Global Information Assurance Certification Paper

GIAC Certified Intrusion Analyst – Practical

Wei-Chieh LIM **Network Security 2000**

Assignment 1 - Network Detects (30 Points)

Assignment 2 - Evaluate an Attack (20 Points)

Assignment 3 - "Analyze This" Scenario (20 Points)

Assignment 4 - Analysis Process (20 Points)

Assignment 1- Network Detects (30 Points)

Detect 1

```
[**] IDS028 - PING NMAP TCP [**]
11/07-09:58:26.646757 192.102.197.234:53 -> server1.my.net:53
TCP TTL:47 TOS:0x0 ID:43478
***A**** Seq: 0x356   Ack: 0x0   Win: 0x578

[**] IDS028 - PING NMAP TCP [**]
11/07-09:58:26.599733 192.102.197.234:80 -> server1.my.net:53
TCP TTL:47 TOS:0x0 ID:43476
***A**** Seq: 0x355   Ack: 0x0   Win: 0x578
```

1. Source of trace

Our firewall network.

2. Detect was generated by:

Detect was generated by Snort-1.6.3.

Time stamps are in SGT (GMT +8)

Explanation of fields:

LINE 01: `[**] IDS028 - PING NMAP TCP [**]`
Snort rule which triggered the detect

LINE 02: `11/07-09:58:26.646757 192.102.197.234:53 -> server1.my.net:53`
Date(month/day), time(hh:mm:ss.ms), source IP and port (x.x.x.x.port), destination IP and port (x.x.x.x.port)

LINE 03: `TCP TTL:47 TOS:0x0 ID:43478`
IP protocol type, time-to-live (TTL), type-of-service (TOS), IP identification value (ID)

LINE 04: `***A**** Seq: 0x356   Ack: 0x0   Win: 0x578`
TCP flags, TCP sequence number, TCP acknowledge bit, TCP window size

3. Probability the source address was spoofed

Low since the attacker will want to see the results of the NMAP TCP ping.

4. Description of attack

Correlating the information obtained from tcpdump indicate that it was not a NMAP TCP ping but rather a DNS behavior which deviates from the norm.

This is not a one off incident but occurs every time the www.intel.com authoritative nameservers are queried.

5. Attack mechanism

Our firewall, *server1.my.net* queries the intel.com nameservers for www.intel.com and gets the answer:

```
Authoritative answers can be found from:
geo164a.cps.intel.com   internet address = 192.198.164.170
geo197a.cps.intel.com   internet address = 192.102.197.234
```

server1.my.net then queries 192.102.197.234 for the IP address for www.intel.com and receives an answer.

192.102.197.234 subsequently generates a number of unsolicited request.

- Sends a DNS response to port 37852 on *server1.my.net* with **Type 0** and **Class 0** which are not defined in *RFC 1035 Domain Names – Implementation and specification*.
- Sends an ICMP echo request to *server1.my.net*.
- Sends a **ACK** with a source port 53 to our server1.my.net at destination port 53.
- Similar attempt with source port 80 to destination port 53 was attempted.

Suspect that the DNS software used by the www.intel.com authoritative nameservers are checking to see if similar software is used by other nameservers. This is done with an out-of-specification DNS packet to port 37852 and hoping for a response.

It's possibly trying to do OS fingerprinting by sending **ACK** packets and using port 80 and 53 to circumvent firewalls by appearing as normal DNS and HTTP traffic.

6. Correlations

Information collected from tcpdump indicates that it was not a NMAP TCP ping.

```
15:20:53.332476 server1.my.net.3671 > 192.102.197.234.53: 3335 (31)
15:20:53.730069 192.102.197.234.53 > server1.my.net.3671: 3335*- 1/0/0 (47)
15:20:53.732357 192.102.197.234.53 > server1.my.net.37852: 0 [0q] Type0 (Class 0)? .
(10)
15:20:53.732455 192.102.197.234 > server1.my.net: icmp: echo request
15:20:53.732538 server1.my.net > 192.102.197.234: icmp: server1.my.net udp port 37852
unreachable
15:20:53.732604 server1.my.net > 192.102.197.234: icmp: echo reply
15:20:53.733192 192.102.197.234.53 > server1.my.net.53: . ack 0 win 1400
15:20:53.733342 server1.my.net.53 > 192.102.197.234.53: R 0:0(0) win 0
15:20:53.736488 192.102.197.234.80 > server1.my.net.53: . ack 0 win 1400
15:20:53.737991 server1.my.net.53 > 192.102.197.234.80: R 0:0(0) win 0
```

```
.242.53 > 192.102.197.234.53: R 0:0(0) win 0
15:20:53.736488 192.102.197.234.80 > server1.my.net.53: . ack 0 win 1400
15:20:53.737991 server1.my.net.53 > 192.102.197.234.80: R 0:0(0) win 0
```

Similar traffic was also seen on

http://www.sans.org/y2k/092200.htm

http://www.sans.org/y2k/111000.htm

7. Evidence of active targeting

No evidence of active targeting as the www.intel.com nameservers performs the same checks on any machine sending a request.

8. Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

Criticality	5 (Firewall was targeted)
Lethality	1 (Attack unlikely to succeed)
System Countermeasures	5 (Carefully secured firewall)
Network Countermeasures	3 (Validated restrictive firewall)

Severity = (5 + 1) - (5 + 3) = -2

However, this is unlikely to be an attack.

9. Defensive Recommendation

Router should block outbound ICMP unreachable messages using packet filters so as not to provide too much information.

10. Multiple choice question

What does a TYPE 0 DNS resource record?

a. Address record (A)

b. Name server record (NS)

c. Start of authority (SOA)

d. Undefined

ANSWER: (d) Type 0 is undefined in RFC 1035.

Detect 2

```
11 01 2000 06:15:04.684819 ppp-225.ogertel.com.3579 > My.Net.139.71.8010:
S 4284628:4284628(0) win 8192  (DF)
11 01 2000 06:15:04.695807 ppp-225.ogertel.com.3578 > My.Domain.8010:
S 4284626:4284626(0) win 8192  (DF)
11 01 2000 06:15:04.696849 ppp-225.ogertel.com.3580 > My.Domain.8010:
S 4284629:4284629(0) win 8192  (DF)
11 01 2000 06:15:07.520960 ppp-225.ogertel.com.3579 > My.Net.139.71.8010:
S 4284628:4284628(0) win 8192  (DF)
```

```
11 01 2000 06:15:07.665390 ppp-225.ogertel.com.3580 > My.Domain.8010:
S 4284629:4284629(0) win 8192  (DF)
11 01 2000 06:15:07.715265 ppp-225.ogertel.com.3578 > My.Domain.8010:
S 4284626:4284626(0) win 8192  (DF)
```

1. **Source of trace**

   http://www.sans.org/y2k/110600-1430.htm

2. **Detect was generated by:**

   Detect was generated by tcpdump.

   Explanation of fields:

```
11     01   2000  06:15:04.684819    ppp-225.ogertel.com.3579       >
Month  Day  Year  Time(hh:mm:ss.ms)  source IP and port (x.x.x.x.port)

My.Net.139.71.8010                    :  S          4284628:4284628(0)
destination IP and port (x.x.x.x.port)    TCP flags  TCP sequence number

win 8192         (DF)
TCP window size  Don't fragment bit set
```

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

   Low since the attacker will want to see the results of the probe.

4. **Description of attack**

   The attacker was probing for servers running

   - CommuniGate Pro that provides web management access on port 8010/tcp (default).CommuniGate Pro is a mail server providing SMTP message routing, and POP/IMAP/HTTP access to mail.
   - WinGate provides sharing of a Internet connection for multiple networked and also serves as a firewall. The WinGate Log File service listens on 8010 and allows users to remotely view log files.

   Vulnerabilities in CommuniGate Pro v3.2.4 and earlier was published in the following:

   - CVE-2000-0634

     http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0634
   - BUGTRAQ:20000717

     http://www.securityfocus.com/archive/1/70403
   - S21SEC-003

     http://www.s21sec.com/en/avisos/s21sec-003-en.txt

   Users are able to exploit well-known "../.." web server problem and perform remote command execution as superuser.

   Multiple vulnerabilities exists for WinGate

   - CVE

     http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wingate

- BUGTRAQ

  http://www.securityfocus.com/archive/1/13124

5. Attack mechanism

The attacker was specifically targeting My.Net.139.71 and My.Domain looking for WinGate and CommuniGate servers. Reconnaissance was probably performed earlier to determine that these servers are either mail and/or firewall servers.

6. Correlations

Muliple detects were previously posted on GIAC

- http://www.sans.org/y2k/032100-2000.htm
- http://www.sans.org/y2k/042500.htm

where 8010 is one of the ports scanned.

7. Evidence of active targeting

Active targeting is evident as the logs provided do not indicate scanning of other servers or ports.

8. Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

Criticality	5 (Firewall and/or mail server was possibly targeted)
Lethality	1 (Attack unlikely to succeed as probably neither CommuniGate or WinGate is used)
System Countermeasures	4 (Carefully monitored servers)
Network Countermeasures	3 (Validated restrictive firewall)

Severity = (5 + 1) - (4 + 3) = -1

9. Defensive Recommendation

If servers are indeed running either CommuniGate and/or WinGate, access should be restricted both on the server and the network through the use of access control lists.

10. Multiple choice question

```
11 01 2000 06:15:04.684819 ppp-225.ogertel.com.3579 > My.Net.139.71.8010:
S 4284628:4284628(0) win 8192  (DF)
11 01 2000 06:15:04.695807 ppp-225.ogertel.com.3578 > My.Domain.8010:
S 4284626:4284626(0) win 8192  (DF)
11 01 2000 06:15:04.696849 ppp-225.ogertel.com.3580 > My.Domain.8010:
S 4284629:4284629(0) win 8192  (DF)
11 01 2000 06:15:07.520960 ppp-225.ogertel.com.3579 > My.Net.139.71.8010:
S 4284628:4284628(0) win 8192  (DF)
11 01 2000 06:15:07.665390 ppp-225.ogertel.com.3580 > My.Domain.8010:
S 4284629:4284629(0) win 8192  (DF)
11 01 2000 06:15:07.715265 ppp-225.ogertel.com.3578 > My.Domain.8010:
S 4284626:4284626(0) win 8192  (DF)
```

Which best describes the detect above?

a. Scanning for port listening on 8010

b. Attack in progress through port 8010

c. TCP retransmission

d. Non-anomalous traffic

ANSWER: (a).

Detect 3

```
[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:47:21.973424 208.184.219.253:20 -> x.x.x.2:515
TCP TTL:244 TOS:0x0 ID:59824
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:47:53.157274 208.184.219.253:20 -> x.x.x.4:515
TCP TTL:244 TOS:0x0 ID:25472
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-18:52:02.641247 208.184.219.253:20 -> x.x.x.20:515
TCP TTL:244 TOS:0x0 ID:12802
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF

[**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
10/31-19:03:59.876453 208.184.219.253:20 -> x.x.x.66:515
TCP TTL:244 TOS:0x0 ID:9143
**S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
```

1. Source of trace

http://www.sans.org/y2k/110200-1430.htm

2. Detect was generated by:

Detect was generated by Snort.

Explanation of fields:

```
LINE 01:   [**] IDS06 - MISC-Source Port Traffic 20 TCP [**]
           Snort rule which triggered the detect

LINE 02:   10/31-18:47:21.973424 208.184.219.253:20 -> x.x.x.2:515
           Date(month/day), time(hh:mm:ss.ms), source IP and port (x.x.x.x.port),
           destination IP and port (x.x.x.x.port)

LINE 03:   TCP TTL:244 TOS:0x0 ID:59824
           IP protocol type, time-to-live (TTL), type-of-service (TOS), IP
           identification value (ID)

LINE 04:   **S***** Seq: 0x1000000 Ack: 0x0 Win: 0x3FFF
           TCP flags, TCP sequence number, TCP acknowledge bit, TCP window size
```

3. Probability the source address was spoofed

Low since the attacker will want to see the results of the probe.

4. Description of attack

The attacker was scanning for any Windows NT 4.0 and Windows 2000 servers providing Microsoft's LPD service (known as Print Services for UNIX in Windows 2000) on the default port 515. Buffer overflow exploit using malformed requests can cause TCPSVC.EXE to crash and

subsequently cause the failure of other services (e.g. DHCP, FTP, etc) that depend on TCPSVC.EXE.

More information are available from the following:

- CVE-2000-0232

  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0232

- MS00-021

  http://www.microsoft.com/technet/security/bulletin/MS00-021.asp

5. Attack mechanism

The attacker was specifically scanning for servers listening on port 515 and using port 20 (ftp-data) to circumvent the firewall.

6. Correlations

Muliple detects were previously posted on GIAC

- http://www.sans.org/y2k/111000-1200.htm
- http://www.sans.org/y2k/102400.htm

7. Evidence of active targeting

There was active scanning of several servers for port 515.

8. Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

Criticality	3 (No evidence of critical servers targeted)
Lethality	2 (Attack unlikely to succeed as TCP/IP Printing Services not installed by default)
System Countermeasures	2 (Vulnerable if systems are not at the recommended patch levels)
Network Countermeasures	2 (Firewall does not block traffic)

Severity = (2 + 2) - (2 + 2) = 0

9. Defensive Recommendation

If systems have TCP/IP Printing Services installed access should be restricted both on the server and the network through the use of access control lists.

10. Multiple choice question

What is the service listening on port 515 for a Windows NT 4.0 or 2000 server?

a. Domain Name Service

b. TCP/IP Printing Services

c. Web Service

d. Undefined service

ANSWER: (a).

Detect 4

```
Nov 11 16:49:53 socretes kernel: Packet log: input REJECT eth1 PROTO=6
  24.3.24.41:1218 xxx.xxx.xxx.xxx:111 L=60 S=0x00 I=28466 F=0x4000 T=53
  SYN (#9)
Nov 11 17:35:57 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31177 F=0x4000 T=53
  SYN #107)
Nov 11 17:36:00 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31326 F=0x4000 T=53
  SYN (#107)
Nov 11 17:36:06 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31847 F=0x4000 T=53
  SYN (#107)
```

1. Source of trace

http://www.sans.org/y2k/111600-1300.htm

2. Detect was generated by:

Detect was generated by ipchains.

Explanation of fields:

```
Nov 11 16:49:53 socretes kernel: Packet log: input REJECT eth1 PROTO=6
  24.3.24.41:1218 xxx.xxx.xxx.xxx:111 L=60 S=0x00 I=28466 F=0x4000 T=53
  SYN (#9)
```

input: the chain which contained the rule which matched the packet, causing the log message.

REJECT: action to take on the packet.

eth1: the interface name the packet came in from.

PROTO=6: the packet was protocol 6.

24.3.24.41: the packet's source IP address

1218: the source port was port 1218. For UDP and TCP, this number is the source port. For ICMP, it's the ICMP type. For others, it will be 65535.

xxx.xxx.xxx.xxx: the destination IP address.

111: the destination port was 111. For UDP and TCP, this number is the destination port. For ICMP, it's the ICMP code. For others, it will be 65535.

L=60: the packet length was 34 bytes long.

S=0x00: the Type of Service (TOS) field (divide by 4 to get the TOS as used by ipchains).

I=18: the IP ID.

F=0x0000: the 16-bit fragment offset plus flags. A value starting with `0x4' or `0x5' means that the Don't Fragment bit is set. `0x2' or `0x3' means the `More Fragments' bit is set; expect more fragments after this. The rest of the number is the offset of this fragment, divided by 8.

T=53: the Time To Live (TTL) of the packet. One is subtracted from this value for every hop, and it usually starts at 15 or 255.

SYN: TCP flag of the packet.

(#9): the rule number which caused the packet log.

3. Probability the source address was spoofed

Low since the attacker will want to see the results of the probe.

4. Description of attack

The attacker appears to be looking for LINUX/x86 servers compromised with a rpc.statd exploit. These servers probably have root shells installed and listening on 9088.

More information are available from the following:

- Security Focus

  http://www.securityfocus.com/archive/75/137609

5. Attack mechanism

The attacker attempts to open a connection to the portmap service on port 111 and subsequently checks if the server is listening on 9088, which is a popular port for root shells.

6. Correlations

Muliple detects were previously posted on GIAC

- http://www.sans.org/y2k/081600.htm

  Contains a packet dump which captures an attempt at compromising the server by the attacker

```
Aug 12 06:56:58 hostp statd[284]: statd: attempt to create
  "/var/statmon/sm/%08x %08x %08x %08x %08x%08x %08x %08x
  %08x %08x %08x %08x %08x %08x %0242x%n%055x%n%012x%n0192x
  %nK^v ^( ^ ^. #^1 F'F* FF+, NV1@/bin/sh -c echo "9088
  stream tcp nowait root /bin/sh -i" >> /tmp/m;
  /usr/sbin/inetd /tmp/m;"
```

- http://www.sans.org/y2k/092900.htm
- http://www.sans.org/y2k/092900.htm

7. Evidence of active targeting

Active targeting is evident as the logs provided do not indicate scanning of other servers or ports.

8. Severity

Severity = (Criticality + Lethality) - (System Countermeasures + Network Countermeasures)

Criticality	1 (Home system targeted)
Lethality	2 (Attack unlikely to succeed if system is at the recommended patch level)

System Countermeasures	3 (Home system might not be adequately secured)
Network Countermeasures	2 (Home system might not be adequately secured)

Severity = (1 + 2) - (3 + 2) = -2

9. Defensive Recommendation

Systems should be configured to restrict access to portmap and other rpc services.

10. Multiple choice question

```
Nov 11 16:49:53 socretes kernel: Packet log: input REJECT eth1 PROTO=6
  24.3.24.41:1218 xxx.xxx.xxx.xxx:111 L=60 S=0x00 I=28466 F=0x4000 T=53
  SYN (#9)
Nov 11 17:35:57 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31177 F=0x4000 T=53
  SYN #107)
Nov 11 17:36:00 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31326 F=0x4000 T=53
  SYN (#107)
Nov 11 17:36:06 socretes kernel: Packet log: input DENY eth1 PROTO=6
  24.3.24.41:3936 xxx.xxx.xxx.xxx:9088 L=60 S=0x00 I=31847 F=0x4000 T=53
  SYN (#107)
```

Which best describes the detect above?

a. Scanning for port listening on 9088

b. Attack in progress through port 9088

c. TCP retransmission

d. Non-anomalous traffic

ANSWER: (d).

Assignment 2 - Evaluate an Attack (20 Points)

1. Attack Tool Identification

WinNuke is a denial of service attack through the NETBIOS port 139. The attack is accomplished by sending out of band (OOB) data to the target host. Most Windows 95/NT operating systems are vulnerable.

Obtained from: http://www.jaydee.cz/files/winnuke.zip

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

2. Description of Attack

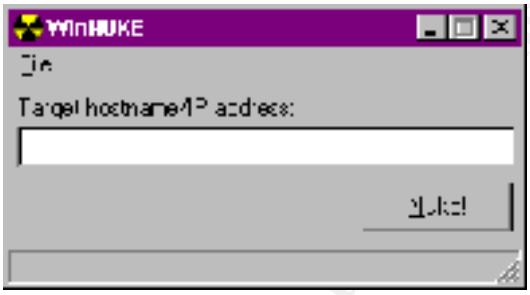
WinNuke exploits bugs in Windows 95/NT operating systems by sending packets that the operating system either cannot handle or is not expecting.

Specifically, a *Stop 0x0000000A* occurs in tcpip.sys on the Windows machine. The attacker sends OOB data by setting the URGENT bit flag

in the TCP header. The target Windows machine on receiving the packet uses the URGENT POINTER to determine where the urgent data ends in the segment. The Windows machine expects normal data to follow and bugchecks when the URGENT POINTER points to the end of the frame instead.

In most cases, the networking system crashes causing the *blue screen of death (BsoD)*. Other times, the machine either hangs or reboots.

The WinNuke tools is a simple to use program. The attacker simply enters the IP address of the target host and clicks on the *Nuke!* Button.



A Windows machine can be protected by installing the latest patches and service packs.

Latest information and fix available from Microsoft,

> Article ID: Q143478 *Stop 0A in Tcpip.sys When Receiving Out Of Band (OOB) Data*
> http://support.microsoft.com/support/kb/articles/Q143/4/78.asp

3. Network Trace of Attack

The following is a Snort output obtained from a tcpdump file of a WinNuke attack which was unsuccessful. Comments are in black fonts.

```
Initializing Network Interface...
snaplen = 1514
Entering readback mode....

-*> Snort! <*-
Version 1.6.3
By Martin Roesch (roesch@clark.net, www.snort.org)
11/22-23:39:03.792680 attacker.evil.net:2246 -> target.good.net:139
TCP TTL:128 TOS:0x0 ID:60363  DF
**S***** Seq: 0x336E54E   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK
```

attacker.evil.net initiates a connection to port 139 on target.good.net with a SYN packet.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.793063 target.good.net:139 -> attacker.evil.net:2246
TCP TTL:128 TOS:0x0 ID:64501  DF
**S***A* Seq: 0x69CAA189   Ack: 0x336E54F   Win: 0x2238
TCP Options => MSS: 1460
```

target.good.net accepts the connection and sends a SYN/ACK packet to attacker.evil.net.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.793215 attacker.evil.net:2246 -> target.good.net:139
TCP TTL:128 TOS:0x0 ID:60619  DF
******A* Seq: 0x336E54F   Ack: 0x69CAA18A   Win: 0x2238
```

attacker.evil.net sends a ACK packet to target.good.net to complete the three way handshake.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.794276 attacker.evil.net:2246 -> target.good.net:139
TCP TTL:128 TOS:0x0 ID:60875  DF
*****PAU Seq: 0x336E54F   Ack: 0x69CAA18A   Win: 0x2238
44 49 45 21                                    DIE!
```

attacker.evil.net then sends OOB data to target.good.net with the PUSH/ACK/URG flags set in the TCP header. *DIE!* is decoded in the Snort dump.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.794740 target.good.net:139 -> attacker.evil.net:2246
TCP TTL:128 TOS:0x0 ID:64757  DF
***F*PA* Seq: 0x69CAA18A   Ack: 0x336E553   Win: 0x2235
83 00 00 01 8F                                 .....
```

target.good.net initiates closing of the connection with a FIN packet to attacker.evil.net.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.794842 attacker.evil.net:2246 -> target.good.net:139
TCP TTL:128 TOS:0x0 ID:61131  DF
***F**A* Seq: 0x336E553   Ack: 0x69CAA18A   Win: 0x2238
```

attacker.evil.net acknowledges and completes the closing of the connection.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/22-23:39:03.794923 attacker.evil.net:2246 -> target.good.net:139
TCP TTL:128 TOS:0x0 ID:61387  DF
****R*** Seq: 0x336E554   Ack: 0x69CAA18A   Win: 0x0

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

attacker.evil.net sends a RESET to target.good.net.

```
Exiting...


===============================================================================
Snort processed 7 packets.
Breakdown by protocol:
    TCP: 7          (100.000%)
    UDP: 0          (0.000%)
   ICMP: 0          (0.000%)
  FRAGS: 0          (0.000%)
    ARP: 0          (0.000%)
   IPv6: 0          (0.000%)
    IPX: 0          (0.000%)
  OTHER: 0          (0.000%)


===============================================================================
```

Assignment 3 - "Analyze This" Scenario (20 Points)

This report is divided into the following sections:

1. All Alerts
2. Top Alerts
3. All Scans
4. Top Scans

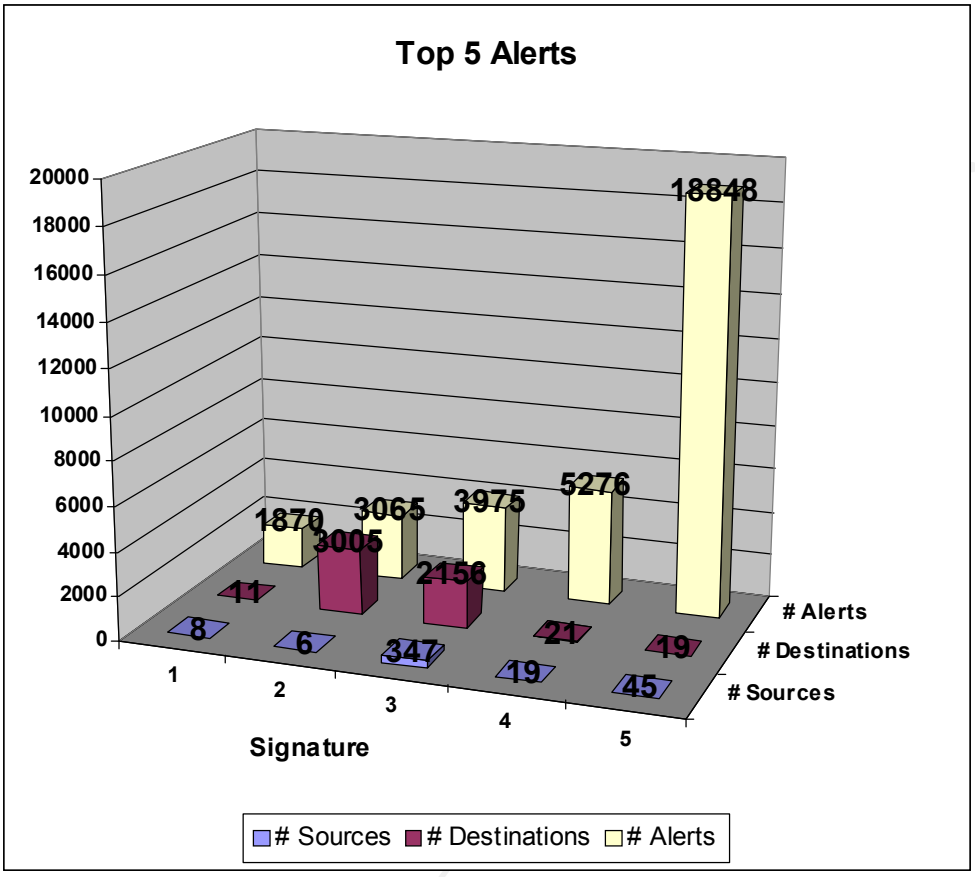
All Alerts

Signature	# Alerts	# Sources	# Destinations
Happy 99 Virus	2	2	2
Possible wu-ftpd exploit - GIAC000623	2	1	2
site exec - Possible wu-ftpd exploit - GIAC000623	6	1	4
TCP SMTP Source Port traffic	8	2	2
Tiny Fragments - Possible Hostile Activity	10	5	8
External RPC call	40	6	3
Probable NMAP fingerprint attempt	41	7	28
Queso fingerprint	46	11	23
SUNRPC highport access!	63	5	3
NMAP TCP ping!	99	10	42
Null scan!	155	63	73
SMB Name Wildcard	321	17	15
SNMP public access	825	16	1
Attempted Sun RPC high port access	1870	8	11
SYN-FIN scan!	3065	6	3005
WinGate 1080 Attempt	3975	347	2156
Watchlist 000220 IL-ISDNNET-990517	5276	19	21
Watchlist 000222 NET-NCFC	18848	45	19

Top 5 Alerts

The top 5 alerts are (not in order):

1. Attempted Sun RPC high port access
2. SYN-FIN scan!
3. WinGate 1080 Attempt
4. Watchlist 000220 IL-ISDNNET-990517
5. Watchlist 000222 NET-NCFC



1. Attempted Sun RPC high port access

Out of the 1870 alerts, 1866 originated from ICQ servers.

Source IP	Source Hostname	# Alerts
205.188.179.33	fes-d021.icq.aol.com	1054
205.188.153.98	fes-d002.icq.aol.com	410
205.188.153.109	fes-d013.icq.aol.com	222
205.188.153.115	fes-d019.icq.aol.com	132
205.188.153.112	fes-d016.icq.aol.com	40
205.188.153.114	fes-d018.icq.aol.com	8

The other 4 detects are false positives:

```
09/12-18:20:59.295476 [**] Attempted Sun RPC high port access [**]
141.213.191.50:3787-> MY.NET.98.160:32771
09/12-18:58:28.164729 [**] Attempted Sun RPC high port access [**]
141.213.191.50:4670-> MY.NET.98.160:32771
09/12-19:14:42.174099 [**] Attempted Sun RPC high port access [**]
141.213.191.50:4090-> MY.NET.98.160:32771

08/20-22:57:10.153306 [**] Attempted Sun RPC high port access [**]
128.211.224.100:2917-> MY.NET.98.111:32771
```

2. SYN-FIN scan!

210.61.144.125 and 213.25.136.60 accounted for 3055 out of 3065 alerts. Both IP are not resolvable to hostnames.

210.61.144.125 conducted an exhaustive scan of 2392 hosts on the MY.NET.0.0/16 network using source port 21 and destination port 21 of the targets.

Information obtained from Asia Pacific Network Information Center (APNIC) indicates the following ownership:

```
inetnum:     210.61.144.64 - 210.61.144.127
netname:     FSCL-NET
descr:       First Securities Co., LTD.
descr:       12F, No. 39, Sec. 2, Tun-Hwa S. Rd,
descr:       Taipei Taiwan
country:     TW
admin-c:     CYC1-TW
tech-c:      CYC1-TW
remarks:     This information has been partially mirrored by APNIC from
remarks:     TWNIC. To obtain more specific information, please use the
remarks:     TWNIC whois server at whois.twnic.net.
mnt-by:      TWNIC-AP
changed:     twnic-update@hinet.net 20000509
source:      TWNIC

person:      Ching Yuan Chen
address:     First Securities Co., LTD.
address:     12F, No. 39, Sec. 2, Tun-Hwa S. Rd,
address:     Taipei Taiwan
phone:       +886-2-2755-5768
fax-no:      +886-2-2784-9504
country:     TW
e-mail:      admin@fst.com.tw
nic-hdl:     CYC1-TW
remarks:     This information has been partially mirrored by APNIC from
remarks:     TWNIC. To obtain more specific information, please use the
remarks:     TWNIC whois server at whois.twnic.net.
changed:     hostmaster@twnic.net 19990924
source:      TWNIC
```

The host 213.25.136.60 conducted a scan of 663 hosts on the MY.NET.0.0/16 network using ports 9704.

Information obtained from Réseaux IP Européens (RIPE) indicates the following ownership:

```
inetnum:     213.25.136.32 - 213.25.136.63
netname:     INFORES
descr:       Infores Bilgoraj
descr:       Bilgoraj
country:     PL
admin-c:     HT2414-RIPE
tech-c:      HT2189-RIPE
status:      ASSIGNED PA
mnt-by:      AS5617-MNT
changed:     tkielb@cst.tpsa.pl 20000216
source:      RIPE
```

The attacker is probably looking for a backdoor shell listening on port 9704 on servers compromised using a RPC stat exploit. More information available from

- SANS GIAC: http://www.sans.org/082200.htm
- CERT: http://www.cert.org/advisories/CA-2000-17.html

- CVE-2000-0666: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0666

3. WinGate 1080 Attempt

168.187.26.157 scanned a total of 1755 hosts in MY.NET.0.0/16 network on port 1080.

Information obtained from American Registry for Internet Numbers (ARIN) indicates the following ownership:

```
Kuwait Ministry of Communations (NET-MOC-KW)
   PO Box No 31811111
   KW

   Netname: MOC-KW
   Netnumber: 168.187.0.0

   Coordinator:
      Sharif, Majeed  (MS695-ARIN)  msharif@KEMS.NET
      (965) 2443808

   Domain System inverse mapping provided by:

   NCC.MOC.KW                196.1.69.98
   NCCDNS.MOC.KW             196.1.69.100

   Record last updated on 23-Jun-1999.
   Database last updated on 21-Nov-2000 18:14:57 EDT.
```

The attacker could be looking for SOCKS servers which listens on port 1080. A higher possibility is looking for compromised servers with the WinHole Trojan living on port 1080.

A total of 347 source hosts targeted 2156 hosts in MY.NET.0.0/16 network.

4. Watchlist 000220 IL-ISDNNET-990517

Traffic from 212.179.0.0/17 (ISDN Net Ltd.) has been placed on a watchlist.

There's a lot of Napster traffic that can potentially be exploited. More information available at:

http://www.sans.org/infosecFAQ/napster.htm

The following hosts may have been compromised:

IP Address	Port	Trojan/Backdoor
MY.NET.221.94	6699	Napster
MY.NET.181.87	6699	Napster
MY.NET.157.200	6699	Napster
MY.NET.221.94	6699	Napster
MY.NET.181.87	6699	Napster
MY.NET.202.58	6688	Unknown (suspect)
MY.NET.53.28	4407	Unknown (suspect)
MY.NET.223.62	2995	Unknown (suspect)
MY.NET.204.150	2669	TOAD

5. Watchlist 000222 NET-NCFC

Traffic from 159.226.0.0/16 (Computer Network Center Chinese Academy of Sciences) has been placed on a watchlist.

There's a lot of port 25, 21, 23, 1080 traffic.

The following hosts may have been compromised:

IP Address	Port	Trojan/Backdoor
MY.NET.253.52	113	Kazimas
MY.NET.6.7	6500	BoKS Master
MY.NET.162.199	1095	RAT
MY.NET.162.199	1097	RAT
MY.NET.163.32	110	ProMail Trojan

All Scans

Signature	# Alerts	# Sources	# Destinations
TCP 21SFR*A* scan	1	1	1
TCP *1SFR*** scan	1	1	1
TCP *1****AU scan	1	1	1
TCP *1*F*PAU scan	1	1	1
TCP *1*F***U scan	1	1	1
TCP 2*S*R**U scan	1	1	1
TCP **S*** scan	1	1	1
TCP 2****PAU scan	1	1	1
TCP *1SF*P** scan	1	1	1
TCP 21SF*P** scan	1	1	1
TCP *1SF**AU scan	1	1	1
TCP *1SFRP*U scan	1	1	1
TCP *1*FR*A* scan	1	1	1
TCP 21SF*PAU scan	1	1	1
TCP *****P** scan	1	1	1
TCP 2*SFRPA* scan	1	1	1
TCP 2*SF*P*U scan	1	1	1
TCP 21*FR**U scan	1	1	1
TCP 21S**PAU scan	1	1	1
TCP **SFRP** scan	1	1	1
TCP *1*FR*** scan	1	1	1
TCP **SFR**U scan	1	1	1
TCP 2*SFRPAU scan	1	1	1
TCP *1SFR*AU scan	1	1	1
TCP 2*S**P** scan	1	1	1
TCP 2*SF**AU scan	1	1	1
TCP 21***P*U scan	1	1	1
TCP 21*FR*AU scan	1	1	1
TCP *1SF**A* scan	1	1	1
TCP *1S*R*AU scan	2	2	2
TCP *1*F**** scan	2	2	2

TCP 21SFRPA* scan	2	1	1
TCP 21S*R*** scan	2	2	2
TCP 2*SFRP*U scan	2	2	2
TCP **SF*PAU scan	2	2	2
TCP 2**FR**U scan	2	2	2
TCP *1****A* scan	2	1	1
TCP 2*S*RP** scan	2	2	2
TCP 21**RP** scan	2	2	2
TCP 2***R**U scan	2	1	1
TCP *1SF***U scan	2	2	2
TCP ***FR**U scan	2	1	1
TCP 21*F**AU scan	2	2	2
TCP 21*F*P** scan	2	2	2
TCP 2*****AU scan	2	2	2
TCP 21***PA* scan	2	2	2
TCP 2*SFR*** scan	2	1	1
TCP *1**RP** scan	2	2	2
TCP *1SFRPA* scan	2	2	2
TCP **S***AU scan	2	2	2
TCP **S*R*AU scan	2	2	2
TCP *1S***AU scan	2	2	2
TCP **SFRPA* scan	2	2	2
TCP 2*S*R*AU scan	2	2	2
TCP 21**R**U scan	2	2	2
TCP **SFR*** scan	2	2	2
TCP 21**RPAU scan	2	2	2
TCP 2**FRPAU scan	2	2	2
TCP 2****P*U scan	2	1	1
TCP 21**RPA* scan	2	2	1
TCP *1**R**U scan	2	1	1
TCP 2**F**** scan	2	2	2
TCP 21S*RPA* scan	2	1	1
TCP 21S****U scan	2	2	2
TCP 21SFRP** scan	3	3	3
TCP 21S**P*U scan	3	2	2
TCP 21SFR*AU scan	3	3	2
TCP 2*****A* scan	3	2	2
TCP 2**F*PA* scan	3	3	3
TCP 21SF*P*U scan	3	2	2
TCP 21*FR*A* scan	3	2	2
TCP *1SF*PA* scan	3	2	2
TCP 21S***AU scan	3	3	2
TCP 21**R*A* scan	3	3	3
TCP *1SF*PAU scan	3	3	3
TCP 21****AU scan	3	2	2
TCP **SFR*AU scan	3	1	1
TCP 21**RP*U scan	3	3	3
TCP 21****** scan	3	1	1
TCP **SF*PA* scan	3	2	1
TCP *1SF**** scan	3	3	2

TCP ****RPAU scan	3	2	2
TCP 2******* scan	3	3	3
TCP *1*FRP** scan	3	2	2
TCP 21S**PA* scan	3	2	2
TCP ****RP*U scan	3	2	2
TCP 2**F*P*U scan	3	1	1
TCP *1S**PAU scan	3	2	2
TCP 2*S*RP*U scan	3	2	2
TCP **S**P*U scan	3	3	3
TCP 2*SFRP** scan	3	3	2
TCP 21*F**A* scan	3	3	3
TCP 21SF***U scan	3	2	2
TCP **SF***U scan	3	2	1
TCP 2***RPAU scan	3	2	2
TCP *1SFRPAU scan	3	2	2
TCP 2***RPA* scan	3	2	2
TCP 2******U scan	4	2	2
TCP 2**F***U scan	4	4	4
TCP **S*RP*U scan	4	3	3
TCP *1*FRPAU scan	4	4	4
TCP *1S*R*** scan	4	4	4
TCP ***FR*AU scan	4	4	4
TCP 2*SFR*AU scan	4	2	1
TCP 21**R*AU scan	4	3	3
TCP 2**FR*A* scan	4	4	4
TCP 2**FRPA* scan	4	3	2
TCP 21*FRPAU scan	4	4	4
TCP 2*SFR**U scan	4	4	4
TCP *1**RPA* scan	4	3	3
TCP 2*SFR*A* scan	4	3	3
TCP 2*SF**** scan	4	3	3
TCP *1S****U scan	4	4	3
TCP 21*F**** scan	4	3	3
TCP ****RP** scan	4	2	3
TCP *1**R*AU scan	4	3	3
TCP 2*SF*PA* scan	4	2	2
TCP *1SFR*A* scan	4	3	3
TCP *1*FRPA* scan	4	3	3
TCP **S**P** scan	4	3	3
TCP 21****A* scan	5	3	3
TCP 2*S***AU scan	5	1	1
TCP *1*F*P*U scan	5	5	5
TCP **S*R**U scan	5	3	2
TCP 2***R*AU scan	5	3	3
TCP ***FR*** scan	5	5	5
TCP ****R*AU scan	5	4	4
TCP 21**R*** scan	5	2	2
TCP 2*S***A* scan	5	3	2
TCP 2***R*A* scan	5	4	3
TCP 2*S****U scan	5	5	5

TCP *1*FR**U scan	5	4	4
TCP 21SF*PA* scan	5	3	2
TCP 21SFR*** scan	5	3	3
TCP 21S*R**U scan	5	4	4
TCP *1*FR*AU scan	5	4	4
TCP 2*S**P*U scan	5	2	2
TCP 21*FRP*U scan	5	4	4
TCP *1**RP*U scan	5	3	3
TCP **S**PAU scan	5	3	3
TCP *1SF*P*U scan	5	5	5
TCP 2*SF***U scan	5	2	2
TCP **SFRPAU scan	5	3	3
TCP 21*F*PAU scan	5	2	2
TCP *******U scan	5	3	3
TCP 21*F*PA* scan	5	2	2
TCP *1S*RPA* scan	5	3	3
TCP 21***P** scan	6	4	4
TCP *1*F**AU scan	6	3	3
TCP 2*S**PAU scan	6	3	2
TCP *****P*U scan	6	4	4
TCP *1S**PA* scan	6	5	5
TCP 2*S*RPA* scan	6	2	2
TCP 21***PAU scan	6	4	4
TCP *1S*RP** scan	6	4	4
TCP **S*RPAU scan	6	3	2
TCP *1**R*A* scan	6	4	4
TCP 2*S*R*** scan	6	1	1
TCP 2**FR*** scan	6	2	1
TCP *1S**P*U scan	6	3	3
TCP *1S*RP*U scan	6	3	3
TCP *1***PA* scan	6	5	4
TCP **S*RP** scan	6	2	2
TCP 21S*RP** scan	6	2	2
TCP **S*RPA* scan	7	6	5
TCP 21S*RP*U scan	7	3	2
TCP 21*F*P*U scan	7	3	3
TCP 21*FRP** scan	7	4	4
TCP 21*****U scan	7	3	2
TCP 2**FRP** scan	7	4	3
TCP **SF*P** scan	7	4	4
TCP 2****P** scan	7	5	4
TCP *1*F*PA* scan	7	2	2
TCP ***FRP** scan	7	5	5
TCP *1S**P** scan	7	2	2
TCP 2*SF**A* scan	7	3	3
TCP 2****PA* scan	7	3	2
TCP 21S*R*A* scan	7	3	2
TCP *1S***A* scan	7	5	5
TCP 21S**P** scan	7	2	2
TCP **SF**AU scan	7	3	2

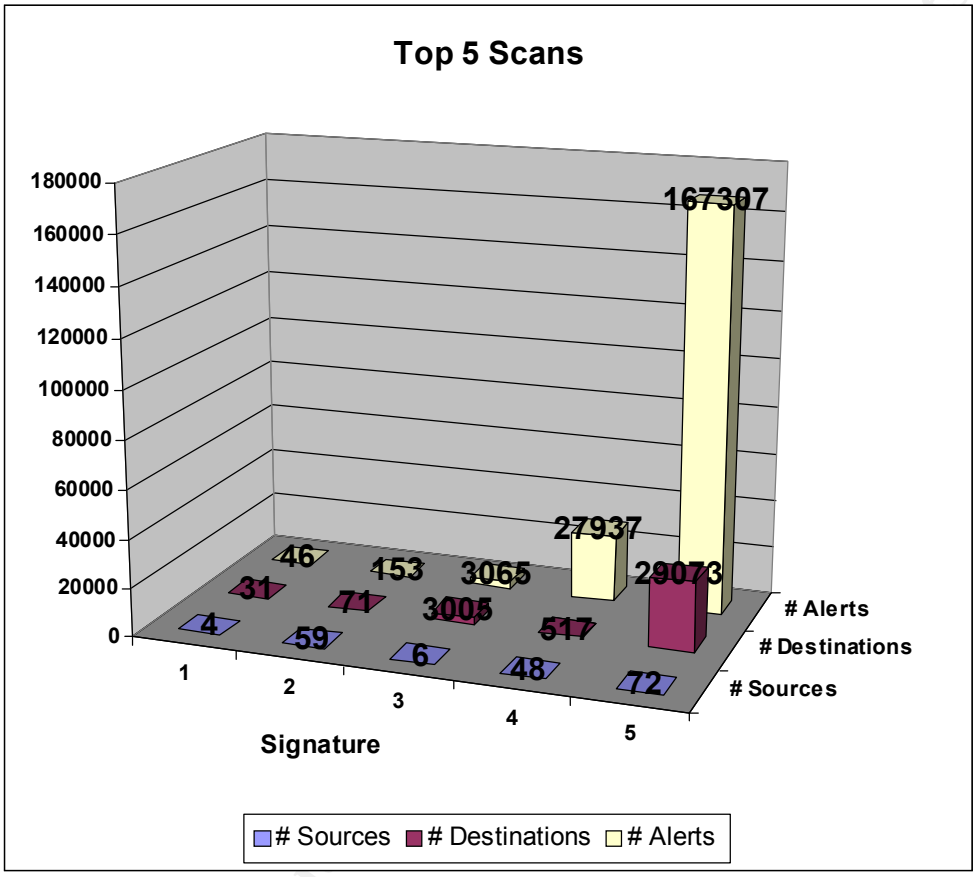
TCP *1*FRP*U scan	8	2	1
TCP 21SFR**U scan	8	4	4
TCP **SF**A* scan	8	3	3
TCP 2**F*PAU scan	8	4	4
TCP ***F***U scan	8	4	4
TCP 21SF**** scan	8	4	4
TCP 2**F*P** scan	8	4	4
TCP **S*R*** scan	8	4	4
TCP 21SFRP*U scan	8	3	3
TCP 2*S*R*A* scan	9	5	5
TCP 2***RP*U scan	9	7	6
TCP *1****** scan	9	5	5
TCP *1*F**A* scan	9	3	3
TCP ***FRPA* scan	9	7	8
TCP **S****U scan	9	4	4
TCP *1***P*U scan	10	3	2
TCP ***FRPAU scan	10	2	2
TCP **S*R*A* scan	10	7	7
TCP 21S*R*AU scan	10	4	3
TCP *1S*RPAU scan	11	6	6
TCP *1SFRP** scan	12	7	7
TCP *1**RPAU scan	12	5	4
TCP **SFR*A* scan	12	4	4
TCP ****R**U scan	12	4	4
TCP 2***R*** scan	12	3	3
TCP **S**PA* scan	12	7	7
TCP *1S*R**U scan	14	5	4
TCP 21S***A* scan	15	2	2
TCP ***FRP*U scan	17	5	4
TCP *1**R*** scan	19	8	9
TCP *1***PAU scan	20	5	5
TCP 21SFRPAU scan	21	8	8
TCP 21S***** scan	33	11	20
TCP 2*S***** scan	33	6	19
TCP ***FR*A* scan	34	11	16
TCP **SF*P*U scan	39	6	27
TCP ***F**** scan	39	19	21
TCP 21SF**A* scan	43	3	3
TCP ***F*P*U scan	46	4	31
TCP ******** scan	153	59	71
TCP **SF**** scan	3065	6	3005
UDP scan	27937	48	517
TCP **S***** scan	167307	72	29073

Top 5 Scans

The top scans are (not in order):

1. TCP ***F*P*U scan

2. TCP ******** scan
3. TCP **SF**** scan
4. UDP scan
5. TCP **S***** scan



These scans attempts to either fingerprint the operating systems or check for listening ports on the hosts in the MY.NET.0.0/16 network.

Assignment 4 - Analysis Process (20 Points)

The following tools were used in analyzing the Snort detects provided in the "Analyze This" Scenario:

1. SnortSnarf (http://www.silicondefense.com/snortsnarf)
2. Microsoft Excel
3. PERL scripts

SnortSnarf

SnortSnarf is a PERL program used for the diagnostic inspection of alert files from the Snort Intrusion Detection System. The program produces HTML output for data analysis.

The alert files (similarly for scan files) provided were concatenated into a single alert file and processed by SnortSnarf to produce the breakdown reports. The reports are then analyzed for false positives and anomalies.

Microsoft Excel

Microsoft Excel is the spreadsheet program included in Microsoft Office.

This software was used to create the charts and also used for sorting/processing sections of alerts.

PERL scripts

PERL is a language built for scanning text files, extracting information from those text files, and printing reports based on that information.

PERL scripts were used to extract data from multiple alert files for further analysis.

Last Updated: July 25th, 2017

Upcoming Training

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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
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 Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
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 Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced