.35	2	0.00025	2	0	0
MY.NET.158.32	2	0.00025	2	0	0
MY.NET.253.112	2	0.00025	2	0	0
MY.NET.110.150	1	0.00012	1	0	0

SOURCE PORT	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
4092	683	0.08382	683	0	0
4103	640	0.07855	640	0	0
2009	576	0.07069	576	0	0
4112	563	0.06910	563	0	0
4094	542	0.06652	542	0	0
4101	450	0.05523	450	0	0
4121	435	0.05339	435	0	0
4107	400	0.04909	400	0	0
4097	395	0.04848	395	0	0
4109	394	0.04836	394	0	0
4082	390	0.04786	390	0	0
4124	380	0.04664	380	0	0
4090	375	0.04602	375	0	0
4115	329	0.04038	329	0	0
3594	194	0.02381	194	0	0
1566	142	0.01743	142	0	0
23	123	0.01510	123	0	0
3460	86	0.01055	86	0	0
3599	78	0.00957	78	0	0
1255	64	0.00785	64	0	0
1562	61	0.00749	61	0	0
2553	43	0.00528	43	0	0
113	37	0.00454	37	0	0
2145	20	0.00245	20	0	0
1157	17	0.00209	17	0	0
1697	16	0.00196	16	0	0
2634	16	0.00196	16	0	0
1590	13	0.00160	13	0	0
1148	12	0.00147	12	0	0
2978	12	0.00147	12	0	0
1788	10	0.00123	10	0	0
6277	10	0.00123	10	0	0
55874	9	0.00110	9	0	0
1093	9	0.00110	9	0	0
4768	8	0.00098	8	0	0
4332	8	0.00098	8	0	0
2518	8	0.00098	8	0	0
3066	7	0.00086	7	0	0
1260	7	0.00086	7	0	0
3564	7	0.00086	7	0	0
3729	7	0.00086	7	0	0
1136	7	0.00086	7	0	0
4398	6	0.00074	6	0	0
4424	6	0.00074	6	0	0
9462	6	0.00074	6	0	0
57926	6	0.00074	6	0	0
2685	6	0.00074	6	0	0
2905	6	0.00074	6	0	0
32898	6	0.00074	6	0	0
3880	6	0.00074	6	0	0

DEST PORT	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL

```
25                    7823  0.96011       7823          0          0
113                    104  0.01276        103          1          0
40627                   70  0.00859         70          0          0
43879                   53  0.00650         53          0          0
443                     11  0.00135         11          0          0
21                      10  0.00123          6          4          0
25459                   10  0.00123         10          0          0
23                       8  0.00098          8          0          0
9704                     3  0.00037          1          1          1
53                       3  0.00037          1          2          0
34171                    3  0.00037          3          0          0
8765                     3  0.00037          3          0          0
22346                    2  0.00025          2          0          0
53259                    2  0.00025          2          0          0
27374                    2  0.00025          0          2          0
1955                     2  0.00025          2          0          0
47626                    2  0.00025          2          0          0
22578                    2  0.00025          2          0          0
44223                    2  0.00025          2          0          0
15276                    1  0.00012          1          0          0
39859                    1  0.00012          1          0          0
35876                    1  0.00012          1          0          0
33995                    1  0.00012          1          0          0
49453                    1  0.00012          1          0          0
21555                    1  0.00012          1          0          0
35505                    1  0.00012          1          0          0
33912                    1  0.00012          1          0          0
35381                    1  0.00012          1          0          0
41834                    1  0.00012          1          0          0
55542                    1  0.00012          1          0          0
41386                    1  0.00012          1          0          0
44861                    1  0.00012          1          0          0
41901                    1  0.00012          1          0          0
43665                    1  0.00012          1          0          0
44082                    1  0.00012          1          0          0
39429                    1  0.00012          1          0          0
1145                     1  0.00012          1          0          0
37566                    1  0.00012          1          0          0
1245                     1  0.00012          1          0          0
64855                    1  0.00012          1          0          0
2255                     1  0.00012          1          0          0
2256                     1  0.00012          1          0          0
1960                     1  0.00012          1          0          0
2258                     1  0.00012          1          0          0
1583                     1  0.00012          1          0          0
1585                     1  0.00012          1          0          0
17341                    1  0.00012          1          0          0
22690                    1  0.00012          1          0          0
9088                     1  0.00012          0          1          0
-------------------------------------------------------------------------
-------------------------------------------------------------------------
total number of events from all 3 data file types = 8148
total number of unique source IPs                 = 45
total number of unique source ports               = 337
total number of unique destination IPs            = 27
total number of unique destination ports          = 52
```

Appendix 5: Output From Running Modified AnalyzeALL - Looking For Source Net 212.179

```
string = 212.179
 212.179 IS present in ALERTS files
 212.179 IS present in SCANS files
 212.179 IS present in LOGS files
-------------------------------------------------------------------------
from ALERT Files:
     30997 Watchlist 000220 IL-ISDNNET-990517
        11 PORTSCAN DETECTED
         4 SYN-FIN scan!
         1 WinGate 1080 Attempt
-------------------------------------------------------------------------
from SCAN Files:
         8  SYN **S*****
         3  SYNFIN **SF****
         1  INVALIDACK ***FRPAU
         1  NOACK *1**RP** RESERVEDBITS
         1  VECNA *1*F*P** RESERVEDBITS
         1  NOACK 2***RP** RESERVEDBITS
         1  NOACK *1*FR**U RESERVEDBITS
         1  UNKNOWN *1*F**A* RESERVEDBITS
         1   INVALIDACK 21S*RPA* RESERVEDBITS
-------------------------------------------------------------------------
SOURCE IP             TOTAL  FRACTION      ALERTS      SCANS      LOGS     SOURCE NAME
                       ALL    OF ALL       FILES      FILES      FILES
                      FILES   FILES        TOTAL      TOTAL      TOTAL

212.179.95.5           6117  0.19711       6117          0          0     cable-95005.bezeqint.net
212.179.27.6           4014  0.12934       4012          2          0     clnt-27006.bezeqint.net
212.179.79.2           3950  0.12728       3950          0          0
212.179.44.115         3938  0.12689       3938          0          0     bzq-44-115.bezeqint.net
212.179.72.226         1591  0.05127       1591          0          0
212.179.41.24          1362  0.04389       1357          5          0     fr-c41024.bezeqint.net
212.179.45.81           950  0.03061        950          0          0     fr-c27081.bezeqint.net
```

212.179.66.2	729	0.02349	729	0	0	PT712002.bezeqint.net
212.179.44.66	667	0.02149	667	0	0	bzq-44-66.bezeqint.net
212.179.29.170	648	0.02088	648	0	0	clnt-29170.bezeqint.net
212.179.95.26	625	0.02014	625	0	0	cable-95026.bezeqint.net
212.179.7.58	589	0.01898	589	0	0	clnt-7058.bezeqint.net
212.179.30.113	579	0.01866	579	0	0	clnt-30113.bezeqint.net
212.179.15.122	564	0.01817	564	0	0	clnt-15122.bezeqint.net
212.179.50.77	505	0.01627	505	0	0	fr-c50077.bezeqint.net
212.179.24.136	475	0.01531	475	0	0	clnt-24136.bezeqint.net
212.179.56.5	439	0.01415	439	0	0	
212.179.23.95	416	0.01340	416	0	0	clnt-23095.bezeqint.net
212.179.45.241	402	0.01295	402	0	0	fr-c27241.bezeqint.net
212.179.58.191	366	0.01179	366	0	0	
212.179.95.45	349	0.01125	349	0	0	cable-95045.bezeqint.net
212.179.7.36	268	0.00864	268	0	0	clnt-7036.bezeqint.net
212.179.19.134	215	0.00693	215	0	0	clnt-19134.bezeqint.net
212.179.27.111	213	0.00686	213	0	0	clnt-27111.bezeqint.net
212.179.16.228	192	0.00619	192	0	0	clnt-16228.bezeqint.net
212.179.45.79	172	0.00554	172	0	0	fr-c27079.bezeqint.net
212.179.34.194	144	0.00464	144	0	0	clnt-34194.bezeqint.net
212.179.127.25	129	0.00416	129	0	0	bzq-128-25.bezeqint.net
212.179.44.106	84	0.00271	84	0	0	bzq-44-106.bezeqint.net
212.179.125.92	61	0.00197	61	0	0	bzq-125-92.bezeqint.net
212.179.39.194	50	0.00161	50	0	0	clnt-39194.bezeqint.net
212.179.33.242	47	0.00151	47	0	0	PT10-33242.bezeqint.net
212.179.44.114	45	0.00145	45	0	0	bzq-44-114.bezeqint.net
212.179.126.227	42	0.00135	42	0	0	cable-95227.bezeqint.net
212.179.42.80	14	0.00045	14	0	0	fr-c42080.bezeqint.net
212.179.42.95	8	0.00026	8	0	0	fr-c42095.bezeqint.net
212.179.175.109	5	0.00016	5	0	0	
212.179.38.200	4	0.00013	4	0	0	clnt-38200.bezeqint.net
212.179.64.189	4	0.00013	4	0	0	PT712189.bezeqint.net
212.179.125.114	4	0.00013	4	0	0	bzq-125-114.bezeqint.net
212.179.42.71	3	0.00010	3	0	0	fr-c42071.bezeqint.net
212.179.33.254	3	0.00010	3	0	0	PT10-33254.bezeqint.net
212.179.29.213	3	0.00010	3	0	0	clnt-29213.bezeqint.net
212.179.41.137	3	0.00010	3	0	0	fr-c41137.bezeqint.net
212.179.77.49	3	0.00010	3	0	0	
212.179.95.16	3	0.00010	3	0	0	cable-95016.bezeqint.net
212.179.41.148	2	0.00006	2	0	0	fr-c41148.bezeqint.net
212.179.41.226	2	0.00006	2	0	0	fr-c41226.bezeqint.net
212.179.29.196	2	0.00006	2	0	0	clnt-29196.bezeqint.net
212.179.67.29	2	0.00006	2	0	0	
212.179.175.216	1	0.00003	1	0	0	
212.179.45.82	1	0.00003	1	0	0	fr-c27082.bezeqint.net
212.179.125.105	1	0.00003	1	0	0	bzq-125-105.bezeqint.net
212.179.30.74	1	0.00003	1	0	0	clnt-30074.bezeqint.net
212.179.42.2	1	0.00003	1	0	0	fr-c42002.bezeqint.net
212.179.45.76	1	0.00003	1	0	0	fr-c27076.bezeqint.net
212.179.45.72	1	0.00003	1	0	0	fr-c27072.bezeqint.net
212.179.67.186	1	0.00003	1	0	0	
212.179.27.189	1	0.00003	1	0	0	clnt-27189.bezeqint.net
212.179.48.199	1	0.00003	1	0	0	fr-c48199.bezeqint.net.48.179.212.IN-ADDR.ARPA
212.179.63.10	1	0.00003	1	0	0	
212.179.45.69	1	0.00003	1	0	0	fr-c27069.bezeqint.net
212.179.79.115	1	0.00003	1	0	0	

DEST IP	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.211.146	4810	0.15499	4810	0	0
MY.NET.223.98	3938	0.12689	3938	0	0
MY.NET.206.90	3916	0.12618	3914	2	0
MY.NET.203.142	1638	0.05278	1638	0	0
MY.NET.218.142	1459	0.04701	1459	0	0
MY.NET.214.170	1358	0.04376	1353	5	0
MY.NET.202.22	950	0.03061	950	0	0
MY.NET.201.174	796	0.02565	796	0	0
MY.NET.214.74	667	0.02149	667	0	0
MY.NET.209.106	648	0.02088	648	0	0
MY.NET.221.146	638	0.02056	638	0	0
MY.NET.223.254	625	0.02014	625	0	0
MY.NET.211.178	609	0.01962	609	0	0
MY.NET.15.215	579	0.01866	579	0	0
MY.NET.227.190	564	0.01817	564	0	0
MY.NET.203.206	505	0.01627	505	0	0
MY.NET.98.181	500	0.01611	500	0	0
MY.NET.225.58	475	0.01531	475	0	0
MY.NET.220.190	433	0.01395	433	0	0
MY.NET.203.118	430	0.01386	430	0	0
MY.NET.207.14	408	0.01315	408	0	0
MY.NET.207.158	366	0.01179	366	0	0
MY.NET.204.34	361	0.01163	361	0	0
MY.NET.206.106	292	0.00941	292	0	0
MY.NET.208.194	290	0.00934	290	0	0
MY.NET.225.38	274	0.00883	274	0	0
MY.NET.225.82	260	0.00838	260	0	0
MY.NET.208.190	257	0.00828	257	0	0
MY.NET.226.130	243	0.00783	243	0	0
MY.NET.201.98	220	0.00709	220	0	0
MY.NET.205.170	214	0.00690	214	0	0
MY.NET.201.238	196	0.00632	196	0	0
MY.NET.202.206	163	0.00525	163	0	0
MY.NET.146.68	147	0.00474	147	0	0
MY.NET.53.95	144	0.00464	144	0	0
MY.NET.222.54	143	0.00461	143	0	0
MY.NET.253.41	141	0.00454	141	0	0

MY.NET.201.130	127	0.00409	127	0	0
MY.NET.211.126	126	0.00406	126	0	0
MY.NET.253.43	126	0.00406	126	0	0
MY.NET.202.202	125	0.00403	125	0	0
MY.NET.205.134	115	0.00371	115	0	0
MY.NET.224.194	104	0.00335	104	0	0
MY.NET.222.250	61	0.00197	61	0	0
MY.NET.209.202	56	0.00180	56	0	0
MY.NET.213.170	47	0.00151	47	0	0
MY.NET.218.78	45	0.00145	45	0	0
MY.NET.208.142	44	0.00142	44	0	0
MY.NET.217.222	44	0.00142	44	0	0

SOURCE PORT	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
1067	2699	0.08697	2699	0	0
6699	1855	0.05977	1855	0	0
1498	1819	0.05861	1819	0	0
1574	1725	0.05558	1725	0	0
13270	1459	0.04701	1459	0	0
32685	1409	0.04540	1409	0	0
1031	1359	0.04379	1354	5	0
1192	1344	0.04331	1344	0	0
1057	1239	0.03992	1239	0	0
2078	1088	0.03506	1087	1	0
1167	950	0.03061	950	0	0
1263	784	0.02526	784	0	0
1271	782	0.02520	782	0	0
2118	673	0.02169	673	0	0
1090	667	0.02149	667	0	0
10120	609	0.01962	609	0	0
1254	589	0.01898	589	0	0
2100	564	0.01817	564	0	0
55021	505	0.01627	505	0	0
7281	500	0.01611	500	0	0
1220	475	0.01531	475	0	0
2637	402	0.01295	402	0	0
3551	366	0.01179	366	0	0
1578	349	0.01125	349	0	0
43526	348	0.01121	348	0	0
48166	290	0.00934	290	0	0
50022	260	0.00838	260	0	0
1197	257	0.00828	257	0	0
1030	245	0.00789	245	0	0
20614	241	0.00777	241	0	0
58794	229	0.00738	229	0	0
25277	220	0.00709	220	0	0
3633	215	0.00693	215	0	0
23193	214	0.00690	214	0	0
2369	213	0.00686	213	0	0
4767	196	0.00632	196	0	0
43527	195	0.00628	195	0	0
1033	185	0.00596	185	0	0
43531	182	0.00586	182	0	0
1203	173	0.00557	173	0	0
1889	172	0.00554	172	0	0
61832	171	0.00551	171	0	0
2696	165	0.00532	165	0	0
61871	147	0.00474	147	0	0
4656	144	0.00464	144	0	0
1306	127	0.00409	127	0	0
1138	125	0.00403	125	0	0
61282	121	0.00390	121	0	0
2182	120	0.00387	120	0	0

DEST PORT	TOTAL ALL FILES	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
6699	9697	0.31246	9692	5	0
4619	5734	0.18477	5733	1	0
4922	4811	0.15502	4811	0	0
6688	3255	0.10488	3255	0	0
4990	1459	0.04701	1459	0	0
1069	648	0.02088	648	0	0
1255	625	0.02014	625	0	0
1476	579	0.01866	579	0	0
6346	437	0.01408	437	0	0
4968	418	0.01347	418	0	0
6700	366	0.01179	366	0	0
25	308	0.00992	308	0	0
4410	290	0.00934	290	0	0
4752	260	0.00838	260	0	0
4722	257	0.00828	257	0	0
4545	243	0.00783	243	0	0
4191	217	0.00699	217	0	0
4519	174	0.00561	174	0	0
4780	163	0.00525	163	0	0
8311	144	0.00464	144	0	0
4433	126	0.00406	126	0	0
4980	125	0.00403	125	0	0
4546	115	0.00371	115	0	0
4341	104	0.00335	104	0	0
4342	59	0.00190	59	0	0
4681	56	0.00180	56	0	0
4134	47	0.00151	47	0	0

```
4739                    44  0.00142         44          0          0
4468                    44  0.00142         44          0          0
4772                    29  0.00093         29          0          0
4764                    22  0.00071         22          0          0
4743                    12  0.00039         12          0          0
4039                    11  0.00035         11          0          0
4515                     8  0.00026          8          0          0
21                       7  0.00023          2          4          1
4470                     6  0.00019          6          0          0
4863                     6  0.00019          6          0          0
4337                     6  0.00019          6          0          0
27374                    5  0.00016          1          3          1
4992                     5  0.00016          5          0          0
13198                    5  0.00016          5          0          0
4707                     4  0.00013          4          0          0
4108                     4  0.00013          4          0          0
4592                     4  0.00013          4          0          0
4171                     4  0.00013          4          0          0
4818                     3  0.00010          3          0          0
4017                     3  0.00010          3          0          0
4564                     3  0.00010          3          0          0
4447                     3  0.00010          3          0          0
------------------------------------------------------------------------
------------------------------------------------------------------------
total number of events from all 3 data file types = 31034
total number of unique source IPs                 = 63
total number of unique source ports               = 219
total number of unique destination IPs            = 110
total number of unique destination ports          = 97
```

Appendix 6: Output From Running Modified AnalyzeALL - Looking For Destination IP MY.NET.220.2

```
string = MY.NET.220.2
 MY.NET.220.2 IS present in ALERTS files
 MY.NET.220.2 IS present in SCANS files
 MY.NET.220.2 NOT in LOGS files
------------------------------------------------------------------------
from ALERT Files:
         5 WinGate 1080 Attempt
         1 SYN-FIN scan!
------------------------------------------------------------------------
from SCAN Files:
     11916  SYN **S*****
         9  UDP
         1  SYNFIN **SF****
------------------------------------------------------------------------
SOURCE IP              ALL   FRACTION      ALERTS     SCANS      LOGS     SOURCE NAME
                      FILES   OF ALL       FILES      FILES      FILES
                      TOTAL   FILES        TOTAL      TOTAL      TOTAL

194.244.78.145       11904  0.99765          0      11904          0
195.245.183.76           5  0.00042          0          5          0
195.149.21.65            4  0.00034          0          4          0
209.212.128.47           2  0.00017          2          0          0     watto.fdt.net
130.225.136.39           2  0.00017          0          2          0     obelix.bmb.sdu.dk
160.78.49.191            2  0.00017          1          1          0     ema.chim.unipr.it
12.105.34.10             1  0.00008          0          1          0
209.191.146.4            1  0.00008          1          0          0     shell.25bway.compuhelp.com
62.157.23.237            1  0.00008          0          1          0     p3E9D17ED.dip.t-dialin.net
66.9.27.254              1  0.00008          0          1          0
64.50.161.162            1  0.00008          0          1          0     public.washingtonhomes.com
63.206.212.112           1  0.00008          0          1          0     adsl-63-206-212-112.dsl.snfc21.pacbell.net
195.247.65.216           1  0.00008          0          1          0     port216.duesseldorf.ivm.de
24.43.30.182             1  0.00008          0          1          0     cr283564-a.brntfd1.on.wave.home.com
62.155.244.68            1  0.00008          0          1          0     p3E9BF444.dip.t-dialin.net
128.211.237.11           1  0.00008          0          1          0     cary-b-011.resnet.purdue.edu
63.94.12.5               1  0.00008          1          0          0     offramp.i2k.com
212.46.76.30             1  0.00008          1          0          0
63.88.175.201            1  0.00008          0          1          0     www.multilateral.com
------------------------------------------------------------------------
DEST IP                ALL   FRACTION      ALERTS     SCANS      LOGS
                      FILES   OF ALL       FILES      FILES      FILES
                      TOTAL   FILES        TOTAL      TOTAL      TOTAL

MY.NET.220.2         11932  1.00000          6      11926          0
------------------------------------------------------------------------
SOURCE PORT            ALL   FRACTION      ALERTS     SCANS      LOGS
                      FILES   OF ALL       FILES      FILES      FILES
                      TOTAL   FILES        TOTAL      TOTAL      TOTAL

27025                    3  0.00025          0          3          0
17066                    3  0.00025          0          3          0
31643                    3  0.00025          0          3          0
14735                    3  0.00025          0          3          0
27781                    3  0.00025          0          3          0
31213                    3  0.00025          0          3          0
26229                    3  0.00025          0          3          0
27373                    3  0.00025          0          3          0
26580                    3  0.00025          0          3          0
26436                    3  0.00025          0          3          0
21352                    3  0.00025          0          3          0
21315                    3  0.00025          0          3          0
```

20486	2	0.00017	0	2	0
34999	2	0.00017	0	2	0
29852	2	0.00017	0	2	0
29854	2	0.00017	0	2	0
27698	2	0.00017	0	2	0
32002	2	0.00017	0	2	0
29860	2	0.00017	0	2	0
26958	2	0.00017	0	2	0
24795	2	0.00017	0	2	0
25495	2	0.00017	0	2	0
27680	2	0.00017	0	2	0
25494	2	0.00017	0	2	0
35690	2	0.00017	0	2	0
18920	2	0.00017	0	2	0
25464	2	0.00017	0	2	0
26938	2	0.00017	0	2	0
33483	2	0.00017	0	2	0
25463	2	0.00017	0	2	0
28378	2	0.00017	0	2	0
33438	2	0.00017	0	2	0
28359	2	0.00017	0	2	0
29755	2	0.00017	0	2	0
20385	2	0.00017	0	2	0
29883	2	0.00017	0	2	0
29884	2	0.00017	0	2	0
20377	2	0.00017	0	2	0
27621	2	0.00017	0	2	0
29076	2	0.00017	0	2	0
27609	2	0.00017	0	2	0
20300	2	0.00017	0	2	0
23997	2	0.00017	0	2	0
35625	2	0.00017	0	2	0
29050	2	0.00017	0	2	0
29890	2	0.00017	0	2	0
35612	2	0.00017	0	2	0
29051	2	0.00017	0	2	0
16668	2	0.00017	0	2	0

DEST PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
21	5	0.00042	0	5	0
1080	5	0.00042	5	0	0
12365	3	0.00025	0	3	0
12157	3	0.00025	0	3	0
17140	3	0.00025	0	3	0
670	3	0.00025	0	3	0
2996	3	0.00025	0	3	0
13709	3	0.00025	0	3	0
13302	3	0.00025	0	3	0
7280	3	0.00025	0	3	0
7243	3	0.00025	0	3	0
12508	3	0.00025	0	3	0
17569	3	0.00025	0	3	0
12466	2	0.00017	0	2	0
13196	2	0.00017	0	2	0
10271	2	0.00017	0	2	0
19632	2	0.00017	0	2	0
13166	2	0.00017	0	2	0
13163	2	0.00017	0	2	0
20453	2	0.00017	0	2	0
12436	2	0.00017	0	2	0
11708	2	0.00017	0	2	0
10253	2	0.00017	0	2	0
1393	2	0.00017	0	2	0
20405	2	0.00017	0	2	0
6407	2	0.00017	0	2	0
10238	2	0.00017	0	2	0
7873	2	0.00017	0	2	0
2098	2	0.00017	0	2	0
7139	2	0.00017	0	2	0
7867	2	0.00017	0	2	0
1367	2	0.00017	0	2	0
7863	2	0.00017	0	2	0
8591	2	0.00017	0	2	0
10221	2	0.00017	0	2	0
12472	2	0.00017	0	2	0
1354	2	0.00017	0	2	0
10200	2	0.00017	0	2	0
17474	2	0.00017	0	2	0
16744	2	0.00017	0	2	0
17473	2	0.00017	0	2	0
9283	2	0.00017	0	2	0
17451	2	0.00017	0	2	0
8540	2	0.00017	0	2	0
11748	2	0.00017	0	2	0
7804	2	0.00017	0	2	0
7802	2	0.00017	0	2	0
17407	2	0.00017	0	2	0
21883	2	0.00017	0	2	0
10991	2	0.00017	0	2	0

total number of events from all 3 data file types = 11932
total number of unique source IPs = 19
total number of unique source ports = 10459
total number of unique destination IPs = 1

total number of unique destination ports = 10454

Appendix 7: Output From Running Modified AnalyzeALL - Looking For SYN-FIN Scans

```
------------------------------------------------------------------
Looking For SYN-FIN scans only
------------------------------------------------------------------
  SYN-FIN         is present in ALERTS files
  SYNFIN **SF**** is present in SCANS files
  **SF***         is present in LOGS files
------------------------------------------------------------------
from ALERT Files:
     56250  1.00000  SYN-FIN scan!
------------------------------------------------------------------
from SCAN Files:
     50523  1.00000   SYNFIN **SF****
------------------------------------------------------------------
```

SOURCE IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL	SOURCE NAME
208.61.4.207	21700	0.13082	6635	6634	8431	adsl-61-4-207.mia.bellsouth.net
209.92.40.32	15673	0.09448	4967	4956	5750	dslcv1-32.fast.net
160.78.49.191	14381	0.08670	7199	7182	0	ema.chim.unipr.it
130.89.229.48	13271	0.08000	3860	3860	5551	cal032044.student.utwente.nl
203.32.161.197	11601	0.06994	3545	3545	4511	adnet.imgserv.com
210.113.89.200	11361	0.06849	3572	3565	4224	
193.64.114.10	10875	0.06556	3295	3288	4292	net10.printeq.fi
195.103.69.159	10547	0.06358	3292	3287	3968	proxy.guest.net
63.195.56.20	8646	0.05212	3897	0	4749	adsl-63-195-56-20.dsl.snfc21.pacbell.net
210.101.101.110	8414	0.05072	2582	2578	3254	
212.0.107.107	7775	0.04687	2338	2334	3103	
213.41.69.52	6790	0.04093	3399	3391	0	hosting-52.69.rev.fr.colt.net
63.167.58.13	5801	0.03497	1531	1531	2739	
143.89.13.3	5338	0.03218	1584	1584	2170	ustlnx6.ust.hk
163.10.19.34	4250	0.02562	1105	1105	2040	decanato.exactas.unlp.edu.ar
128.2.81.133	3641	0.02195	1569	0	2072	8TH-DWARF.REM.CMU.EDU
212.187.21.156	3303	0.01991	1085	1082	1136	c21156.upc-c.chello.nl
211.46.110.81	671	0.00405	276	276	119	
139.130.61.206	626	0.00377	267	0	359	alphac.lnk.telstra.net
63.71.23.4	528	0.00318	0	264	264	athena.eiic.com
202.153.112.222	457	0.00276	186	0	271	
24.7.227.215	170	0.00102	51	51	68	c921627-a.alntn1.tx.home.com
62.96.171.103	9	0.00005	6	3	0	m-dialin-583.addcom.de
MY.NET.181.131	4	0.00002	0	0	4	
MY.NET.217.194	3	0.00002	0	0	3	
212.177.241.101	3	0.00002	1	1	1	
129.130.98.92	2	0.00001	1	1	0	rn-098-092.reshall.k-state.net
MY.NET.219.2	2	0.00001	0	0	2	
24.65.121.98	2	0.00001	1	1	0	h24-65-121-98.ss.shawcable.net
MY.NET.224.2	2	0.00001	0	0	2	
129.93.206.170	2	0.00001	1	1	0	pcp008790pcs.unl.edu
24.112.51.119	2	0.00001	1	1	0	cr1021515-c.lndn1.on.wave.home.com
212.120.113.229	2	0.00001	0	0	2	CC5693-a.ensch1.ov.nl.home.com
129.101.18.16	2	0.00001	2	0	0	PC008144.reshall.uidaho.edu
MY.NET.218.106	2	0.00001	0	0	2	
193.237.127.49	2	0.00001	0	1	1	ffoo.demon.co.uk
MY.NET.218.182	2	0.00001	0	0	2	
164.8.21.101	2	0.00001	0	0	2	
MY.NET.217.222	1	0.00001	0	0	1	
MY.NET.209.110	1	0.00001	0	0	1	
MY.NET.226.234	1	0.00001	0	0	1	
141.30.234.236	1	0.00001	0	0	1	xwums-102aa.wh18.tu-dresden.de
24.200.140.155	1	0.00001	1	0	0	modemcable155.140-200-24.mtl.mc.videotron.ca
198.144.202.250	1	0.00001	0	0	1	drunken.raving.linuxfreaks.org
MY.NET.229.10	1	0.00001	0	0	1	
129.241.139.224	1	0.00001	0	0	1	s224b.studby.ntnu.no
212.185.235.7	1	0.00001	0	1	0	pD4B9EB07.dip.t-dialin.net
MY.NET.150.139	1	0.00001	0	0	1	
MY.NET.100.149	1	0.00001	0	0	1	
211.188.156.72	1	0.00001	0	0	1	
24.112.198.166	1	0.00001	0	0	1	cr995732-a.pr1.on.wave.home.com
MY.NET.208.82	1	0.00001	0	0	1	
MY.NET.220.142	1	0.00001	0	0	1	
MY.NET.219.18	1	0.00001	0	0	1	
24.112.150.20	1	0.00001	1	0	0	cr518339-a.wlfdle1.on.wave.home.com
62.155.175.124	1	0.00001	0	0	1	p3E9BAF7C.dip.t-dialin.net

DEST IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
MY.NET.223.251	27	0.00016	10	8	9
MY.NET.224.79	25	0.00015	8	8	9
MY.NET.253.82	23	0.00014	8	8	7
MY.NET.1.167	23	0.00014	8	6	9
MY.NET.106.204	22	0.00013	7	8	7
MY.NET.104.90	22	0.00013	8	8	6
MY.NET.207.9	22	0.00013	7	7	8
MY.NET.215.165	22	0.00013	7	7	8
MY.NET.1.88	22	0.00013	8	7	7
MY.NET.232.31	21	0.00013	7	7	7

MY.NET.213.120	21	0.00013	7	7	7
MY.NET.224.98	21	0.00013	7	7	7
MY.NET.70.84	21	0.00013	8	7	6
MY.NET.221.233	21	0.00013	8	7	6
MY.NET.231.155	20	0.00012	7	6	7
MY.NET.198.219	20	0.00012	7	7	6
MY.NET.232.44	20	0.00012	7	7	6
MY.NET.98.131	20	0.00012	7	7	6
MY.NET.217.166	20	0.00012	7	7	6
MY.NET.190.65	20	0.00012	7	6	7
MY.NET.206.178	20	0.00012	7	6	7
MY.NET.204.129	20	0.00012	7	7	6
MY.NET.68.220	20	0.00012	7	7	6
MY.NET.224.242	19	0.00011	7	7	5
MY.NET.140.27	19	0.00011	7	6	6
MY.NET.188.233	19	0.00011	7	6	6
MY.NET.214.200	19	0.00011	6	6	7
MY.NET.212.12	19	0.00011	7	6	6
MY.NET.100.140	19	0.00011	6	7	6
MY.NET.154.154	19	0.00011	6	6	7
MY.NET.212.211	19	0.00011	7	5	7
MY.NET.229.245	19	0.00011	6	6	7
MY.NET.204.53	19	0.00011	6	6	7
MY.NET.232.241	19	0.00011	7	7	5
MY.NET.182.159	19	0.00011	6	6	7
MY.NET.206.236	19	0.00011	6	5	8
MY.NET.120.19	19	0.00011	6	6	7
MY.NET.216.189	19	0.00011	6	6	7
MY.NET.224.81	19	0.00011	7	6	6
MY.NET.207.203	19	0.00011	7	6	6
MY.NET.157.55	19	0.00011	6	6	7
MY.NET.214.244	19	0.00011	7	6	6
MY.NET.158.5	19	0.00011	6	6	7
MY.NET.201.95	19	0.00011	7	6	6
MY.NET.75.83	19	0.00011	7	5	7
MY.NET.13.164	18	0.00011	6	6	6
MY.NET.158.117	18	0.00011	6	6	6
MY.NET.190.46	18	0.00011	7	6	5
MY.NET.232.61	18	0.00011	6	6	6
MY.NET.203.156	18	0.00011	6	5	7

SOURCE PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
21	55900	0.33699	19613	14207	22080
53	51312	0.30933	18273	18247	14792
9704	45787	0.27602	14184	14168	17435
27374	11361	0.06849	3572	3565	4224
4	841	0.00507	327	327	187
109	626	0.00377	267	0	359
6699	11	0.00007	6	3	2
17664	2	0.00001	0	1	1
1084	2	0.00001	0	0	2
1065	2	0.00001	1	1	0
1675	2	0.00001	0	0	2
2568	2	0.00001	1	1	0
1	2	0.00001	0	0	2
1264	2	0.00001	1	1	0
2552	2	0.00001	1	1	0
2922	1	0.00001	1	0	0
2384	1	0.00001	0	0	1
1698	1	0.00001	0	0	1
17777	1	0.00001	0	0	1
1455	1	0.00001	0	0	1
23	1	0.00001	0	0	1
1082	1	0.00001	0	0	1
1226	1	0.00001	0	0	1
6688	1	0.00001	0	0	1
1094	1	0.00001	0	0	1
67	1	0.00001	0	0	1
73	1	0.00001	0	0	1
1102	1	0.00001	0	0	1
8311	1	0.00001	0	0	1
2420	1	0.00001	0	0	1
1382	1	0.00001	0	0	1
0	1	0.00001	0	0	1
1560	1	0.00001	0	1	0
1268	1	0.00001	0	0	1
2916	1	0.00001	1	0	0
210	1	0.00001	0	0	1
1212	1	0.00001	0	0	1
1030	1	0.00001	1	0	0
1686	1	0.00001	0	0	1
156	1	0.00001	1	0	0
199	1	0.00001	0	0	1

DEST PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
21	55900	0.33699	19613	14207	22080
53	51312	0.30933	18273	18247	14792
9704	45787	0.27602	14184	14168	17435
27374	11361	0.06849	3572	3565	4224
23	841	0.00507	327	327	187
109	626	0.00377	267	0	359
6699	11	0.00007	5	3	3

```
3106                      9  0.00005          6          3          0
119                       8  0.00005          0          0          8
6688                      4  0.00002          0          0          4
5190                      2  0.00001          0          0          2
226                       2  0.00001          0          1          1
2099                      2  0.00001          1          1          0
8311                      1  0.00001          0          0          1
1507                      1  0.00001          0          0          1
4810                      1  0.00001          0          0          1
1180                      1  0.00001          1          0          0
2176                      1  0.00001          0          0          1
1307                      1  0.00001          0          0          1
4                         1  0.00001          0          0          1
2774                      1  0.00001          0          0          1
1134                      1  0.00001          0          0          1
80                        1  0.00001          0          0          1
1056                      1  0.00001          0          0          1
4968                      1  0.00001          0          1          0
1944                      1  0.00001          1          0          0
4078                      1  0.00001          0          0          1
1842                      1  0.00001          0          0          1
-------------------------------------------------------------------------
-------------------------------------------------------------------------
total number of events from all 3 data file types = 165880
total number of unique source IPs                 = 56
total number of unique source ports               = 41
total number of unique destination IPs            = 27440
total number of unique destination ports          = 28
```

Appendix 8: Output From Running Modified AnalyzeALL - Looking For Crafted Packets From MY.NET

```
search = MY.NET as source IP for crafted packets

  NOT in ALERTS files
  NOT in SCANS files
  IS present in LOGS files
-------------------------------------------------------------------------
from ALERT Files:
-------------------------------------------------------------------------
from SCAN Files:
-------------------------------------------------------------------------
SOURCE IP             ALL    FRACTION       ALERTS      SCANS       LOGS     SOURCE NAME
                     FILES    OF ALL        FILES       FILES       FILES
                     TOTAL    FILES         TOTAL       TOTAL       TOTAL

MY.NET.218.106          92  0.30769           0           0          92
MY.NET.217.194          33  0.11037           0           0          33
MY.NET.224.2            32  0.10702           0           0          32
MY.NET.220.142          24  0.08027           0           0          24
MY.NET.219.2            16  0.05351           0           0          16
MY.NET.203.150          14  0.04682           0           0          14
MY.NET.203.198           8  0.02676           0           0           8
MY.NET.211.130           7  0.02341           0           0           7
MY.NET.213.138           6  0.02007           0           0           6
MY.NET.201.14            5  0.01672           0           0           5
MY.NET.209.110           5  0.01672           0           0           5
MY.NET.208.82            4  0.01338           0           0           4
MY.NET.181.131           4  0.01338           0           0           4
MY.NET.214.142           3  0.01003           0           0           3
MY.NET.202.66            3  0.01003           0           0           3
MY.NET.217.222           3  0.01003           0           0           3
MY.NET.227.186           2  0.00669           0           0           2
MY.NET.219.18            2  0.00669           0           0           2
MY.NET.227.150           2  0.00669           0           0           2
MY.NET.218.182           2  0.00669           0           0           2
MY.NET.213.90            2  0.00669           0           0           2
MY.NET.208.234           1  0.00334           0           0           1
MY.NET.221.210           1  0.00334           0           0           1
MY.NET.218.6             1  0.00334           0           0           1
MY.NET.224.206           1  0.00334           0           0           1
MY.NET.221.6             1  0.00334           0           0           1
MY.NET.204.18            1  0.00334           0           0           1
MY.NET.227.110           1  0.00334           0           0           1
MY.NET.220.34            1  0.00334           0           0           1
MY.NET.222.94            1  0.00334           0           0           1
MY.NET.225.26            1  0.00334           0           0           1
MY.NET.205.206           1  0.00334           0           0           1
MY.NET.201.110           1  0.00334           0           0           1
MY.NET.205.142           1  0.00334           0           0           1
MY.NET.207.194           1  0.00334           0           0           1
MY.NET.220.22            1  0.00334           0           0           1
MY.NET.219.234           1  0.00334           0           0           1
MY.NET.222.22            1  0.00334           0           0           1
MY.NET.225.10            1  0.00334           0           0           1
MY.NET.214.42            1  0.00334           0           0           1
MY.NET.229.10            1  0.00334           0           0           1
MY.NET.226.94            1  0.00334           0           0           1
MY.NET.226.234           1  0.00334           0           0           1
MY.NET.224.62            1  0.00334           0           0           1
MY.NET.219.14            1  0.00334           0           0           1
MY.NET.217.34            1  0.00334           0           0           1
MY.NET.225.54            1  0.00334           0           0           1
```

MY.NET.218.50	1	0.00334	0	0	1
MY.NET.100.149	1	0.00334	0	0	1
MY.NET.219.38	1	0.00334	0	0	1
MY.NET.150.139	1	0.00334	0	0	1

DEST IP	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
207.172.3.46	196	0.65552	0	0	196
129.2.224.108	5	0.01672	0	0	5
205.188.3.194	4	0.01338	0	0	4
24.113.104.105	4	0.01338	0	0	4
163.10.19.34	3	0.01003	0	0	3
208.184.87.88	3	0.01003	0	0	3
200.27.11.181	2	0.00669	0	0	2
129.21.105.31	2	0.00669	0	0	2
134.126.193.61	2	0.00669	0	0	2
64.12.15.17	2	0.00669	0	0	2
137.99.162.73	2	0.00669	0	0	2
205.188.1.95	2	0.00669	0	0	2
205.188.3.207	2	0.00669	0	0	2
129.21.115.141	2	0.00669	0	0	2
205.188.3.192	2	0.00669	0	0	2
152.163.241.80	2	0.00669	0	0	2
206.74.88.215	2	0.00669	0	0	2
205.188.3.203	1	0.00334	0	0	1
128.205.218.221	1	0.00334	0	0	1
209.10.169.42	1	0.00334	0	0	1
204.48.18.116	1	0.00334	0	0	1
205.188.3.201	1	0.00334	0	0	1
64.32.182.114	1	0.00334	0	0	1
134.129.152.33	1	0.00334	0	0	1
128.2.162.68	1	0.00334	0	0	1
208.184.87.73	1	0.00334	0	0	1
129.173.172.216	1	0.00334	0	0	1
199.8.228.115	1	0.00334	0	0	1
192.232.16.70	1	0.00334	0	0	1
63.208.24.181	1	0.00334	0	0	1
192.232.16.79	1	0.00334	0	0	1
64.124.41.226	1	0.00334	0	0	1
205.188.1.91	1	0.00334	0	0	1
128.59.75.216	1	0.00334	0	0	1
146.151.77.78	1	0.00334	0	0	1
24.7.227.215	1	0.00334	0	0	1
203.96.146.134	1	0.00334	0	0	1
168.159.206.138	1	0.00334	0	0	1
152.163.241.65	1	0.00334	0	0	1
128.119.12.31	1	0.00334	0	0	1
152.163.241.87	1	0.00334	0	0	1
209.232.3.99	1	0.00334	0	0	1
141.213.160.222	1	0.00334	0	0	1
24.11.48.83	1	0.00334	0	0	1
147.188.152.131	1	0.00334	0	0	1
64.124.41.232	1	0.00334	0	0	1
168.122.203.78	1	0.00334	0	0	1
131.128.142.149	1	0.00334	0	0	1
207.153.221.169	1	0.00334	0	0	1
205.188.126.6	1	0.00334	0	0	1

SOURCE PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
0	37	0.12375	0	0	37
1226	14	0.04682	0	0	14
1	12	0.04013	0	0	12
1094	11	0.03679	0	0	11
6688	10	0.03344	0	0	10
8311	9	0.03010	0	0	9
3332	9	0.03010	0	0	9
1079	7	0.02341	0	0	7
3043	6	0.02007	0	0	6
255	6	0.02007	0	0	6
1086	5	0.01672	0	0	5
1455	5	0.01672	0	0	5
21	5	0.01672	0	0	5
1698	5	0.01672	0	0	5
1621	5	0.01672	0	0	5
73	4	0.01338	0	0	4
1119	4	0.01338	0	0	4
4785	4	0.01338	0	0	4
10	3	0.01003	0	0	3
70	3	0.01003	0	0	3
1084	3	0.01003	0	0	3
1897	3	0.01003	0	0	3
4765	3	0.01003	0	0	3
1090	3	0.01003	0	0	3
1612	3	0.01003	0	0	3
2420	3	0.01003	0	0	3
34	3	0.01003	0	0	3
4234	3	0.01003	0	0	3
6699	3	0.01003	0	0	3
1547	3	0.01003	0	0	3
4972	3	0.01003	0	0	3
4633	3	0.01003	0	0	3
1560	3	0.01003	0	0	3
2256	3	0.01003	0	0	3

166	2	0.00669	0	0	2
1675	2	0.00669	0	0	2
61	2	0.00669	0	0	2
1479	2	0.00669	0	0	2
1188	2	0.00669	0	0	2
1649	2	0.00669	0	0	2
84	2	0.00669	0	0	2
1102	2	0.00669	0	0	2
1337	2	0.00669	0	0	2
17	2	0.00669	0	0	2
2705	2	0.00669	0	0	2
1087	2	0.00669	0	0	2
1842	2	0.00669	0	0	2
2068	2	0.00669	0	0	2
1706	2	0.00669	0	0	2
2095	1	0.00334	0	0	1

DEST PORT	ALL FILES TOTAL	FRACTION OF ALL FILES	ALERTS FILES TOTAL	SCANS FILES TOTAL	LOGS FILES TOTAL
119	137	0.45819	0	0	137
5190	21	0.07023	0	0	21
8311	9	0.03010	0	0	9
6688	7	0.02341	0	0	7
1698	6	0.02007	0	0	6
21	6	0.02007	0	0	6
1094	5	0.01672	0	0	5
6699	5	0.01672	0	0	5
1226	5	0.01672	0	0	5
1612	4	0.01338	0	0	4
1136	4	0.01338	0	0	4
2420	3	0.01003	0	0	3
1139	3	0.01003	0	0	3
1079	3	0.01003	0	0	3
1706	3	0.01003	0	0	3
4785	3	0.01003	0	0	3
3332	2	0.00669	0	0	2
1270	2	0.00669	0	0	2
2800	2	0.00669	0	0	2
4948	2	0.00669	0	0	2
1560	2	0.00669	0	0	2
443	2	0.00669	0	0	2
1086	2	0.00669	0	0	2
1621	2	0.00669	0	0	2
2705	2	0.00669	0	0	2
1256	2	0.00669	0	0	2
1996	1	0.00334	0	0	1
2687	1	0.00334	0	0	1
1205	1	0.00334	0	0	1
3500	1	0.00334	0	0	1
1207	1	0.00334	0	0	1
1045	1	0.00334	0	0	1
2810	1	0.00334	0	0	1
1281	1	0.00334	0	0	1
1082	1	0.00334	0	0	1
1399	1	0.00334	0	0	1
1479	1	0.00334	0	0	1
1841	1	0.00334	0	0	1
2333	1	0.00334	0	0	1
3937	1	0.00334	0	0	1
3257	1	0.00334	0	0	1
1484	1	0.00334	0	0	1
7777	1	0.00334	0	0	1
1568	1	0.00334	0	0	1
2774	1	0.00334	0	0	1
1635	1	0.00334	0	0	1
4226	1	0.00334	0	0	1
1238	1	0.00334	0	0	1
1516	1	0.00334	0	0	1
1334	1	0.00334	0	0	1

```
total number of events from all 3 data file types = 299
total number of unique source IPs                 = 51
total number of unique source ports               = 112
total number of unique destination IPs            = 79
total number of unique destination ports          = 81
```

Appendix 9: Results of Whois 212.79

```
Whois results:
Input String: 212.179.16.228
Server: whois.ripe.net (Europe)

% Rights restricted by copyright. See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 212.179.16.224 - 212.179.16.239
netname: AEROIAM-LTD
descr: AEROIAM-LAN
country: IL
admin-c: ES4966-RIPE
```

```
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
hostmaster@isdn.net.il 20000503

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
changed: hostmaster@isdn.net.il 19990610

person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
changed: registrar@ns.il 20000309

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
changed: registrar@ns.il 19990902
```

Appendix 10: Results of Whois 159.226

```
Whois results:
Input String: 159.226.5.77
Server: whois.arin.net (North and South America)

The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China

Netname: NCFC
Netnumber: 159.226.0.0

Coordinator:
Qian, Haulin (QH3-ARIN) hlqian@NS.CNC.AC.CN

Domain System inverse mapping provided by:

NS.CNC.AC.CN 159.226.1.1
GINGKO.ICT.AC.CN 159.226.40.1

Record last updated on 25-Jul-1994.
Database last updated on 22-Dec-2000 07:12:08 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced