Global Information Assurance Certification Paper

SANS Intrusion Detection Practical Assignment
Capitol SANS 2000
Scott Zimmerman

Assignment 1- Network Detects

Detect 1 - Horizontal SYN-FIN Scan of FTP port 21

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

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/01-01:19:43.355584 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                              ......

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

Color Legend

Time	Source Host:port	Target Host:port
Protocol	Flags	

1. Source of Trace.

This Snort trace comes from the example Capitol SANS 2000 GIAC website data for assignment two.

2. Detect was generated by:

This detect was generated by the open source Snort Intrusion Detection System (IDS).

3. Probability the source address was spoofed:

The IP address used in this scan was more then likely not spoofed as the person is looking to obtain information regarding the targeted network. The IP address 203.32.161.197 is a member of the Bell South Domain. Upon doing an DNS reverse lookup on that address I was able to determine the host name of *adsl-61-44-215.mia.bellsouth.net* . From the beginning of the name "adsl" it appeared as

though the address is apart of a DSL network. I examined the www.bellsouth.net website and that is exactly what it is.

4. Description of attack:

This was an SYN-FIN scan of the entire Class B network MY.NET.X.X. The attacker started at the lowest address in the IP address range and begun a horizontal scan of port 21 (FTP) on each host in that range.

5. Attack mechanism:

More then likely the attacker used a tool such as Nmap or some other port mapper. This would allow him to scan a much large number of IP addresses without having to intervene. The idea behind the SYN-FIN scan of port 21 is too prompt a response from a listening host. A port that is not active on the host will not respond to the SYN-FIN scan. A port that is active will return an error message because the TCP/IP three way handshake did not take place. This would provide the attacker the information that he is looking for.

6. Correlations:

There are many articles available that explain the use of an SYN-FIN scan. The reason the person was targeting the FTP server ports is probably due to the many easily available FTP server exploits.

http://www.insecure.org/nmap/, http://www.synfin.net

7. Evidence of active targeting:

The attacker was performing a scan of the entire class B network. He didn't target a specific host but he was targeting the FTP service.

8. Severity:

Calculated with the formula you learned in class.

We use the following formula to calculate severity of the attack. The metrics are assigned on the five point scale, 5 being the highest, 1 being the lowest.

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

System Criticality – **5**, the scan was able to reach a great deal of machines

Attack Lethality – **0**, the purpose of the scan was to provide reconnaissance data

System Countermeasures – **0**, Due to the nature of the IP stack a machine will respond to these scans

Network Countermeasures – **5**, The Snort IDS was able to detect this scan

Severity – **0**, Scans are a normal occurrence in the Internet community

9. Defensive recommendation:

In the data that I was given I was unable to find a response from any of the hosts protected by this IDS. So I would assume that either a firewall is blocking the response or there are no FTP servers located in the IP address range.

If you do allow FTP services on your network I would suggest the following. Keep FTP servers within a DMZ area so that the access to the machine can be controlled. Minimize the number of machines providing FTP services and keep them current with OS and application patches.

10. Multiple choice test question:

In the trace above, what is the attacker trying to achieve?

a) Create a Distributed Denial of Service Attack

b) Find all listening FTP servers on the network

c) Transmit data to a user using the FTP application

d) Create a buffer overflow of the FTP service by sending a packet with only SF set

Answer B

Detect 2 – wu-ftpd Exploit

10/01-07:38:44.859097 [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**] 208.61.44.215:3815 -> MY.NET.99.130:21

10/01-07:38:51.118666 [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**] 208.61.44.215:3816 -> MY.NET.130.81:21

10/01-07:38:55.557580 [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**] 208.61.44.215:3818 -> MY.NET.130.242:21

Color Legend
Time **Source Host:port** **Target Host:port**

1. Source of Trace.

This Snort trace comes from the example Capitol SANS 2000 GIAC website data for assignment two.

2. Detect was generated by:

This detect was generated by the open source Snort IDS.

3. Probability the source address was spoofed:

A response from the host is critical, so that the likelihood that the address is spoofed is very low.

4. Description of attack:

This is a buffer overflow exploit against the Washington University ftp daemon (wu-ftpd). The wu-ftpd daemon can be found on many different versions of Linux.

5. Attack mechanism:

The attacker is able to compromise the system using the SITE EXEC implementation. The attacker is able to input directly into a format string for a *printf function. This enables them to overwrite data such as the return address on the stack. The attacker is then able to execute shellcode as root.

6. Correlations:

Additional information regarding this compromise can be found on both bugtraq www.securityfocus.com and also the CVE at www.cve.mitre.org.

CVE CAN-2000-0574
BUGTRAQ ID BugtraqID 1387

7. Evidence of active targeting:

This is tough to determine. The way in which the attacker bounced from host to host makes me believe that this is not active targeting but a search for possible ftp servers. But if you look at the information contained within Detect 1- SYN-FIN scan, they are also looking for ftp servers and about the same time. I was look further into this.

8. Severity:

We use the following formula to calculate severity of the attack. The metrics are assigned on the five point scale, 5 being the highest, 1 being the lowest.

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

System Criticality – **5**, the scan was able to reach a great deal of machines

Attack Lethality – **0**, the purpose of the scan was to provide reconnaissance data

System Countermeasures – **0**, Due to the nature of the IP stack a machine will respond to these scans

Network Countermeasures – **5**, The Snort IDS was able to detect this scan

Severity – **0**, Scans are a normal occurrence in the Internet community

9. Defensive recommendation:

If the GIAC Enterprises utilizes servers running the Washington University ftp service ensure that the latest patches are applied to these machines.

10. Multiple choice test question:

The wu-ftpd exploit is classified as what type of attack?

a) A Distributed Denial of Service Attack

b) A buffer overflow

c) A reconnaissance technique

d) An exploit of the Washington University Telnet service

Answer B

Detect 3 – Ipr Utility Exploit

11/22-11:24:06.406682 [**] connect to 515 from inside [**] MY.NET.179.78:2274-> 64.244.202.110:515

11/22-11:33:56.296324 [**] connect to 515 from inside [**] MY.NET.179.78:2707-> 64.244.202.66:515

Color Legend
Time **Source Host:port** **Target Host:port**

1. Source of Trace.

This Snort trace comes from the example Capitol SANS 2000 GIAC website data for assignment two.

2. Detect was generated by:

This detect was generated by the open source Snort IDS.

3. Probability the source address was spoofed:

Since the data stream was generated from within the network the address was not spoofed.

4. Description of attack:

lpr is a utility which listens on port 515 and queues print jobs and submits them to a destination. It is possible for an attacker to use functions within the utility to either crash the host or execute arbitrary code.

5. Attack mechanism:

The lpr utility contains a function called checkremote() which returns a pointer to a null terminated character string. This string is then passed to syslog() as its primary argument. This string is constructed so that malicious format specifiers can be included, syslog can then be crashed or be exploited to execute arbitrary code.

6. Correlations:

Additional information regarding this compromise can be found on bugtraq, www.securityfocus.com and also the CVE at www.cve.mitre.org.

CVE CAN-2000-0917
BUGTRAQ ID BugtraqID 1711

7. Evidence of active targeting:

Without root access to the target host, a user may not input into the string. Because of this I feel that the source host was configured incorrectly and that active targeting did not take place. It is also possible that some other service is configured to operate on that port. More data is needed to make a call on this attack. I searched the OOS files and found no indications one way or the other.

8. Severity:

We use the following formula to calculate severity of the attack. The metrics are assigned on the five point scale, 5 being the highest, 1 being the lowest.

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

System Criticality – **0**, the host was not a member of the GIAC network

Attack Lethality – **0**, without root access the attack can not be carried through

System Countermeasures – **0**, the possible attack occurred on a remote host

Network Countermeasures – **5**, The Snort IDS was able to detect this scan

Severity – **5**, This more then likely was a false positive

9. Defensive recommendation:

Through the use of a Firewall or access list do not allow any access to port 515 from the Internet. A filter should be created on the Snort box to minimize the number of false positives created by this signature.

10. Multiple choice test question:

What would be considered the best defensive practice to minimize the risk of the lpr(port 515) exploit against these hosts ?

a) Ensure that all hosts have the latest available patches

b) Change administrative passwords on a regular basis

c) Eliminate unneeded services from these hosts

d) All of the above

Answer D

Detect 4 – Back Orifice Scan

10/03-23:46:39.847665 [**] Back Orifice [**] 203.155.129.50:31338-> 200.66.98.44:31337

10/03-23:46:40.024489 [**] Back Orifice [**] 203.155.129.50:31338-> 200.66.98.75:31337

10/03-23:46:40.488358 [**] Back Orifice [**] 203.155.129.50:31338-> 200.66.98.220:31337

10/03-23:50:29.318825 [**] Back Orifice [**] 203.155.129.50:31338-> 200.66.98.163:31337

Color Legend
Time **Source Host:port** **Target Host:port**

1. Source of Trace.

This Snort trace comes from the example Capitol SANS 2000 GIAC website data for assignment two.

2. Detect was generated by:

This detect was generated by the open source Snort IDS.

3. Probability the source address was spoofed:

This attack is probably not spoofed. They are scanning for Trojans, and the information is useful only if it is returned to the scanner.

4. Description of attack:

This is a network scan for hosts that have been compromised with the Back Orifice Trojan, which if found will give the attacker control of the target host.

5. Attack mechanism:

The attacker is performing reconnaissance using either a scanning tool or the Back Orifice client application to search for systems that will respond to the probe to port 31337. Since no response is seen from the target host it can be assumed the Trojan does not reside on the host.

6. Correlations:

This is a well-known and well-documented exploit.

Whiteshats.com IDS397

CVE CAN-1999-0660.

7. Evidence of active targeting:

It appears as though this was an arbitrary scan of these hosts as no other connections were examined.

8. Severity:

We use the following formula to calculate severity of the attack. The metrics are assigned on the five point scale, 5 being the highest, 1 being the lowest.

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

System Criticality – **3**, I am unsure of the criticality of these particular machines.

Attack Lethality – **0**, the purpose of the scan was to provide reconnaissance data

System Countermeasures – **0**, It appears as no host responded back to the probe. This would make feel that none of these machines have been compromised.

Network Countermeasures – **5**, The Snort IDS was able to detect this scan

Severity – **-2**, scans for Trojans are a normal occurrence in the Internet community

9. Defensive recommendation:

Though the use of a management tool or Anti-Virus software the Windows workstations should be checked periodically for all well know Trojan applications. Also, since this Trojan almost always resides on the same port continue to check those machines that are scanned by the scanning hosts in the same way.

10. Multiple choice test question:

In order for the Back Orifice Trojan to function what must occur?

a) The Back Orifice client application must be installed on the compromised host

b) The host must be running a version of Linux

c) The Back Orifice server application must be installed on the compromised host

d) Root access must first be obtained

Answer C

Assignment 2 - "Analyze This" Scenario

Background

My organization has been asked to provide a bid for security services to GIAC Enterprises, an e-business startup that sells electronic fortune cookie sayings. We have been provided with one month's worth of data from a Snort IDS with a fairly standard rulebase. Contained within this report is my organization analysis of the data provided.

GIAC Enterprises IDS Data Overview

Snort Alarm/Scan/Packet Data

The Snort alarm data that was examined was collected from the morning of September 26, 2000 through the evening of November 22, 2000. An extensive overview of this data can be found in the body of this report.

Detects

Snortsnarf (http://www.silicondefense.com/snortsnarf/) was used in the analysis of the Snort data. SnortSnarf is an application that takes alarm files from Snort and produces HTML reports. In order for the engine to process the Snort data I needed too first concatenate the data. I then changed the IP addresses for the host network from my.net.x.x to 200.66.x.x and then back again to my.net.x.x for this report.

During this time period the following detects were examined. These detects are sorted in ascending order on the # Alerts field.

Signature	# Alerts	# Sources	# Destinations
1. SYN-FIN scan!	56250	30	25751
2. Watchlist 000220 IL-ISDN66-990517	30998	61	108
3. Watchlist 000222 66-NCFC	8166	45	26
4. WinGate 1080 Attempt	4802	570	2655
5. TCP SMTP Source Port traffic	2893	4	2836
6. Attempted Sun RPC high port access	2542	20	33
7. Broadcast Ping to subnet 70	1813	216	1
8. Back Orifice	1697	40	932
9. SNMP public access	468	23	1
10. Null scan!	283	204	196
11. SMB Name Wildcard	218	33	33
12. Queso fingerprint	142	29	58
13. NMAP TCP ping!	96	21	20
14. SUNRPC highport access!	60	13	12
15. connect to 515 from inside	56	2	3
16. Probable NMAP fingerprint attempt	15	14	13
17. External RPC call	13	8	3
18. Tiny Fragments - Possible Hostile Activity	7	5	6
19. SITE EXEC - Possible wu-ftpd exploit - GIAC000623	7	1	4
20. site exec - Possible wu-ftpd exploit - GIAC000623	6	4	4
21. Happy 99 Virus	2	2	2

Detect Descriptions

Happy 99 Virus	HAPPY99.EXE is a email worm
site exec - Possible wu-ftpd exploit - GIAC000623	FTP server exploit (Buffer overflow)
Tiny Fragments - Possible Hostile Activity	Packets that don't meet min threshold, generally 256 bytes. This is technique to evade a firewall and also an IDS that does not do packet reassembly. Nmap can create these packets. Many sites turn the reassembly feature off because of the performance hit it creates.
SITE EXEC - Possible wu-ftpd exploit - GIAC000623	FTP server exploit (Buffer overflow)
External RPC call	Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. There are many reasons to target these RPC ports including buffer overflows, host information for finger printing and NFS mounts.
Probable NMAP fingerprint attempt	NMAP has templates built into it that allow it to do Operating System (OS) fingerprinting. If OS is determined by this technique the attacker has a huge head start as he can be more specific about the attack.
connect to 515 from inside	This is a format string vulnerability in use_syslog() function in Redhat 7. syslog can then be crashed or be exploited to execute arbitrary code.
SUNRPC highport access!	Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. There are many reasons to target these RPC ports including buffer overflows, host information for finger printing and NFS mounts.
NMAP TCP ping!	TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-lis- tener. If a SYN|ACK is received, a RST is immedi- ately sent to tear down the connection (actually our OS kernel does this for us). The primary advan- tage to this scanning technique is that fewer sites will log it. Unfortunately you need root privi- leges to build these custom SYN packets. http://www.nmap.org/nmap/nmap_manpage.html
Queso fingerprint	Queso is an OS fingerprinting tool much like Nmap. It has a distinct fingerprint of Syn 1,2 . http://www.whithats.com
SMB Name Wildcard	SMB traffic is very common on networks that have hosts running the Windows operating system. The hosts are trying to locate other hosts on the network and utilize the "*" wildcard which creates the alarm.
Null scan!	The idea is that closed ports are required to reply to

	your probe packet with an RST, while open ports must ignore the packets in question (see RFC 793 pp 64). The Null scan turns off all flags. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows95/NT. http://www.nmap.org/nmap/nmap_manpage.html
SNMP public access	Simple Network Management Protocol is a protocol that allows a network engineer to manage networked devices. SNMP has three tiers of security access. The first being a read only or Public access. Many engineers install network hardware and don not change the default community string (password) of SNMP. This allows for each reconnaissance of a network.
Back Orifice	Back Orifice is a trojan that is used to remotely access a host. The Back Orifice server once installed on a hacked machine will listen on port# 31337.
Broadcast Ping to subnet 70	The broadcast ping is a reconnaissance technique in which any live host will respond to the sender. This signature could also be a possible Ddos as an attacker would be looking for a Smurf amplifier.
Attempted Sun RPC high port access	Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. There are many reasons to target these RPC ports including buffer overflows, host information for finger printing and NFS mounts.
TCP SMTP Source Port traffic	This signature looks for both the source host and the receiving host to be communicating on port 25 (SMTP).
WinGate 1080 Attempt	Wingate is a Windows based proxy server with many known vulnerabilities.
Watchlist 000222 66-NCFC	This is a mechanism to generate alerts from a given range of IP addresses.
Watchlist 000220 IL-ISDN66-990517	This is a mechanism to generate alerts from a given range of IP addresses.
SYN-FIN scan!	The SYN-FIN scan is a popular reconnaissance technique.

Event Analysis

Signature – SYN-FIN Scan

The SYN-FIN scan is a popular reconnaissance technique. The person using this technique is either looking for a particular live service or host. The scan is accomplished by send a packet to a host with the SIN-FIN bits set. This is done to evade the firewall or router rulesets. The SYN and FIN bits should never be set in the same packet, which is a trigger for anomalous behavior.

SYN-FIN scan!	30 sources	25751 destinations

Sources triggering this attack signature

Source / Registration	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))	Description of Alarm
160.78.49.191 Centro di Calcolo di Ateneo	7199	7199	7199	7199	Horizontal Scan. The scan targeted port 53 (DNS)
208.61.4.207 BellSouth.net Inv	6635	6635	6635	6635	Horizontal Scan. The scan targeted port 9704 (rpc.statd exploit)
209.92.40.32 FASTNET(tm)-You Tools Corporation	4967	4967	4967	4967	Horizontal Scan. The scan targeted port 9704 (rpc.statd exploit)
63.195.56.20 Pacific Bell Internet Services	3897	3897	3897	3897	Horizontal Scan. The scan targeted port 21 (FTP)
130.89.229.48 University Twente	3860	3860	3860	3860	Horizontal Scan. The scan targeted port 53 (DNS)
210.113.89.200 Asia Pacific Network Information Center	3572	3572	3572	3572	Horizontal Scan. The scan targeted port 27374 (SubSeven Trojan)
203.32.161.197 Asia Pacific Network Information Center	3545	3545	3545	3545	Horizontal Scan. The scan targeted port 21 (FTP)
213.41.69.52 European Regional Internet Registry	3399	3399	3399	3399	Horizontal Scan. The scan targeted port 21 (FTP)
193.64.114.10 European Regional Internet Registry	3295	3295	3295	3295	Horizontal Scan. The scan targeted port 21 (FTP)
195.103.69.159 European Regional Internet Registry	3292	3292	3292	3292	Horizontal Scan. The scan targeted port 53 (DNS)

Time - Earliest such alert at **13:10:30**.153412 *on 09/30*, Latest such alert at **09:33:33**.732424 *on 11/22*

Conclusion

Since all of these scans were of a horizontal nature I feel that this shows common recon and if the correct defensive steps are taken that nothing was compromised. The rpc.statd and DNS seems to be the most popular of scans. I would ensure that all servers running these services are up to date with the latest patches and are secure.

Signature – Watchlist 000220 IL-ISDN66-990517

The administrator of this particular Snort IDS has included a Watchlist for any activity of from this block of addresses. This block of addresses is registered under the European Regional Internet Registry (RIPE). Upon checking with RIPE (www.ripe.net) the majority of this block of addresses are registered an Israeli Telecommunication companies by the name of bezeqint.net.

Watchlist 000220 IL-ISDN66-990517	61 sources	108 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
212.179.95.5	6117	6117	9	9
212.179.27.6	4011	4011	15	15
212.179.79.2	3950	3950	14	14
212.179.44.115	3938	3938	1	1
212.179.72.226	1591	1591	4	4
212.179.41.24	1353	1353	1	1
212.179.45.81	950	950	1	1
212.179.66.2	729	729	4	4
212.179.44.66	667	667	1	1
212.179.29.170	648	648	1	1
212.179.95.26	625	625	1	1
212.179.7.58	589	589	1	1
212.179.30.113	579	579	1	1
212.179.15.122	564	564	1	1
212.179.50.77	505	505	1	1
212.179.24.136	475	475	1	1
212.179.56.5	439	439	2	2
212.179.23.95	416	416	4	4
212.179.45.241	402	402	12	12
212.179.58.191	366	366	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.211.146	4810	4814	1	3
MY.NET.223.98	3938	3940	1	3
MY.NET.206.90	3914	3918	2	6
MY.NET.203.142	1638	1640	1	3
MY.NET.218.142	1459	1463	1	5
MY.NET.214.170	1353	1371	1	8
MY.NET.202.22	950	952	1	3
MY.NET.201.174	796	803	1	8
MY.NET.214.74	667	669	1	3
MY.NET.209.106	648	655	1	6

MY.NET.221.146	638	639	2	3
MY.NET.223.254	625	627	1	3
MY.NET.211.178	609	610	1	2
MY.NET.15.215	579	582	1	4
MY.NET.227.190	564	565	1	2
MY.NET.203.206	505	508	1	4
MY.NET.98.181	500	501	1	2
MY.NET.225.58	475	477	1	3
MY.NET.220.190	433	435	2	4
MY.NET.203.118	430	434	1	4

Time - Earliest such alert at **01:14:52**.325234 *on 09/26*, Latest such alert at **14:58:55**.189582 *on 11/22*

Conclusion

I was unable to find any signs of malicious intent from the connections that I examined. All of the TCP and UDP ports were above 1024. I searched on the ports used in the communication and was unable to find any of them in the commonly know ports that a Trojan would use. Bezeqint.net where most of this traffic originates from is involved in e-commerce and also acts as an ISP in Israel.

Signature – Watchlist 000222 66-NCFC

The administrator of this particular Snort IDS has included a Watchlist for any activity of from this block of addresses. This block of addresses (159.226.0.0 - 159.226.255.255) is registered under The Computer Network Center Chinese Academy of Sciences.

Watchlist 000222 66-NCFC	45 sources	26 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
159.226.45.3	6297	6297	8	8
159.226.91.20	1212	1212	4	4
159.226.41.166	123	123	2	2
159.226.5.77	96	96	1	1
159.226.228.1	65	65	5	5
159.226.157.1	38	38	7	7
159.226.66.130	33	33	6	6
159.226.92.10	29	29	1	1
159.226.63.200	23	23	1	1
159.226.114.1	21	21	2	2
159.226.159.1	19	19	4	4
159.226.118.9	18	18	3	3
159.226.21.3	18	18	4	4
159.226.5.222	16	16	1	1
159.226.39.1	14	14	1	1
159.226.6.5	14	14	2	2
159.226.115.1	12	12	2	2
159.226.45.204	12	12	1	1

159.226.49.157	12	12	1	1
159.226.5.83	9	9	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.6.7	5801	5808	8	14
MY.NET.100.230	1299	1302	7	9
MY.NET.253.43	461	589	17	21
MY.NET.253.41	186	331	16	21
MY.NET.253.42	155	171	12	20
MY.NET.99.51	70	73	1	4
MY.NET.100.81	53	56	1	4
MY.NET.145.9	41	86	2	5
MY.NET.6.34	13	15	1	3
MY.NET.145.18	13	14	2	3
MY.NET.6.47	12	46	2	7
MY.NET.253.24	9	10	1	2
MY.NET.1.2	8	11	2	4

Time - Earliest such alert at **01:43:43**.866602 *on 09/26*, Latest such alert at **21:27:46**.757337 *on 11/22*

Conclusion

The majority of these alerts are generated by 159.226.45.3 which is a mail server communicating solely with one other machine.

220 aphy.iphy.ac.cn ESMTP Sendmail 8.9.3/8.9.3; Fri, 2 Feb 2001 00:37:42 +0800 (CST) 221 aphy.iphy.ac.cn closing connection

I would think that most of this communication is between two mail servers. Possibly the 159.226.45.3 is a list server.

It also could be that there are email clients from this block of addresses that are using your Email Server. This may or may not be allowable in your organization. The fact that it is on your Watchlist confuses the matter.

Since the organization is in the e-commerce business of electronic fortune cookies this could also explain some of this traffic.

Signature – Wingate 1080 attempt

Wingate is a Windows based proxy server that allows many users to share an Internet connection. Socks proxy server also uses Port 1080. Over the past few years many exploits have been developed to take advantage of some of weaknesses in these applications.

WinGate 1080 Attempt	570 sources	2655 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))

63.193.210.208 Pacific Bell Internet Services	1883	1883	1837	1837
208.194.161.155 UUNET Technologies	222	222	104	104
198.63.2.192 Verio	179	179	9	9
204.117.70.5 US Sprint	157	157	36	36
64.86.5.250 Teleglobe	137	137	68	68
207.114.4.46 ABSnet Internet Services	132	132	107	107
212.72.75.236 ONLINEREGIONS	114	114	23	23
63.26.7.170 UUNET Technologies	95	95	1	1
24.169.61.162	89	89	75	75
168.120.16.250	72	72	36	36
24.214.18.65	70	70	58	58
198.139.244.22	58	58	7	7
213.96.27.142	58	58	5	5
194.75.152.237	51	51	44	44
216.179.0.37	42	42	22	22
64.86.6.250	33	33	28	28
207.126.106.118	31	31	15	15
63.238.214.65	29	29	20	20
194.84.208.118	29	29	22	22
216.234.161.197	24	24	23	23

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.206.118	372	374	7	9
MY.NET.225.154	126	127	6	7
MY.NET.60.11	76	79	44	47
MY.NET.60.8	67	73	38	44
MY.NET.60.16	40	42	23	24
MY.NET.203.78	34	41	1	6
MY.NET.60.38	34	39	25	29
MY.NET.53.91	29	30	6	7
MY.NET.222.102	25	26	9	10
MY.NET.53.219	24	25	9	10
MY.NET.221.138	23	26	5	8
MY.NET.212.214	19	21	1	3

Time - Earliest such alert at **00:00:52**.873106 *on 09/26*, Latest such alert at **23:32:20**.988483 *on 11/22*

Conclusion

It is hard to determine without the payload of the packets what the intent of the source addresses was. It could be that a proxy service is running on some of these machines.

The benefit that would be gained by exploiting this service would be to do telnet redirection from the proxy host. This would allow the attacker complete anonymity in exploiting other hosts.

Signature – TCP SMTP Source Port Traffic

This signature looks for both the source host and the receiving host to be communicating on port 25 (SMTP).

TCP SMTP Source Port traffic	4 sources	2836 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
211.46.110.81 Korea Network Information Center	1789	2068	1789	2048
24.7.227.215 @Home Network	1096	1148	1096	1144
194.67.168.11 RELSOFT	6	6	6	6
194.88.77.240 LONDON1-DIAL-POOL2	2	2	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.9.67	2	6	2	6
MY.NET.6.203	2	6	2	6
MY.NET.75.144	2	4	2	3
MY.NET.110.18	2	5	2	5
MY.NET.142.211	2	4	2	4
MY.NET.70.197	2	4	2	4
MY.NET.13.157	2	5	2	5
MY.NET.9.73	2	6	2	6
MY.NET.94.94	2	5	2	5
MY.NET.10.44	2	5	2	5
MY.NET.143.85	2	3	2	3
MY.NET.146.172	2	4	2	4
MY.NET.60.134	2	2	2	2
MY.NET.11.35	2	4	2	4
MY.NET.71.206	2	4	2	4

MY.NET.94.218	2	4	2	4
MY.NET.145.98	2	3	2	3
MY.NET.98.26	2	7	2	7
MY.NET.142.23	2	4	2	4
MY.NET.115.178	2	9	2	6

Time - Earliest such alert at **13:10:15**.618101 *on 10/23*, Latest such alert at **20:09:16**.403626 *on 11/19*

Conclusion

The address 211.46.110.81 is the source address of the largest number of alerts. From this it looks as though it is a mail server because it is running Sendmail. But then looking at it closer the host attempts to connect to 2068 hosts. I would consider this very suspicious. I would set up an access list on my border router that would not permit a host to connect to port 25 of any host behind my firewall unless it was a mail server.

SMTP at 211.46.110.81 says (may reveal owner of machine):
220 ns.yongma3.es.kr ESMTP Sendmail 8.9.3/8.9.3; Fri, 2 Feb 2001 01:07:54 +0900
221 ns.yongma3.es.kr closing connection

The second host (24.7.227.215) also is doing the same thing as the host above and I also would consider this very suspicious.

Your mail server also may be being used as a mail relay. Organizations that create SPAM mail use this technique.

Signature – Attempted Sun RPC high port access

Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. It works within the client-server model. There are many reasons to target these RPC ports including buffer overflows, host information for finger printing and NFS mounts.

Attempted Sun RPC high port access	20 sources	33 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
205.188.153.108 AOL.COM	628	628	4	4
205.188.153.107 AOL.COM	517	517	4	4
205.188.153.116	435	435	1	1
205.188.153.109	334	334	3	3
205.188.153.101	110	110	3	3
205.188.153.102	101	101	2	2
205.188.153.99	98	98	3	3
205.188.153.104	91	91	4	4
205.188.153.110	59	59	2	2
205.188.153.100	51	51	2	2
205.188.153.98	48	48	3	3
205.188.153.105	29	29	1	1

205.188.153.111	13	13	3	3
205.188.153.115	9	9	1	1
205.188.153.114	7	7	2	2
205.188.153.97	4	4	1	1
63.83.225.106	3	3	1	1
205.188.153.106	2	2	2	2
205.188.179.33	2	2	1	1
200.53.184.66	1	1	1	1

Destinations receiving this attack signature (Top 20 Shown)

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.221.246	488	490	1	3
MY.NET.225.210	435	437	1	3
MY.NET.217.214	365	366	1	2
MY.NET.206.222	299	323	6	11
MY.NET.222.98	187	187	1	1
MY.NET.226.74	154	157	2	5
MY.NET.228.42	132	136	1	5
MY.NET.227.50	97	100	1	2
MY.NET.152.198	61	63	2	4
MY.NET.223.18	53	55	1	3
MY.NET.209.182	49	54	1	6
MY.NET.225.98	37	39	2	4

Conclusion

These are attempts to connect to RPC service ports running on these hosts. The majority of these attempts originate from America Online or AOL. The targeted port is 32771, which depending on the query can provide information such as what NFS mounts are available and RPC services request. I am not sure that is what was happening here. Most of the source traffic is originating on port 4000. Port 4000 is commonly used by an application known as ICQ (www.icq.com). This application works like an instant messenger. I feel that in these cases there are employees using these tools to communicate to someone on the Internet.

Signature – Broadcast Ping to subnet 70

The broadcast ping is a reconnaissance technique in which any live host will respond to the sender. This alarm could also be a Denial of Service (DOS) attempt.

Broadcast Ping to subnet 70	216 sources	1 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
193.231.169.166 MEDIASAT, Romania	88	88	1	1

193.226.60.179 Universitatea Ovidius, Romania	55	55	1	1
193.231.220.101 FX Internet , Romania	50	50	1	1
213.154.131.131 PCNET, Romania	49	49	1	1
217.10.206.79 MOBIFON , Romania	43	43	1	1
193.231.220.71 FX Internet , Romania	43	43	1	1
213.154.133.190 PCNET, Romania	40	40	1	1
63.227.65.135 U S WEST Communications, USA	37	37	1	1
193.231.220.17	33	33	1	1
193.231.253.224	32	32	1	1
194.102.242.65	32	32	1	1
193.230.129.169	30	30	1	1
129.186.67.59	24	24	1	1
208.212.171.155	22	22	1	1
213.154.134.74	21	21	1	1
193.230.162.79	21	21	1	1
193.231.6.40	19	19	1	1
193.226.127.20	19	19	1	1
217.10.206.93	19	19	1	1
193.226.127.19	19	19	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.70.255	1813	1813	216	216

Conclusion

This is either a possible attempt at a DOS, improperly configured equipment or an attempt at reconnaissance. The best thing to do in this case would be to create a filter on the border router that would disallow these packets from being forwarded. There is no good reason to allow this type of activity on your network.

There is also a good argument that it is a DOS and your network could be being used as an amplifier for a Smurf or Fraggle attack. If it were a DOS attempt most likely the source address would be a spoofed address. The lack of trace files for these attempts hamper in saying for sure.

Signature – Back Orifice

Back Orifice is a Trojan application that is used to remotely access a host. The Back Orifice server once installed on a hacked host will listen on port# 31337.

Back Orifice	40 sources	932 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
62.136.90.120 Planet Online Limited	306	306	189	189
63.46.46.143 UUNET Technologies	291	291	291	291
203.148.182.108 ANET-TH, Thailand	111	111	100	100
213.43.69.72 Iksir Uluslararasi Elektronik Ticaret, Turkey	99	99	91	91
203.155.130.111 COMNET-TH, Thailand	79	79	72	72
209.94.199.186 Telecommunications Services of Trinidad and Tobago	78	78	78	78
213.43.69.126	75	75	68	68
203.148.183.44	75	75	67	67
168.120.12.33	70	70	63	63
209.94.199.141	69	69	59	59
203.170.144.127	58	58	53	53
203.170.154.9	52	52	49	49
203.170.157.154	33	33	33	33
213.43.86.72	31	31	31	31
203.148.183.22	26	26	26	26
213.43.80.51	25	25	25	25
203.170.157.178	24	24	24	24
24.128.48.165	23	23	23	23
62.136.10.186	22	22	22	22
212.187.106.231	21	21	21	21
212.253.18.249	19	19	19	19
62.136.2.72	17	17	17	17
213.43.72.158	15	15	15	15
213.43.77.66	12	12	12	12

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.97.208	7	10	5	8
MY.NET.98.150	7	11	7	11
MY.NET.98.81	6	9	5	8
MY.NET.98.151	6	11	5	10
MY.NET.98.82	6	8	4	6
MY.NET.98.77	6	6	5	5
MY.NET.98.119	6	16	6	15
MY.NET.97.142	6	8	3	5
MY.NET.97.205	5	10	4	8
MY.NET.98.254	5	8	4	7
MY.NET.97.55	5	6	4	5
MY.NET.97.192	5	5	4	4
MY.NET.97.200	5	10	4	9
MY.NET.97.175	5	7	4	6
MY.NET.98.149	5	11	5	10
MY.NET.98.145	5	10	4	9
MY.NET.97.179	5	6	3	4
MY.NET.97.209	5	11	4	9
MY.NET.97.36	5	6	2	3
MY.NET.98.140	5	11	4	10

Time - Earliest such alert at **15:01:27**.048398 *on 10/01*, Latest such alert at **03:16:06**.961852 *on 11/21*

Conclusion

In most of the alarms generated it appears as though the attacker is trolling for Trojans. They are attempting to locate the Back Orifice server on these machines. There are signs of active targeting of two particular subnets 98 and 97. This may or may not mean that a machine has been infected already. Determine which hosts are running Windows 95/NT and use these steps to remove the application.

* Back Orifice key is:
1)*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
-> Standard Value .exe *There is a space before the .exe
2)When used With SilkRope the key is something like
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
-> 412124.TMP Value=412124.TMP *Wierd numbers with the ending TMP.
* Original Boserve.exe is exactly *124.928 Bytes.* With BT Plugin it is something around *193.149 Bytes*
Crypted Verion called Infector is *184.832 Bytes,* Size may vary due to lot of plugins

* Information taken from http://www.whitehats.com/ids/trojan/

Signature – SNMP public access

Simple Network Management Protocol is a protocol that allows a network engineer to manage networked devices. SNMP has three tiers of security access. The first being a read only or Public access. Many engineers install network hardware and don not change the default community string (password) of SNMP. This allows for each reconnaissance of a network.

SNMP public access	23 sources	1 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
MY.NET.98.106	58	58	1	1
MY.NET.98.174	49	49	1	1
MY.NET.97.185	44	44	1	1
MY.NET.97.171	40	40	1	1
MY.NET.97.204	37	37	1	1
MY.NET.98.122	36	36	1	1
MY.NET.98.197	32	32	1	1
MY.NET.97.178	31	31	1	1
MY.NET.98.132	29	29	1	1
MY.NET.97.130	19	19	1	1
MY.NET.97.115	19	19	1	1
MY.NET.98.160	16	16	1	1
MY.NET.97.215	12	12	1	1
MY.NET.97.108	8	8	1	1
MY.NET.97.159	6	6	1	1
MY.NET.97.192	6	6	1	1
MY.NET.98.191	6	6	1	1
MY.NET.97.189	5	5	1	1
MY.NET.98.109	5	5	1	1
MY.NET.98.123	3	3	1	1
MY.NET.98.141	3	3	1	1
MY.NET.97.219	3	3	1	1
MY.NET.97.208	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.101.192	468	561	23	24

Time - Earliest such alert at **11:17:47**.004982 *on 10/01*, Latest such alert at **17:32:56**.420810 *on 11/19*

Conclusion

The SNMP protocol is very common on most IP networks. Many different network management tools utilize this protocol. I feel that these are either traps being sent to this station or are normal management traffic.

Signature – Null Scan

The goal of this scan is that closed ports are required to reply to the probe packet with an RST, while open ports must ignore the packets in question. The Null scan turns off all flags.
http://www.nmap.org/nmap/nmap_manpage.html

Null scan!	204 sources	196 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.113.148.32 Rogers@Home BC	8	8	1	1
128.253.247.116 Cornell University	8	13	2	2
24.112.150.20 Rogers@Home	8	9	1	1
128.195.229.11 University of California, Irvine	7	7	2	2
24.200.14.91 Videotron Ltee	5	5	1	1
195.132.238.93	4	4	3	3
132.178.218.181	4	5	3	3
24.200.140.155	4	5	1	1
195.132.96.165	4	4	1	1
130.75.178.186	3	3	2	2
134.88.222.41	3	3	1	1
24.226.167.52	3	3	1	1
24.65.80.127	3	3	2	2
24.200.9.10	3	3	1	1
207.123.161.43	3	3	1	1
24.94.47.81	2	2	2	2
152.2.174.136	2	2	1	1
132.199.222.167	2	2	1	1
24.13.195.174	2	2	1	1
128.253.97.158	2	2	2	2

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.218.46	8	11	2	4
MY.NET.214.166	8	10	1	3
MY.NET.105.120	8	17	1	7
MY.NET.227.10	7	14	1	3
MY.NET.214.90	5	10	2	7
MY.NET.210.238	5	10	2	6
MY.NET.207.114	4	5	1	2

MY.NET.220.46	4	6	2	4
MY.NET.201.130	4	136	3	9
MY.NET.205.2	3	6	1	4
MY.NET.225.50	3	7	2	6
MY.NET.208.142	3	50	2	8
MY.NET.253.114	3	9	1	5
MY.NET.212.142	3	6	1	4
MY.NET.217.62	3	6	2	4
MY.NET.204.46	2	6	2	6
MY.NET.202.90	2	2	2	2
MY.NET.6.44	2	5	2	5
MY.NET.130.190	2	7	2	7
MY.NET.201.238	2	199	1	3

Time - Earliest such alert at **10:58:55**.817608 *on 09/26*, Latest such alert at **20:33:10**.371736 *on 11/22*

Conclusion

There is a combination of both horizontal and vertical scanning of the hosts on the GIAC network. Most of the source hosts have no other alarm generated by them other then other scans. Because of that I feel that nothing was compromised.

S*ignature* – SMB Name Wildcard

SMB traffic is very common on networks that have hosts running the Windows operating system. The hosts are trying to locate other hosts on the network and utilize the "*" wildcard which creates the alarm. The larger problem occurs when Windows units are connected to the Internet and have file sharing turned on with no security. In most cases this traffic is only normal traffic.

SMB Name Wildcard	33 sources	33 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
MY.NET.101.160	93	93	1	1
141.157.99.21 Bell Atlantic	33	33	1	1
169.254.184.161	24	24	9	9
141.157.98.201 BLACKHOLE.ISI.EDU	20	22	1	2
MY.NET.98.154	5	5	4	4
MY.NET.97.207	4	4	4	4
129.37.159.177 IBM Corporation	4	4	1	1
130.227.195.57	3	3	1	1
MY.NET.97.120	3	3	3	3
MY.NET.101.113	2	2	2	2
MY.NET.98.116	2	2	2	2
24.29.206.229	2	2	1	1

MY.NET.222.42	2	2	1	1
MY.NET.97.205	2	2	1	1
130.127.196.96	1	1	1	1
213.48.182.156	1	1	1	1
MY.NET.98.165	1	1	1	1
38.38.25.126	1	1	1	1
207.172.148.202	1	1	1	1
MY.NET.101.152	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.101.192	93	561	1	24
MY.NET.6.15	53	63	2	9
MY.NET.101.53	9	9	5	5
MY.NET.101.153	7	7	4	4
MY.NET.101.117	7	7	3	3
MY.NET.101.147	4	4	2	2
MY.NET.100.130	4	8	1	5
MY.NET.101.89	4	4	2	2
MY.NET.101.145	3	3	3	3
MY.NET.101.113	3	3	1	1
MY.NET.152.110	3	6	1	4
MY.NET.101.99	2	2	2	2
MY.NET.71.38	2	3	2	3
MY.NET.233.154	2	2	1	1
MY.NET.253.134	2	2	1	1
MY.NET.101.158	2	2	2	2
MY.NET.97.139	2	7	2	7
MY.NET.23.4	1	1	1	1
MY.NET.98.165	1	7	1	7
MY.NET.253.125	1	4	1	4

Time - Earliest such alert at **11:19:08**.075062 *on 10/01*, Latest such alert at **09:27:51**.910085 *on 11/22*

Conclusion

If the source of the alarm is a host located within your network this should not cause alarm, as this is more then likely normal traffic. If the source host is outside of your network then they are more then likely looking for information that is located on these hosts. I would look further into the alarms generated by 141.157.99.21. There are 33 instances of it connecting to the same machine over a couple of hour period. I would consider this very suspicious.

Signature – Queso Fingerprint

Queso is an OS fingerprinting tool much like Nmap. It has a distinct fingerprint of Syn 1,2 . In most cases the attacker is looking to fingerprint operating systems.

Queso fingerprint	29 sources	58 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.3.161.193 @Home Network	45	45	2	2
195.115.7.2 European Regional Internet Registry	22	22	1	1
129.242.219.27 University of Tromso	19	24	18	22
64.80.63.121 PaeTec Communications	15	15	9	9
24.163.42.82 ServiceCo LLC - Road Runner	8	8	1	1
128.253.247.116 Cornell University	5	13	1	2
63.202.13.20 Pacific Bell Internet Services	5	6	5	6
216.164.109.15 Erol's Internet Services	2	2	2	2
216.86.203.177 MM Internet	1	1	1	1
203.33.188.165 Asia Pacific Network Information Center	1	1	1	1
130.89.229.162 University Twente	1	1	1	1
195.127.250.109 European Regional Internet Registry	1	1	1	1
133.46.212.81 Japan Network Information Center	1	3	1	1
203.66.42.129 Asia Pacific Network Information Center	1	1	1	1
195.154.188.66 European Regional Internet Registry	1	1	1	1
24.0.39.207 @Home Network	1	1	1	1
24.163.114.140 ServiceCo LLC - Road Runner	1	1	1	1

148.217.14.205 NIC-Mexico	1	1	1	1
64.81.30.185 Speakeasy Network	1	1	1	1
131.238.3.47 University of Dayton	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.145.9	43	86	1	5
MY.NET.217.26	23	26	2	4
MY.NET.130.116	8	13	1	6
MY.NET.227.10	5	14	1	3
MY.NET.227.118	4	6	1	3
MY.NET.60.38	2	39	1	29
MY.NET.205.194	2	8	2	7
MY.NET.211.202	2	4	1	3
MY.NET.202.162	2	6	1	5
MY.NET.253.112	2	6	1	4
MY.NET.217.150	2	7	1	6
MY.NET.218.110	1	3	1	3
MY.NET.98.119	1	16	1	15
MY.NET.97.176	1	6	1	5
MY.NET.105.120	1	17	1	7
MY.NET.225.14	1	5	1	5
MY.NET.218.134	1	6	1	6
MY.NET.203.118	1	434	1	4
MY.NET.211.146	1	4814	1	3
MY.NET.205.94	1	11	1	8

Time - Earliest such alert at **04:27:59**.343599 *on 09/26*, Latest such alert at **16:10:36**.268157 *on 11/22*

Conclusion

The majority of these alarms are simple Queso scans of the network. The host 24.3.161.193 is scanning port 110 or POP3. I was unable to find any evidence that a compromise took place. The host 195.115.7.2 is scanning port 6436 of the same host. I am unclear as what they were looking for.

Signature – NMAP TCP Ping

TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets. Reference taken from http://www.nmap.org/nmap/nmap_manpage.html

NMAP TCP ping!	21 sources	20 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
192.102.197.234 Intel Corporation	47	47	3	3
202.187.24.3 Asia Pacific Network Information Center	9	9	6	6
63.119.91.2 UUNET Technologies	6	6	4	4
205.128.11.157 SURAnet	5	5	2	2
12.43.88.5 AT&T ITS	4	4	3	3
63.104.49.126 UUNET Technologies	3	3	1	1
64.64.226.2 Teligent	3	3	2	2
216.104.228.102 Exodus Communications	2	2	2	2
204.155.48.3 Southwire Company	2	2	2	2
24.6.151.155 @Home Network	2	4	1	2
213.8.52.189 European Regional Internet Registry	2	2	2	2
2.2.2.2 Internet Assigned Numbers Authority	2	2	2	2
199.36.49.2 Brown Group	1	1	1	1
24.180.134.156 @Home Network	1	3	1	1
63.119.91.3 UUNET	1	1	1	1
192.116.207.178 European Regional Internet Registry	1	1	1	1
198.78.16.3 SURAnet	1	1	1	1
212.160.78.75 European Regional Internet Registry	1	1	1	1
209.218.228.201 @Home Network	1	1	1	1
203.75.25.62 Asia Pacific Network	1	1	1	1

Information Center				
195.54.105.6 European Regional Internet Registry	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.1.8	51	53	7	9
MY.NET.1.9	6	8	2	4
MY.NET.100.165	5	11	3	5
MY.NET.1.3	5	8	3	6
MY.NET.1.4	4	6	3	5
MY.NET.6.7	4	5808	3	14
MY.NET.6.47	3	46	3	7
MY.NET.162.36	2	6	1	4
MY.NET.253.42	2	171	2	20
MY.NET.100.230	2	1302	1	9
MY.NET.1.10	2	4	1	3
MY.NET.60.14	2	5	2	5
MY.NET.110.39	1	3	1	3
MY.NET.202.134	1	12	1	6
MY.NET.6.34	1	15	1	3
MY.NET.6.14	1	2	1	2
MY.NET.6.35	1	5	1	4
MY.NET.253.43	1	589	1	21
MY.NET.253.125	1	4	1	4
MY.NET.1.5	1	4	1	4

Time - Earliest such alert at **05:40:00**.709907 *on 09/26,* Latest such alert at **22:06:00**.355840 *on 11/22*

Conclusion

These alarms also are simple network scans generated by the Nmap application. The hosts residing on the .1 subnet are scanned the most often.

Signature – SUNRPC highport access

Remote Procedure Call or RPC protocol (RFC1831) is a means by which a host can execute code on a remote a host. It works within the client-server model. There are many reasons to target these RPC ports including buffer overflows, host information for finger printing and NFS mounts.

SUNRPC highport access!	13 sources	12 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
216.10.12.30 Virtual Development Inc	33	33	2	2
216.148.218.160 TCG CERFnet	6	6	1	1
205.188.3.211 America Online	4	4	1	1
24.18.90.197 @Home Network	3	3	2	2
195.34.28.117 European Regional Internet Registry	3	9	1	3
205.188.3.239 America Online	3	3	1	1
205.188.4.2 America Online	2	2	1	1
212.86.129.227 European Regional Internet Registry	1	1	1	1
24.40.46.225 Suburban Cable	1	1	1	1
129.123.6.14 Utah State University	1	1	1	1
216.10.12.2 Virtual Development	1	1	1	1
205.188.1.105 America Online	1	1	1	1
211.46.110.81 Asia Pacific Network	1	2068	1	2048

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.206.222	21	323	2	11
MY.NET.202.242	20	38	3	5
MY.NET.212.186	4	7	1	4
MY.NET.228.62	3	5	1	3
MY.NET.97.59	3	9	1	3

MY.NET.253.114	2	9	1	5
MY.NET.53.23	2	5	1	4
MY.NET.53.14	1	3	1	3
MY.NET.6.15	1	63	1	9
MY.NET.206.218	1	3	1	3
MY.NET.140.51	1	1	1	1
MY.NET.179.78	1	2	1	2

Time - Earliest such alert at **13:28:03**.304676 *on 09/28*, Latest such alert at **03:50:53**.188444 *on 11/21*

Conclusion

These are connections or attempted connections to port 32771 on the target host. The query was sent to the rpcbind/portmap daemon requesting port information for rpc services. There is no evidence that a compromise took place, but I would investigate these further.

Signature – connect to 515 from inside

Port 515 is a spooler port used for printing. Format string vulnerability in use_syslog() function in Red Hat 7 allows remote attackers to execute arbitrary commands.

connect to 515 from inside	2 sources	3 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
MY.NET.101.142 Internal to ORG	54	54	1	1
MY.NET.179.78 Internal to ORG	2	2	2	2

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.100.3	54	58	1	5
64.244.202.110 Business Internet, Inc.	1	1	1	1
64.244.202.66 Business Internet, Inc.	1	1	1	1

Time - Earliest such alert at **13:26:43**.509292 *on 11/19,* Latest such alert at **11:33:56**.296324 *on 11/22*

Conclusion

Although port 515 is used to connect to a host outside of your network without additional information it is difficult to make the decision as to the intent. I would investigate this further.

The use of port 515 within your network should not be viewed as abnormal. This constitutes the majority of alarms for this attack signature.

Signature – Probable NMAP Fingerprint

NMAP has templates built into it that allow it to do Operating System (OS) fingerprinting. If OS is determined by this technique the attacker has a huge head start as he can be more specific about the attack.

Probable NMAP fingerprint attempt	14 sources	13 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.95.192.51 ServiceCo LLC - Road Runner	2	2	1	1
24.69.214.58 Shaw Fiberlink ltd.	1	1	1	1
193.231.207.72 European Regional Internet Registry	1	1	1	1
128.54.203.218 University of California, San Diego	1	1	1	1
24.9.64.57 @Home Network	1	1	1	1
132.178.218.181 Boise State University	1	5	1	3
128.194.79.228 Texas A&M University	1	1	1	1
62.226.88.88 European Regional Internet Registry	1	1	1	1
205.251.201.36 Cable Atlantic Inc.	1	1	1	1
195.132.57.32 European Regional Internet Registry	1	1	1	1
169.233.14.204 University of California, Office of the President	1	1	1	1
24.6.151.155 @Home Network	1	4	1	2
24.108.140.159 Videon CableSystems Alberta Inc	1	1	1	1
24.180.134.156 @Home Network	1	3	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.211.94	2	4	1	3
MY.NET.207.14	2	413	2	7
MY.NET.218.162	1	2	1	2
MY.NET.201.126	1	12	1	7
MY.NET.162.39	1	4	1	4
MY.NET.219.146	1	1	1	1
MY.NET.204.170	1	6	1	3
MY.NET.70.93	1	7	1	5
MY.NET.202.134	1	12	1	6
MY.NET.224.150	1	4	1	4
MY.NET.206.50	1	3	1	3
MY.NET.60.38	1	39	1	29
MY.NET.204.202	1	1	1	1

Time - Earliest such alert at **13:38:00**.767581 *on 10/06,* Latest such alert at **22:44:52**.018936 *on 11/22*

Conclusion

These all appear to be basic scans of the network using the Nmap application. The majority of them are attempts at fingerprinting the version of DNS that could possibly be running on these machines.

Signature – External RPC call

External RPC call	8 sources	3 destinations

Sources triggering this attack signature

Source/Regisrtation	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
63.162.239.69 Sprint	3	3	3	3
200.191.80.206 RNP (Brazilian Research Network)	2	2	1	1
200.191.80.181 RNP (Brazilian Research Network)	2	2	1	1
211.46.110.81 Asia Pacific Network Information Center	2	2068	2	2048
12.34.21.196 AT&T ITS	1	1	1	1
24.23.151.112 @Home Network	1	1	1	1
24.7.227.215 @Home Network	1	1148	1	1144

38.200.223.8 Performance Systems International	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.6.15	9	63	7	9
MY.NET.100.130	3	8	3	5
MY.NET.15.127	1	4	1	4

Conclusion

I am unable to determine the exact cause of this alarm, as this is not apart of the standard Snort ruleset. I suspect that the source host made an RPC call to the target host, which triggered the alarm.

Signature – Tiny Fragments

IP packets that don't meet a minimum threshold, generally 256 bytes create this alarm. This is technique is used to evade a firewall and also an IDS that does not do packet reassembly. Nmap can create these packets. Many sites turn the reassembly feature off because of the performance hit it creates.

Tiny Fragments - Possible Hostile Activity	5 sources	6 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
62.6.71.0 European Regional Internet Registry	2	2	1	1
216.43.55.44 McLeodUSA Incorporated	2	2	2	2
172.157.126.93 America Online, Inc.	1	1	1	1
202.156.51.76 Asia Pacific Network Information Center	1	1	1	1
192.206.151.152 Toronto Star Newspapers	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.181.144	2	4	1	3
MY.NET.201.2	1	3	1	3
MY.NET.202.102	1	5	1	5
MY.NET.201.198	1	5	1	5

MY.NET.211.2	1	24	1	7
MY.NET.1.8	1	53	1	9

Time - Earliest such alert at **21:25:17**.293957 *on 09/26,* Latest such alert at **14:39:19**.160234 *on 11/16*

Conclusion

There could be several reasons for this alarm. The first being that these are bad packets that have been somehow corrupted in transit. The possibility could be that they are being generated by the fragrouter (www.anzen.com) application. This tool fragments attack streams so that the IDS not pick them up as an attack.

Signature - wu-ftpd exploit (19,20)

The wu-ftpd exploit is a buffer overflow targeted at the Washington University FTP server. An attacker can log into a wu_ftpd server and execute a recursive *nlist* that takes a great deal of system resources effectively creating a DOS. There is also a buffer overflow associated with this ftp service.

Sources triggering this attack signature (19)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
208.61.44.215 BellSouth.net Inc	7	9	4	5

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.130.242	3	5	1	3
MY.NET.205.94	2	11	1	8
MY.NET.130.81	1	3	1	3
MY.NET.99.130	1	2	1	2

Time - Earliest such alert at **07:38:44**.859097 *on 10/01,* Latest such alert at **07:46:19**.967002 *on 10/01*

Sources triggering this attack signature (20)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
208.61.44.215 BellSouth.net Inc	2	9	2	5
24.31.88.99 ServiceCo LLC - Road Runner	2	2	1	1
202.9.188.89 Asia Pacific Network Information Center	1	1	1	1
63.202.13.20 Pacific Bell Internet Services	1	6	1	6

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.221.82	2	3	1	2
MY.NET.205.94	2	11	2	8
MY.NET.100.209	1	2	1	2
MY.NET.97.206	1	9	1	8

Time - Earliest such alert at **06:17:23**.004770 *on 10/01,* Latest such alert at **16:57:49**.491247 *on 10/16*

Conclusion

I was unable to find any correlating data within the OOS files to determine if this was in fact a compromise. The key to this compromise is that the attacker be able to gain root access to make this occur. I would investigate these machines further and change root passwords.

Signature - Happy99 Virus (21)

Happy99 is an email worm or virus. The snort engine looks for a pattern match within its ruleset to generate this alarm. The Happy99 worm propagates itself by sending itself to other users when the computer is on-line.

Happy 99 Virus	2 sources	2 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
209.94.224.13 Reaction Systems, Inc	1	1	1	1
216.6.117.11 NS2.HYPERIA.COM	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
MY.NET.6.35	1	5	1	4
MY.NET.253.41	1	331	1	21

Time - Earliest such alert at **03:59:51**.460766 *on 10/05*, Latest such alert at **16:06:44**.170359 *on 11/06*

Conclusion

Chances are that the destination host received this via an email. If the host computer is running a current anti-virus application this should not pose any future threat. The risk for this is low**.**

Suggested Defensive Strategies

- Disable all unneeded or unused services on hosts that are connected directly to the Internet.
- Create a filter to disallow any host to communicate outside of network to a service that is not required. An example would be the alarm for the port 515.
- Setup an access list on the border router that would not permit a host to connect to port 25 of any host behind the firewall unless it was a designated mail server.
- If ICQ or other Internet Relay Chat applications were not permitted on the network I would also suggest creating a filter to block this activity. Some common ports are 4000 and 194.
- Do not allow border or perimeter routers to forward packets that are directed to a broadcast address.
- Do not allow any ICMP traffic that originates outside of your network to enter your network. This is used in many common reconnaissance techniques.
- Create filters for the SNORT IDS so that certain traffic internal to your organization does not appear as an attack or alarm. Traffic such SMB, SNMP and RPC. These created a large number of false positives.
- On an ongoing and regular basis change all administrator and root level passwords.
- Ensure that on a regular basis all anti-virus software is patched and updated.

Summary

My feeling is that overall nothing of significant proportion took place during the time period examined. Although there are several areas that need further consideration. The first area of consideration should be the hosts that were reached by both the scans and the attempted exploits. These should be checked for possible compromise. Because while the Snort data provides a great deal of information, there is still a risk that something did occur. I would also suggest that the Snort operator discuss with the router/firewall people ways to improve the overall network security. It seems to me as though too many of the company's machines are accessible from the Internet.

Reference

www.whitehats.com/ids/
www.sans.org
www.snort.org
www.arin.net/cgi-bin/whois.pl
www.ripe.net/db/whois.html
www.apnic.net/
www.robertgraham.com/pubs/firewall-seen.html
www.insecure.com

Assignment 3 - Analysis Process (30 Points)

Assumptions
The first thing I did to assess the alarms generated by the GIAC Enterprises Snort IDS was to make some assumptions to the following questions.

- What is normal and abnormal traffic for the organization?
- What are the security policies of the organization?

These things are critical when providing an assessment of the organization's IDS. The reason is that if it is a standard implementation of the Snort ruleset, and the organization is involved in e-commerce, I would assume that the false positive rate is fairly high for the IDS. An example of this would be the RPC alarms that were generated. Without knowing if this is traffic is normal or abnormal it is very hard to make a determination. The security policies for the firm are also very important in making an assessment. Without a set of ground rules to go by it is difficult to determine what is anomalous and what is not.

Tools Used
To start the assessment of the data I first had to decide on what type of tools I was going to use. I had never worked much with Snort so I was unsure as to what tools were available. After some research I decided on the SnortSnarf application from Silicon Defense was the best choice for me. The reason I choose this tool is that I like working in a browser environment and it had the features that I required. Once I installed the application I then needed to concatenate all of the Snort files from the SANS website. The reason that I needed to do this was to have the SnortSnarf application process it all at the same time and have it all included in the same report. This would allow me a more encompassing overall view of the alarms. I also found the following tools to be very helpful in my analysis process:

- Basic Snort Ruleset, I downloaded this from www.snort.org
- Common Trojan list, I downloaded this from www.sans.org
- Course material from the GIAC track at Capitol SANS
- Common port list from RFC793
- A whitepaper I found at www.robertgraham.com/pubs/firewall-seen.html
- The IDS database at www.whitehats.com

Once I had the reports I began the correlation of the data. I tried first to determine how many of the machines that were scanned had also generated other alarms. I then searched the OOS files for traces to go along with the alarms. I then followed through on whatever matches that I had. The other technique that I used what to focus more on the possible exploits. Alarms such as Wingate 1080, wu-ftpd, etc.. I would search the OOS files for packet traces that would substantiate the alarm.