Global Information Assurance Certification Paper

GIAC Certification Practical
SANS Capital SANS – Practical

Prepared by Jeffrey Dell

Assignment 1 – Network Detects:

1.1 – Detect 1 : Firewalk traffic

Log Format:

[**] IDS03 / Traceroute UDP [**]							
Attack Signature description							
01/25	22:58:47.380045	0:1:96:B8:7C:E1		0:D0:B7:84:F6:32	type:0x800		len:0x4E
Date	**Timestamp**	**Source MAC Address**		**Destination MAC**	**Type of Service**		
209.249.169.61:53	my.net.92.15:0	UDP	TTL:1	TOS:0x0	ID:32463	IpLen:20	DgmLen:64
Source IP:Port	**Destination IP:Port**	**Protocol**	**Time to Live**	**Type Of Service**	**IP ID number**	**IP Header**	**Datagram Length**
Len:44							
TCP Flags							
33 C0 80 81 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00					3.....		
Hexidecimal Payload					**Ascii Decode Payload**		

Trace:

```
[**] IDS03 / Traceroute UDP [**]
01/25-22:58:47.380045 0:1:96:B8:7C:E1 -> 0:D0:B7:84:F6:32 type:0x800 len:0x4E
209.249.169.61:53 -> my.net.92.15:0 UDP TTL:1 TOS:0x0 ID:13248 IpLen:20 DgmLen:64
Len: 44
33 C0 80 81 00 00 00 00 00 00 00 00 00 00 00 00  3...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

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

[**] IDS03 / Traceroute UDP [**]
01/25-22:58:47.403142 0:1:96:B8:7C:E1 -> 0:D0:B7:84:F6:32 type:0x800 len:0x4E
209.249.169.61:53 -> my.net.92.15:0 UDP TTL:1 TOS:0x0 ID:13249 IpLen:20 DgmLen:64
Len: 44
33 C1 80 81 00 00 00 00 00 00 00 00 00 00 00 00  3...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

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

[**] IDS03 / Traceroute UDP [**]
01/25-22:58:47.404255 0:1:96:B8:7C:E1 -> 0:D0:B7:84:F6:32 type:0x800 len:0x4E
209.249.169.61:53 -> my.net.92.15:0 UDP TTL:1 TOS:0x0 ID:13250 IpLen:20 DgmLen:64
Len: 44
33 C2 80 81 00 00 00 00 00 00 00 00 00 00 00 00  3...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

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

[**] / Source Port Traffic 0-52 [**]
01/25-22:58:47.430563 0:1:96:B8:7C:E1 -> 0:D0:B7:84:F6:32 type:0x800 len:0x4E
209.249.169.61:53 -> my.net.92.15:0 UDP TTL:2 TOS:0x0 ID:13251 IpLen:20 DgmLen:64
```

```
Len: 44
33 C3 80 81 00 00 00 00 00 00 00 00 00 00 00 00  3...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

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

[**] / Source Port Traffic 0-52 [**]
01/25-22:58:47.436780 0:1:96:B8:7C:E1 -> 0:D0:B7:84:F6:32 type:0x800 len:0x4E
209.249.169.61:53 -> my.net.92.15:0 UDP TTL:2 TOS:0x0 ID:13252 IpLen:20 DgmLen:64
Len: 44
33 C4 80 81 00 00 00 00 00 00 00 00 00 00 00 00  3...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....
```

< Truncated – Total of 164 packets >

1. Source of Trace
The source of the trace is from my work's Network with a tap in between the Internet router and the Firewall.

2. Detect was generated by:
This trace was detect by Snort IDS 1.7 with the following rule:
alert udp !$HOME_NET 53 -> $HOME_NET 0:52 (msg:" / Source Port Traffic 0-52";)

This signature is looking for any UDP traffic that is not from my network with a source port 53 and is destination is to my network with a port from 0 to 52. This should never happen unless the packet is crafted.

3. Probability the source address was spoofed:
The attacker was trying to get through the firewall and get a response from the email server. It is very unlikely that this attack is being spoofed.

4. Description of attack:
The attack is against our Email server. It looks like the attacker is using a technique called firewalking. It looks like firewalking because the TTL is incrementing my one and the ID is also incrementing by one.

5. Attack mechanism:
Firewalking uses a traceroute-like IP packet analysis to determine whether or not a particular packet can pass from the attacker's host to a destination host through a packet-filtering device. This technique can be used to map 'open' or 'pass through' ports on a gateway. More over, it can determine whether packets with various control information can pass through a given gateway. Also, using this technique, an attacker can map routers behind a packet-filtering device.

After looking at the code for the latest version of firewalk, I found the following interesting information.

Code from Firewalk:

```
case 'I':   /* The initial port to use for TTL ramping */
        fp->init_probe_port = atoi(optarg);
        if (fp->init_probe_port > 65535 || fp->init_probe_port < 1)
        {
           fprintf(stderr, "Invalid probe port : %d\n", fp->init_probe_port);
           usage(argv[0]);
        }
        break;
```

As you can see, the port must be greater then 1 and the ports on my trace are 0. Because of this, the person probably changed the code before he/she compiled it. This means that the person has some basic skills over someone who just compiles a program.

6. Correlations:
whois -h whois.arin.net 209.249.169.61
Abovenet Communications, Inc. (NETBLK-ABOVENET-4)
50 W. San Fernando St., Suite 1010
San Jose, CA 95113 US

Netname: ABOVENET-4
Netblock: 209.249.0.0 - 209.249.my.net
Maintainer: ABVE

I search SANS website for correlations and I found that Laurie @ .edu found the following scans several days later with the same signature.

Jan 30 07:53:41 hosty snort[324969]: MISC-Source Port Traffic 0-52: 209.249.169.61:53 -> z.y.w.34:0
Jan 30 07:53:41 hostm snort[318]: MISC-Source Port Traffic 0-52: 209.249.169.61:53 -> z.y.w.98:0

7. Evidence of active targeting:
This seems to be a targeted attack. The attacker could have done a DNS MX record lookup to find our email server. There were over 160 packets that were directed at our email server. Fortunately no packets made it though the firewall.

8. Severity:

Criticality: The target is critical (our email server) 5.
Lethality: The attack was ineffective 1.
System Countermeasures: The will not respond to port 0. 5
Network Countermeasures: A Pix firewall is setup with ingress and egress filters that stop all traffic destined for port 0 ***5***.
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
-4 = (5 + 1) – (5 + 5)

9. Defensive recommendations:
Again, this is exactly the kind of thing a firewall is there to block. However, one should still try to keep up with patching the seemingly endless list of RPC program exploits. If not to protect yourself from the kiddies outside the firewall, then from the inside job.

10. Multiple choice questions:

TCP Port 53 is used for?

a) Telnet
b) ftp
c) DNS
d) pop3

Answer **C** – DNS Traffic is passed on port 53 for both TCP and UDP.

1.2 Detect 2 : lpr traffic

Log Format:

Feb 15	12:18:02	takahe snort[146]:	IDS181 MISC Shellcode X86 NOPS:
Date	Time	Machine	Alert
12.16.3.2:2225	->	130.216.35.102:515	
Source IP & Port	Direction	Destination IP & Port	

Trace:

```
Feb 15 12:18:02 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2225 -> 130.216.35.102:515
Feb 15 12:18:15 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2227 -> 130.216.35.102:515
Feb 15 12:18:34 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2231 -> 130.216.35.102:515
Feb 15 12:18:51 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2235 -> 130.216.35.102:515
Feb 15 12:19:20 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2237 -> 130.216.35.102:515
Feb 15 12:19:24 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2239 -> 130.216.35.102:515
Feb 15 12:19:27 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2241 -> 130.216.35.102:515
Feb 15 12:20:20 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2245 -> 130.216.35.102:515
Feb 15 12:20:21 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2247 -> 130.216.35.102:515
Feb 15 12:20:23 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS:
  12.16.3.2:2249 -> 130.216.35.102:515
```

1. Source of Trace
Sans Web site. http://www.sans.org/y2k/021601.htm

2. Detect was generated by:
The trace was generated by Snort IDS system with the following Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "IDS181/shellcode-x86-nops"; flags: A+; content: "|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|";)

This signature is looking for TCP traffic from an external ip address on any port to an internal ip address on any port with the ack flag and any other flag set with the content of many NOP operations.

3. Probability the source address was spoofed:
The probability that the source address was spoofed is very low because the attack is using TCP and they are looking for a legitimate response. Also the fact that the signature is looking for an Ack flag says that it is probably not spoofed.

4. Description of attack:
This is an attack against the lpr service which sits on tcp port 515. There was a vulnerability that was released late last year that talks about it.

5. attack mechanism:
lpr is a utility which queues print jobs and submits them to a destination. lpr contains a function called checkremote() which returns a pointer to a null terminated character string. This string is passed to syslog() as its primary argument, the format string. As a result, if this string is constructed so that malicious format specifiers can be included, syslog can crash or be exploited to execute arbitrary code. It has been reported that intentional user input into this string is not possible without root access and thus It is considered unlikely that this vulnerability is exploitable.

As OpenBSD lpr is derived from the BSD source tree, other modern BSD distributions may be vulnerable as well.

RedHat advisory RHSA-2000:066-03 makes note of additional minor issues relating to LPR including a potential DoS as well as a race condition allowing the queue to become wedged. See Reference section for details.

6. Correlations:
Port 515 scans are very popular and I found many systems that have been scanned on Sans web site. Here are a couple of links that show several scans:
http://www.sans.org/newlook/alerts/port515.htm
http://www.sans.org/y2k/112700-1400.htm

The following shows code on how to do this attack
www.netcat.it/download/SEClpd.c

The following link has detailed information about a multiple vendor LPR format string vulnerability that was popular late last year.
http://www.securityfocus.com/bid/1711

The following shows correlations data the happened a short time before the above attack.

15 Feb 01 12:16:10	tcp	12.16.3.2.4977	o>	130.216.4.12.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.4983	o>	130.216.4.18.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.4985	o>	130.216.4.20.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.4988	o>	130.216.4.23.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.4991	o>	130.216.4.26.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.4993	o>	130.216.4.28.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.1053	o>	130.216.4.58.515	s
15 Feb 01 12:16:10	tcp	12.16.3.2.1055	o>	130.216.4.60.515	s

15 Feb 01 12:16:10 tcp 12.16.3.2.1056 o> 130.216.4.61.515 s

7. Evidence of active targeting:
The evidence of active targeting is very high. We first see the attacker scan a range of ip addresses, and then we see him go for one particular machine that has port 515 open.

8. Severity:

Criticality: The target is somewhat critical 3.
Lethality: The attack could have been very deadly but was ineffective 2.
System Countermeasures: The system had no counter measures against this attack. 0
Network Countermeasures: There were no Network countermeasures running except for Snort IDS. 1
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
5 = (5 + 1) – (0 + 1)

9. Defensive recommendations:
Unless absolutely needed, the lpr service should be turned off. If the lpr service cannot be turned off, then a version that supports tcpwrappers should be installed. A firewall should also be setup in front of the machine and only designated hosts should be able to get to this machine. Once these two protections are in place the attackers ip address should be placed in the hosts.deny file and in the firewall with deny all policy in place. This will protect allow protection at both the host and network.

10. Multiple choice question:

Feb 15 12:18:15 takahe snort[146]: IDS181 - MISC - Shellcode X86 NOPS: 12.16.3.2:2227 -> 130.216.35.102:515

The above alert is triggered because?

A) Attacker was scanning port 181
B) Attacker was sending shellcode to port 86
C) Attacker was sending NOPS to port 515
D) Attacker was scanning port 515

Answer: **C** Attacker was sending NOPS to port 515.

1.2 Detect 3

Log Format:

[**] IDS7/SourcePortTraffic-53-tcp [**]			
Attack Signature description			
02/13	16:30:12.281696	131.211.212.160:53	a.b.20.2:53
Date	**Timestamp**	**Source IP:Port**	**Destination IP:Port**
TCP	TTL:239	TOS:0x0	ID:36255
Type of protocol	**Time to Live**	**Type Of Service**	**IP ID number**
S***	Seq: 0x67310CB1	Ack: 0x4DD5B6B	Win: 0x28
TCP Flags	**Sequence Number**	**Acknowledgment Number**	**Windows Size**
00 00 00 00 00 00			.....
Hexadecimal Payload			**ASCII decoded payload**

Trace:

[**] IDS7/SourcePortTraffic-53-tcp [**]

02/13-16:30:12.281696 131.211.212.160:53 -> a.b.20.2:53

TCP TTL:239 TOS:0x0 ID:36255

S*** Seq: 0x67310CB1 Ack: 0x4DD5B6B Win: 0x28

00 00 00 00 00 00 .....

[**] Source Port traffic [**]

02/13-16:30:12.509481 131.211.212.160:53 -> a.b.20.2:53

TCP TTL:239 TOS:0x0 ID:59358

****R*** Seq: 0x67310CB2 Ack: 0x0 Win: 0x0

00 00 00 00 00 00 .....

[**] IDS277/named-probe-iquery [**]

02/13-16:30:13.287517 131.211.212.160:1524 -> a.b.20.2:53

UDP TTL:48 TOS:0x0 ID:59369

Len: 35

97 BA 09 80 00 00 00 01 00 00 00 00 00 00 01 00 ....

01 00 00 7A 69 00 04 04 03 02 01 ...zi.....

[**] IDS278/named-probe-version [**]

02/13-16:30:13.514771 131.211.212.160:1524 -> a.b.20.2:53

UDP TTL:48 TOS:0x0 ID:59374

Len: 38

09 FA 01 80 00 01 00 00 00 00 00 00 07 76 65 72 .....ver

73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....

1. Source of Trace
SANS web site: http://www.sans.org/y2k/021501.htm

2. Detect was generated by:
Trace 1 was generated by Snort IDS system with the following Signature:

alert UDP $EXTERNAL any -> $INTERNAL 53 (msg: "IDS277/named-probe-iquery"; content: "|0980 0000 0001 0000 0000|"; depth: 16; offset: 2;)

and

alert UDP $EXTERNAL any -> $INTERNAL 53 (msg: "IDS278/named-probe-version"; content: "|07|version|04|bind"; depth: 26; offset: 12; nocase;)

3. Probability the source address was spoofed:
The probability that the source address was spoofed is very low because the attacker is probing the computer and is looking for a legitimate response back.

4. Description of attack:
The first 2 packets were doing reconnaissance. It was probably scanning a large range of ip addresses to look for a DNS server. We know that it found a DNS server because it sent a Reset packet back with a sequence number plus one. Now the attacker knows that there is a DNS server at ip address a.b.20.2 so it sends a named-robe-iquery and a named-probe-version. These two packets have the same source port so we know that these are crafted packets. These packets are also discovered by well-known signatures that can be found above.

This alert indicates a probe to determine the version of BIND running on the remote host. This query is usually seen as a pre-attack probe, prior to an attempted overflow of BIND. In 1998 a buffer overflow was discovered that affects certain versions of BIND, the name server daemon currently maintained by the Internet Software Consortium. These older versions of the BIND software would fail to properly bind the data received when processing an inverse query. Upon a memory copy, portions of the program would be overwritten, and arbitrary commands could be run on the affected host.

5. Attack mechanism:
this program will tell you if the remote host has their fake-iquery option turned on

6. Correlations:
Here is some correlation from GIAC:

[**] IDS278/named-probe-version [**]
01/03-23:54:23.184062 18.31.0.163:1132 -> a.b.20.2:53
UDP TTL:51 TOS:0x0 ID:32836 Len: 38
00 06 01 00 00 01 00 00 00 00 00 00 07 76 65 72 .....ver
73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....

http://www.securityfocus.com/bid/134

http://www.securityfocus.com/archive/1/8965

http://www.whitehats.com/info/IDS277

http://www.whitehats.com/info/IDS278

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0009

7. Evidence of active targeting:
The evidence of active targeting is very high. We first see the attacker doing a syn scan on the address, and then we see him probe the server for vulnerabilities.

8. Severity:

Criticality: The target is critical 5.
Lethality: The attack was ineffective 1.
System Countermeasures: The system had no counter measures against this attack. 0
Network Countermeasures: There were no Network countermeasures running except for Snort IDS. 1
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
5 = (5 + 1) – (0 + 1)

9. Defensive recommendations:
The first step to protecting this server is to make sure the server has the latest version of BIND. The latest version can be obtained from http://www.isc.org/products/BIND/. Making sure your bind server is up to date is the only way to truly protect against this type of attack. To further protect yourself you can also block TCP port 53 at the firewall or at a screening router. The only reason that TCP port 53 would be used is if someone wanted to do a zone transfer, normal DNS traffic uses UDP port 53. If this port was blocked the attacker would have skipped right by this server.. This will protect allow protection at both the host and network level.

10. Multiple choice question:

What is the best way to protect against this attack without losing functionality?

a) Disable BIND
b) Change the DNS port
c) Block all IP traffic on port 53
d) Remove the MX record
e) Upgrade BIND to latest version

Answer **E** – Upgrade BIND to the latest version – This is the best way to protect against all bind attacks. Any other answer would limit or lose all functionality of DNS.

1.2 Detect 4

Trace Format

10/31	15:03:58.385633	[**] Queso fingerprint [**]	129.242.219.27:4075	my.net.60.11:1080
Date	**Time**	**Alert Message**	**Source IP & port**	**Destination IP & Port**

Trace:

10/31-15:03:58.385633 [**] Queso fingerprint [**] 129.242.219.27:4075-> my.net.60.11:1080
10/31-19:11:48.174953 [**] Queso fingerprint [**] 129.242.219.27:3585-> my.net.208.134:1080
11/01-23:45:54.325018 [**] Queso fingerprint [**] 129.242.219.27:2844-> my.net.210.246:1080
11/04-20:37:51.624439 [**] Queso fingerprint [**] 129.242.219.27:4268-> my.net.203.170:1080
11/10-14:18:26.690898 [**] Queso fingerprint [**] 129.242.219.27:1190-> my.net.53.153:1080
11/10-21:29:38.826875 [**] Queso fingerprint [**] 129.242.219.27:2705-> my.net.98.213:23

1. Source of Trace
The Source of the Trace was from the GIAC Practical Assignment.

2. Detect was generated by:

alert TCP $EXTERNAL any -> $INTERNAL any (msg: "Queso Fingerprint"; flags: S12;)

3. Probability the source address was spoofed:
This host is looking of a response so the probability that the packet is spoofed is very low.

4. Description of attack:
A query was sent to the rpcbind/portmap daemon on a Solaris machine, requesting port information for rpc services. There are many, many techniques which can be used to fingerprint networking stacks. Basically, you just look for things that differ among operating systems and write a probe for the difference. If you combine enough of these, you can narrow down the OS very tightly.

For more information about this type of attack, refer to the following web page:
www.insecure.org/nmap

5. Attack mechanism:
Queso sets bogus flags 1 and 2 to see how the operating system responds to them. Different operating systems respond differently so it is a way to fingerprint the operating system.

6. Correlations:
On our previous report we found 64 alerts making this alert decreased by 7%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **129.242.219.27**: Official name: **nonet.td.org.UiT.No**
University of Tromso (NET-UITNET)
N-9001 Tromso NORWAY
Netname: UITNET
Netblock: 129.242.0.0 - 129.242.my.net

This Norway server that is looking for wingates and telnet servers. Most of this traffic is just reconnaissance and it would be wise to double-check these hosts to make sure there is no open wingate (1080) or telnet (23) ports.

After searching google, I found that this server use to have the dns name of **viking.no.eu.dal.net**. The following web page referes to it as a DAL IRC server:
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=IRC_FLOODER&VSect=T

If this is the case, that might descript why we are seeing the 1080 scan, but that doesn't say why they were doing a Queso Fingerprint. It also doesn't tell us why it would be scanning port 23.

7. Evidence of active targeting:
The evidence of active targeting is very high. We see many probes from this host directed at my.net.

8. Severity:

Criticality: The target is not critical 1.
Lethality: The attack was ineffective 1.
System Countermeasures: The system had no counter measures against this attack. 0
Network Countermeasures: There were no Network countermeasures running except for Snort IDS. 1
Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
1 = (1 + 1) – (0 + 1)

9. Defensive recommendations:
Check to see if wingate or telnet is running on either of these two machines. If it is, you might want to double check the configuration and install tcpwrappers if it is not already installed on the servers.

10. Multiple choice question:
What flags does Queso use for fingerprinting?

A) Syn , Syn
B) Syn , Fin
C) Syn , Rst
D) Syn,1,2

Answer: **D** Syn,1,2 - One of the tests that queso does is to set the syn, 1 and 2 flags to see how the operating system responds to it. This is also how we detect this scan with snort.

Assignment 2 – "Analyze This" Scenario

2.1 – Introduction

GIAC Enterprises:

Thank you again for the opportunity to assist you in evaluating your security posture. Previously my co-worker Teri Bidwell analyzed your traffic and found some interesting traffic. I had the opportunity to talk with Teri and he gave me a copy of the previous report. In this report I will correlate with his findings and with other security experts to give you an overview of your security posture.

2.2 – Source of Alerts

SnortA10.txt	SnortA29.txt	SnortA44.txt	SnortA28.txt
SnortA11.txt	SnortA3.txt	SnortA45.txt	SnortA40.txt
SnortA12.txt	SnortA30.txt	SnortA46.txt	SnortA41.txt
SnortA13.txt	SnortA31.txt	SnortA47.txt	SnortA42.txt
SnortA14.txt	SnortA32.txt	SnortA48.txt	SnortA43.txt
SnortA15.txt	SnortA33.txt	SnortA49.txt	SnortA57.txt
SnortA19.txt	SnortA34.txt	SnortA5.txt	SnortA59.txt
SnortA2.txt	SnortA35.txt	SnortA50.txt	SnortA6.txt
SnortA20.txt	SnortA36.txt	SnortA51.txt	SnortA7.txt
SnortA21.txt	SnortA37.txt	SnortA52.txt	SnortA8.txt
SnortA22.txt	SnortA38.txt	SnortA53.txt	SnortA9.txt
SnortA23.txt	SnortA39.txt	SnortA54.txt	SnortAle.txt
SnortA24.txt	SnortA4.txt	SnortA55.txt	SnortA26.txt
SnortA25.txt	SnortA27.txt		

OOSche10.txt	OOSche3.txt	OOSche6.txt	OOSche46.txt
OOSche17.txt	OOSche34.txt	OOSche7.txt	OOSche5.txt
OOSche19.txt	OOSche4.txt	OOScheck.txt	OOSche50.txt
OOSche2.txt	OOSche44.txt	OOSche25.txt	OOSche24.txt
OOSche20.txt	OOSche45.txt	OOSche29.txt	

SnortS10.txt	SnortS22.txt	SnortS38.txt	SnortS7.txt
SnortS11.txt	SnortS23.txt	SnortS39.txt	SnortS8.txt
SnortS12.txt	SnortS24.txt	SnortS4.txt	SnortS9.txt
SnortS13.txt	SnortS27.txt	SnortS41.txt	SnortSca.txt
SnortS14.txt	SnortS3.txt	SnortS42.txt	SnortS56.txt
SnortS15.txt	SnortS30.txt	SnortS45.txt	SnortS58.txt
SnortS16.txt	SnortS31.txt	SnortS47.txt	SnortS6.txt
SnortS17.txt	SnortS32.txt	SnortS48.txt	SnortS35.txt
SnortS18.txt	SnortS33.txt	SnortS49.txt	SnortS36.txt
SnortS2.txt	SnortS34.txt	SnortS5.txt	SnortS37.txt
SnortS20.txt	SnortS21.txt		

2.3.4 Signature Detects in Detail

2.3.4.1 Summary of the possible exploit from the Snort Scans:

Top 3 types of scans:

Signature	# of Alerts	# Sources	# Destinations
UDP scan	22330	79	1406
TCP **SF**** scan	41055	24	22612
TCP **S***** scan	220529	269	35777

Definition of Scanning from Phrack 51 (An electronic magazine for hackers)
Scanning, as a method for discovering exploitable communication channels, has been around for ages. The idea is to probe as many listeners as possible, and keep track of the ones that are receptive or useful to your particular need. Much of the field of advertising is based on this paradigm, and the "to current resident" brute force style of bulk mail is an almost perfect parallel to what we will discuss. Just stick a message in every mailbox and wait for the responses to trickle back.
Scanning entered the h/p world along with the phone systems. Here we have this tremendous global telecommunications network, all reachable through codes on our telephone. Millions of numbers are reachable locally, yet we may only be interested in 0.5% of these numbers, perhaps those that answer with a carrier.
The logical solution to finding those numbers that interest us is to try them all. Thus the field of "wardialing" arose. Excellent programs like Toneloc were developed to facilitate the probing of entire exchanges and more. The basic idea is simple. If you dial a number and your modem gives you a CONNECT, you record it. Otherwise the computer hangs up and tirelessly dials the next one.
While wardialing is still useful, we are now finding that many of the computers we wish to communicate with are connected through networks such as the Internet rather than analog phone dialups. Scanning these machines involves the same brute force technique. We send a blizzard of packets for various protocols, and we deduce which services are listening from the responses we receive (or don't receive).

2.3.4.1.1 Syn Scan

220529 alerts with this signature among the files:

Earliest such alert at **01:39:55** *on 9/27*
Latest such alert at **19:42:37** *on 11/23*

TCP **S***** scan	269 sources	35777 destinations

Top 5 Sources triggering this attack signature:

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
66.9.27.254	20649	20649	19322	19322
62.252.21.241	13057	13057	8267	8267
194.244.78.145	11904	11904	1	1
63.88.175.201	11717	11718	10646	10647
62.157.23.237	9639	9641	8725	8726

Top 5 Destinations receiving this attack signature:

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.220.2	11915	11915	11	11
my.net.162.77	1756	1757	6	7
my.net.60.16	1303	1305	2	3
my.net.204.26	1166	1168	6	8
my.net.140.57	1155	1220	6	7

From Phrack 51 (An electronic magazine for hackers):
TCP SYN scanning : 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 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, you immediately send a RST to tear down the connection (actually the 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. SYN scanning is the -s option of nmap.

2.3.4.1.2 Syn Fin Scan

41055 alerts with this signature among the files:
Earliest such alert at **00:57:59** *on 10/1*
Latest such alert at **19:10:47** *on 11/23*

TCP **SF**** scan	24 sources	22612 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
208.61.4.207	6634	6634	6634	6634
209.92.40.32	4956	4956	4956	4956
130.89.229.48	3860	3860	3860	3860
210.113.89.200	3565	3566	3565	3566
203.32.161.197	3545	3562	3545	3559

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.224.79	9	17	8	15
my.net.232.31	8	14	7	13
my.net.106.204	8	12	7	11
my.net.232.44	7	15	6	12
my.net.253.82	7	11	7	11

From Phrack 51 (An electronic magazine for hackers): **TCP FIN scanning** : There are times when even SYN scanning isn't clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like synlogger and Courtney are available to detect these scans. FIN packets, on the other hand, may be able to pass through unmolested. This scanning technique was featured in detail by Uriel Maimon in Phrack 49, article 15. The idea is that closed ports tend to reply to your FIN packet with the proper RST. Open ports, on the other hand, tend to ignore the packet in question. As Alan Cox has pointed out, this is required TCP behavior. However, some systems (notably Micro$oft boxes), are broken in this regard. They send RST's regardless of the port state, and thus they aren't vulnerable to this type of scan. It works well on most other systems I've tried. Actually, it is often useful to discriminate between a *NIX and NT box, and this can be used to do that. FIN scanning is the -U (Uriel) option of nmap.

Correlation:
The following is a syn-fin packet from OOSsche2.txt:
10/03-08:56:32.939829 209.92.40.32:9704 -> MY.NET.178.139:9704
TCP TTL:28 TOS:0x0 ID:39426
SF** Seq: 0x616D05EC Ack: 0x43BA486E Win: 0x404
00 00 00 00 00 00 .....
This host continued to scan over 5000 hosts with port 9704. After cross examining the GIAC web site. We see that port 9704 is a common backdoor port. GIAC has some similar traces:
Oct 29 23:39:49 router 30199: list 101 denied tcp 216.103.84.187(9704) -> a.b.193.101(9704), 1 packet
Oct 29 23:39:49 router 30200: list 101 denied tcp 216.103.84.187(9704) -> a.b.193.124(9704), 1 packet

The following website talks about the backdoor that is placed on a machine after a common rpc.statd attack: http://www.cert.org/advisories/CA-2000-17.html.

2.3.4.1.3 UDP Scan

22330 alerts with this signature among the files:

Earliest such alert at **01:57:45** *on 9/27*
Latest such alert at **21:15:34** *on 11/23*

UDP scan	79 sources	1406 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
63.248.55.245	8561	8561	9	9
24.9.152.152	4702	4702	1	1
my.net.5.25	2311	2311	559	559
128.61.37.65	1535	1535	4	4
my.net.1.3	559	559	4	4

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.218.50	4702	4710	1	9
my.net.206.94	1784	1798	2	16
my.net.120.36	1586	1590	9	13
my.net.205.214	1584	1589	1	6
my.net.215.210	1360	1367	1	8

From Phrack 51 (An electronic magazine for hackers):
UDP ICMP port unreachable scanning : This scanning method varies from the above in that we are using the UDP protocol instead of TCP. While this protocol is simpler, scanning it is actually significantly more difficult. This is because open ports don't have to send an acknowledgement in response to our probe, and closed ports aren't even required to send an error packet. Fortunately, most hosts do send an ICMP_PORT_UNREACH error when you send a packet to a closed UDP port. Thus you can find out if a port is NOT open, and by exclusion determine which ports which are. Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners of this sort must also implement retransmission of packets that appear to be lost (or you will get a bunch of false positives). Also, this scanning technique is slow because of compensation for machines that took RFC 1812 section 4.3.2.8 to heart and limit ICMP error message rate. For example, the Linux kernel (in net/ipv4/icmp.h) limits destination unreachable message generation to 80 per 4 seconds, with a 1/4 second penalty if that is exceeded. At some point I will add a better algorithm to nmap for detecting this. Also, you will need to be root for access to the raw ICMP socket necessary for reading the port unreachable. The -u (UDP) option of nmap implements this scanning method for root users.

UDP recvfrom() and write() scanning : While non-root users can't read port unreachable errors directly, Linux is cool enough to inform the user indirectly when they have been received. For example a second write() call to a closed port will usually fail. A lot of scanners such as netcat and Pluvius' pscan.c does this. I have also noticed that recvfrom() on non-blocking UDP sockets usually return EAGAIN ("Try Again", errno 13) if the ICMP error hasn't been received, and ECONNREFUSED ("Connection refused", errno 111) if it has. This is the technique used for determining open ports when non-root users use -u (UDP). Root users can also use the -l (lamer UDP scan) options to force this, but it is a really dumb idea.

2.3.4.2 Summary of the possible exploit from the Snort Alerts:

110534 alerts found among the file: Alert.txt
Earliest alert at **00:00:52**.873106 *on 09/26*
Latest alert at **23:32:20**.988483 *on 11/22*

Signature (click for definition)	# Alerts	# Sources	# Destinations	Previous # of Alerts
Happy 99 Virus	2	2	2	2
site exec - Possible wu-ftpd exploit - GIAC000623	6	4	4	2
Tiny Fragments - Possible Hostile Activity	7	5	6	12
?SITE EXEC - Possible wu-ftpd exploit - GIAC000623	7	1	4	6
External RPC call	13	8	3	40
Probable NMAP fingerprint attempt	15	14	13	64
connect to 515 from inside	56	2	3	0
SUNRPC highport access!	60	13	12	64
NMAP TCP ping!	96	21	20	138
Queso fingerprint	142	29	58	54
SMB Name Wildcard	218	33	33	338
Null scan!	283	204	196	181
SNMP public access	468	23	1	922
Back Orifice	1697	40	932	0
Broadcast Ping to subnet 70	1813	216	1	0
Attempted Sun RPC high port access	2542	20	33	1990
TCP SMTP Source Port traffic	2893	4	2836	0
WinGate 1080 Attempt	4802	570	2655	6193
Watchlist 000222 NET-NCFC	8166	45	26	19478
Watchlist 000220 IL-ISDNNET-990517	30998	61	108	5276
SYN-FIN scan!	56250	30	25751	5457

2.3.4.2.1 Happy 99

2 alerts with this signature among the files:
Earliest such alert at **03:59:51**.460766 *on 10/05*
Latest such alert at **16:06:44**.170359 *on 11/06*

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	1	1	1	1
216.6.117.11	1	1	1	1

Destinations receiving this attack signature

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

Snort Signature:
alert tcp any any -> $HOME_NET any (msg:"Happy99 Virus"; content:"X-Spanska\:Yes";)

Information about Virus:
W32/Ska is a worm that was first posted to several newsgroups and has been reported to several of the AVERT Labs locations worldwide. When this worm is run it displays a message "Happy New Year 1999!!" and displays "fireworks" graphics. The posting on the newsgroups has lead to its propagation. It can also spread on its own, as it can attach itself to a mail message and be sent unknowingly by a user. To learn more about this virus please see the following web page:
http://vil.mcafee.com/dispVirus.asp?virus_k=10144&

Correlation:
On our previous report we also found 2 alerts. These have been incoming emails, so the risk is low.
Host **209.94.224.12** : Official name: **server9.vonl.com**
Host **216.6.117.11** : Official name: **mail.hyperia.com**

Recommendation:
This alert was destined for mail servers internally. Make sure that the anti-virus program that is on these mail servers protect against the happy 99 virus.

2.3.4.2.2 site exec - Possible wu-ftpd exploit - GIAC000623

13 alerts with this signature among the files:
Earliest such alert at **06:17:23**.004770 *on 10/01*
Latest such alert at **16:57:49**.491247 *on 10/16*

site exec - Possible wu-ftpd exploit - GIAC000623	5 sources	8 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
208.61.44.215	9	9	6	5
24.31.88.99	2	2	1	1
202.9.188.89	1	1	1	1
63.202.13.20	1	6	1	6

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.130.242	3	4	1	2
my.net.205.94	2	11	1	8
my.net.221.82	2	3	1	2
my.net.205.94	2	11	2	8
my.net.97.206	1	9	1	8

Snort Signature:
alert tcp any any -> $HOME_NET 21 (msg:"site exec – Possible wu-ftpd exploit – GIAC000623"; content:"site exec";)

Information about attack:
An attempt has been made to exec a command on an ftp server. Some old versions of wu-ftpd 2.4 and earlier were vulnerable to remote compromise due to poor security restrictions of the site exec command. To find out more information about this alert, please see the following web pages:
http://www.whitehats.com/info/IDS317
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0080

Correlation:
On our previous report we found 8 alerts making this alert an increase of 162%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **63.202.13.20**: Official name: **adsl-63-202-13-20.dsl.snfc21.pacbell.net**
Registrant:
Pacific Bell Internet Services (PACBELL2-DOM)
303 Second Street Suite 830
San Francisco, CA 94107
Pacific Bell Internet Services,Inc. (NETBLK-PBI-NET-7) PBI-NET-7
63.192.0.0 - 63.207.my.net
Tim Kay (NETBLK-SBCIS-10036-13751) SBCIS-10036-13751
63.202.13.16 - 63.202.13.23

This host has also done several Queso scans on 5 different computers. It looks like this attacker is doing queso fingerprinting to find out what operating system the host is using to then exploit them. These attacks also happened within a few minutes of each other. The attacker could have been doing random scans or could have known that each of these hosts had ftp servers running.

10/04-11:56:00.850049 [**] Queso fingerprint [**] 63.202.13.20:1187-> my.net.100.127:21
10/04-11:56:14.289566 [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**] 63.202.13.20:1188-> my.net.100.209:21
10/04-11:56:27.511836 [**] Queso fingerprint [**] 63.202.13.20:1190-> my.net.130.98:21
10/04-11:56:46.630183 [**] Queso fingerprint [**] 63.202.13.20:1192-> my.net.163.17:21
10/04-11:57:24.186779 [**] Queso fingerprint [**] 63.202.13.20:1196-> my.net.205.94:21
10/04-11:57:46.592127 [**] Queso fingerprint [**] 63.202.13.20:1198-> my.net.214.186:21

Recommendation:
Take a closer look at these machines and make sure they are secure. If they have a ftp server running, make sure that tcpwrappers is installed.

.

2.3.4.2.3 Tiny Fragments - Possible Hostile Activity

7 alerts with this signature among the files:
Earliest such alert at **21:25:17**.293957 *on 09/26*
Latest such alert at **14:39:19**.160234 *on 11/16*

Tiny Fragments - Possible Hostile Activity	5 sources	6 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
62.6.71.0	2	2	1	1
216.43.55.44	2	2	2	2
172.157.126.93	1	1	1	1
202.156.51.76	1	1	1	1
192.206.151.152	1	1	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.181.144	2	4	1	3
my.net.201.198	1	5	1	5
my.net.201.2	1	3	1	3
my.net.1.8	1	52	1	9
my.net.211.2	1	24	1	7

Snort Signature:
Packets that are smaller then a router would normally fragment a packet are detected by snort.

Information about attack:
Tiny Fragments are used to try and evade Intrusion detection systems.

Correlation:
On our previous report we found 12 alerts making this alert decreased by 42%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **62.6.71.0**:This host is invalid. This is the network address for the network 62.6.71.0. This has to have been spoofed. We see no other correlations to this address at this time.

Host **216.43.55.44** : Official name: **ats-3ccpe-0806.mcleodusa.net**
Registrant:
McLeod, Inc (MCLEODUSA2-DOM)
6400 C Street SW
P.O. Box 3177
Cedar Rapids, IA 52406-3177 US
Domain Name: MCLEODUSA.NET

Host **172.157.126.93** : Official name: **AC9D7E5D.ipt.aol.com**

Host **202.156.51.76** : Official name: **mcns76.docsis51.singa.pore.net**

Registrant:
SINGAPORE CABLE VISION LTD (PORE2-DOM)
2D AYER RAJAH CRESCENT
-, SINGAPORE 139938
Domain Name: PORE.NET
inetnum: 202.156.0.0 - 202.156.95.255
netname: SCVCABLENET-AP
descr: SINGAPORE CABLE VISION LTD
descr: SINGAPORE CABLE NETWORK PROVIDER

Host **192.206.151.152** : Official name: **tweety.tgrace.com**

Toronto Star Newspapers, Limited (NET-TORSTAR)
One Yonge Street, Corporate
Information Technology
Toronto, ON M5E 1E6
CA
Netname: TORSTAR
Netblock: 192.206.146.0 - 192.206.151.255

Recommendation:
Watch tiny fragment traffic to make sure it does not correlate with any other alerts.

2.3.4.2.4 External RPC call

9 alerts with this signature among the files:
Earliest such alert at **20:23:36**.018641 *on 10/10*
Latest such alert at **20:28:54**.871290 *on 11/10*

External RPC call	6 sources	3 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
63.162.239.69	3	3	3	3
211.46.110.81	2	2068	2	2048
24.23.151.112	1	1	1	1
12.34.21.196	1	1	1	1
24.7.227.215	1	1148	1	1144

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.6.15	5	59	5	7
my.net.100.130	3	8	3	5
my.net.15.127	1	4	1	4

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL 111 (msg: "IDS428/portmap-listing-111"; flags: A+; rpc: 100000,*,*;)

Information about attack:
A query was sent to the portmap daemon, requesting port information for rpc services.

Correlation:
On our previous report we found 40 alerts making this alert increased by 444%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host: **63.162.239.69** : Official name: **63_162_239_69.belz.com**
Registrant:
Belz Enterprises (BELZ-DOM)
100 Peabody Place Suite 1400
Memphis, TN 38103
Domain Name: BELZ.COM

Host: **211.46.110.81** :
inetnum: 211.42.0.0 - 211.51.my.net
netname: KRNIC-KR-23
descr: KRNIC
descr: Korea Network Information Center
This host has many alerts coming from it. Here is a list of them
SUNRPC highport access :1
External RPC Call :2
Syn-Fin Scan :276

TCP SMTP Source Port :1789
As you can see this person has been busy. All of these attacks started on 11/10 and continued for about 24 hours.

Host: **24.7.227.215** :
Host: **24.23.151.112** : Official name: **cx673530-a.vbch1.va.home.com**
Registrant:
Home Network (HOME-DOM)
425 Broadway St.
Redwood City, CA 94063 US
Domain Name: HOME.COM
Host: **12.34.21.196** :
CFS EUROPE LTD (NETBLK-CFSEUROPE18-21-192)
300 PEN CENTRE BOULEVARD SUITE 500
PITTSBURGH, PA 15235 US
Netname: CFSEUROPE18-21-192
Netblock: 12.34.21.192 - 12.34.21.223

The following is a trace from this host:

```
10/28-19:41:44.513820 [**] External RPC call [**] 12.34.21.196:700-> my.net.6.15:111
```

After searching SANS GIAC website we also found a correlation with this host on October 29th, one day after my.net was scanned. You can find it at the following web page: http://www.sans.org/y2k/110200-1230.htm. As you can see this attacker was also scanning someone else at the same time.

Oct 29 12:03:55 hostre rpcbind: refused connect from 12.34.21.196 to dump()
Oct 29 12:03:58 hostbe rpcbind: refused connect from 12.34.21.196 to dump()
Oct 29 12:10:31 hostmau portsentry[148]: attackalert: Connect from host: 12.34.21.196/12.34.21.196 to TCP port: 111
Oct 29 12:15:19 hostj snort[24697]: RPC Info Query: 12.34.21.196:901 -> z.y.w.66:111
Oct 29 12:15:20 hostmi snort[23025]: RPC Info Query: 12.34.21.196:905 -> z.y.w.98:111
Oct 29 12:43:55 hostp in.ftpd[12693]: connect from 12.34.21.196
Oct 29 12:43:56 hostp in.ftpd[12694]: connect from 12.34.21.196

Recommendation:
This is primarily reconnaissance, make sure all hosts are using tcpwrappers and watch for any correlation with any other type of attack.

2.3.4.2.5 Probable NMAP fingerprint attempt

15 alerts with this signature among the files:
Earliest such alert at **13:38:00**.767581 *on 10/06*
Latest such alert at **22:44:52**.018936 *on 11/22*

Probable NMAP fingerprint attempt	14 sources	13 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.95.192.51	2	2	1	1
24.69.214.58	1	1	1	1
193.231.207.72	1	1	1	1
128.54.203.218	1	1	1	1
24.9.64.57	1	1	1	1

Top 5 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.201.126	1	12	1	7
my.net.219.146	1	1	1	1
my.net.60.38	1	37	1	29

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "nmap fingerprint attempt"; flags: SFPU;)

Information about attack:
This alert indicates that a remote used the NMAP tool to attempt to determine the server operating system. OS Fingerprinting is a common practice and may provide useful information to an attacker. Typically this particular signature is only seen when probing an open TCP port. For additional information see the following web pages:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0454
http://www.whitehats.com/info/IDS05
http://www.sans.org/newlook/resources/IDFAQ/TCP_fingerprinting.htm

Correlation:
On our previous report we found 64 alerts making this alert decreased by 77%. The source and destination addresses have also changed. There are no reoccurring attacks.

Recommendation:
Watch for any correlations with any other attacks. This is only reconnaissance to gather information for the real attack.

2.3.4.2.6 connect to 515 from inside

56 alerts with this signature among the files:
Earliest such alert at **13:26:43**.509292 *on 11/19*
Latest such alert at **11:33:56**.296324 *on 11/22*

connect to 515 from inside	2 sources	3 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
my.net.101.142	54	54	1	1
my.net.179.78	2	2	2	2

Top 5 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	1	1	1	1
64.244.202.66	1	1	1	1

Snort Signature:
alert TCP $INTERNAL any -> any 515 (msg: "Connect to 515 from inside"; flags: A+;)

This signature is looking for all traffic going toward port 515 from inside.

Information about attack:
The alert is letting you know that there is internal traffic destined for port 515 the lpr service. The lpr service is a utility, which queues print jobs and submits them to a destination.

Correlation:
Port 515 scans are very popular and I found many systems that have been scanned on SANS web site. Here are a couple of links that show several scans:
http://www.sans.org/newlook/alerts/port515.htm
http://www.sans.org/y2k/112700-1400.htm

The following link has detailed information about a multiple vendor LPR format string vulnerability that was popular late last year.
http://www.securityfocus.com/bid/1711

Recommendation:
Unless absolutely needed, the lpr service should be turned off. If the lpr service cannot be turned off, then a version that supports tcpwrappers should be installed. A firewall should also be setup in front of the machine and only designated hosts should be able to get to this machine. Once these two protections are in place the attackers ip address should be placed in the hosts.deny file and in the firewall with deny all policy in place. This will protect allow protection at both the host and network.

2.3.4.2.7 SUNRPC highport access!

60 alerts with this signature among the files:
Earliest such alert at **13:28:03**.304676 *on 09/28*
Latest such alert at **03:50:53**.188444 *on 11/21*

SUNRPC highport access!	13 sources	12 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
216.10.12.30	33	33	2	2
216.148.218.160	6	6	1	1
205.188.3.211	4	4	1	1
24.18.90.197	3	3	2	2
195.34.28.117	3	9	1	3

Top 5 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	6	1	3
my.net.228.62	3	5	1	3
my.net.97.59	3	7	1	2

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL 32771 (msg: "SUNRPC highport access!"; flags: A+; rpc: 100000,*,*;)

Information about attack:
A query was sent to the rpcbind/portmap daemon on a Solaris machine, requesting port information for rpc services.

Correlation:
On our previous report we found 64 alerts making this alert decreased by 7%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **195.34.28.117**: Official name: **dialup-28117.dialup.ptt.ru**

inetnum: 195.34.28.0 - 195.34.28.255
netname: PTTNET-DIALUP3
descr: PTTNET Dialup network
country: RU
admin-c: SK6742-RIPE
tech-c: AVM1-RIPE

This is a Russian dialup account that is not only looking for SUNRPC high access ports, but is also looking for wingates. Most of this traffic is just reconnaissance and it would be wise to double-check these three hosts to make sure there is no open wingate (1080) or sunrpc (32771) ports.

10/14-12:16:30.632088 [**] WinGate 1080 Attempt [**] 195.34.28.117:2086-> my.net.97.59:1080
10/14-12:29:11.273137 [**] WinGate 1080 Attempt [**] 195.34.28.117:3156-> my.net.97.59:1080
10/14-12:29:16.379139 [**] SUNRPC highport access! [**] 195.34.28.117:3191-> my.net.97.59:32771
10/14-12:29:17.223784 [**] WinGate 1080 Attempt [**] 195.34.28.117:3156-> my.net.97.59:1080
10/14-12:33:34.298088 [**] SUNRPC highport access! [**] 195.34.28.117:3364-> my.net.97.59:32771
10/14-12:33:35.990374 [**] SUNRPC highport access! [**] 195.34.28.117:3364-> my.net.97.59:32771
10/14-15:14:08.468329 [**] WinGate 1080 Attempt [**] 195.34.28.117:1099-> my.net.60.38:1080
10/14-15:14:49.709770 [**] WinGate 1080 Attempt [**] 195.34.28.117:1132-> my.net.253.114:1080
10/14-15:15:14.416890 [**] WinGate 1080 Attempt [**] 195.34.28.117:1165-> my.net.253.114:1080

Recommendation:
Make sure all hosts are secure and watch for any future correlations with this host.

2.3.4.2.8 NMAP TCP ping!

94 alerts with this signature among the files:
Earliest such alert at **05:40:00**.709907 *on 09/26*
Latest such alert at **22:06:00**.355840 *on 11/22*

NMAP TCP ping!	21 sources	20 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
192.102.197.234	47	47	3	3
202.187.24.3	9	9	6	6
63.119.91.2	6	6	4	4
205.128.11.157	5	5	2	2
12.43.88.5	3	3	3	3

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.1.8	50	52	7	9
my.net.1.9	6	8	2	4
my.net.1.3	5	8	3	6
my.net.100.165	4	10	3	5
my.net.6.7	4	5808	3	14

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "nmap tcp ping"; ack: 0; flags: A;)

This signature looks for external traffic to an internal host with an acknowledgement of 0 with the acknowledgement flag set.

Information about attack:
A remote user has used the NMAP port-scanning tool to probe the server. This alert indicates that an NMAP TCP ping was sent to determine if a host is reachable. This unfortunately is also used for global server load balancing and as you can see from the below correlations, most of the alerts were from that and not NMAP.

Correlation:
On our previous report we found 202 alerts making this alert decreased by 54%.

Host: **192.102.197.234**: Official name: **geo197a.cps.intel.com**
The following is correlation from the GIAC web site on February 12, 2001:

This is in response to inquiries about suspicious network traffic coming to systems from IP address 192.102.197.234, also known as geo197a.cps.intel.com. geo197a is a geographic www load balancer. It performs a very intrusive and promiscuous method of determining which Web server in the www.intel.com pool is the closest server prior to serving data to a client that has asked to view www.intel.com. In other words, geo197a generated those packets in response to a user on the affected system accessing the www.intel.com Web site. There is nothing we can do about these

questionable packets'. It is the way in which our current product works. However, Intel will be replacing this product with a new geographic load balancing product in the near future, in large part because the current solution is so intrusive to external networks.

Jan 12 23:27:53 hostmi snort[318]: IDS28 - PING NMAP TCP:192.102.197.234:80 -> z.y.w.98:53
Jan 12 23:27:53 hostmi snort[318]: IDS28 - PING NMAP TCP:192.102.197.234:53 -> z.y.w.98:53
Jan 27 12:04:20 hostj snort[488]: IDS28 - PING NMAP TCP:192.102.197.234:80 -> z.y.w.66:53
Jan 27 12:04:20 hostj snort[488]: IDS28 - PING NMAP TCP:192.102.197.234:53 -> z.y.w.66:53
Jan 27 15:42:44 hostmi snort[318]: IDS28 - PING NMAP TCP:192.102.197.234:80 -> z.y.w.98:53
Jan 27 15:42:44 hostmi snort[318]: IDS28 - PING NMAP TCP:192.102.197.234:53 -> z.y.w.98:53
Feb 7 15:46:57 hostmi snort[10550]: IDS28 - PING NMAP TCP:192.102.197.234:80 -> z.y.w.98:53
Feb 7 15:46:57 hostmi snort[10550]: IDS28 - PING NMAP TCP:192.102.197.234:53 -> z.y.w.98:53
Feb 9 10:09:21 hostmi snort[10550]: IDS28 - PING NMAP TCP:192.102.197.234:80 -> z.y.w.98:53
Feb 9 10:09:21 hostmi snort[10550]: IDS28 - PING NMAP TCP:192.102.197.234:53 -> z.y.w.98:53

Host: **202.187.24.3**:

inetnum:	202.187.24.0 - 202.187.24.255
netname:	JARING-UNITAR2
descr:	Universiti Tun Abdul Razak
descr:	Plaza CCL, Jalan SS 6/12
descr:	Kelana Jaya Urban Centre
descr:	47300 Petaling Jaya Selangor
country:	MY

Host: **63.119.91.2**:
UUNET Technologies, Inc. (NETBLK-UUNET63)
3060 Williams Drive, Suite 601
Fairfax, Virginia 22031
Netname: UUNET63
Netblock: 63.64.0.0 - 63.127.my.net
Host **12.43.88.5** :
AT&T ITS (NET-ATT) ATT
12.0.0.0 - 12.my.net.255
ARCHER DANIELS MIDLAND (NETBLK-ADMWORLD551-88) ADMWORLD551-88
12.43.88.0 - 12.43.91.255

Host **205.128.11.157**: Official name: **atl-lb2.headhunter.net**
Registrant:
Headhunter.net, Inc (HEADHUNTER23-DOM)
333 Research Court, Suite 333
Norcross, GA 30092
US
This host was also seen on our previous report with 35 alerts to my.net.1.8. Again we see this host probing the same host with a source port 53 and a destination port 53, but it has decreased to 5 alerts. This host has no other correlations with any other type of alerts. By a look at the hostname it is probably one of two things. 1. www.headhunter.net is doing global server load balancing and it is doing a ping to determine which server is closer or 2. A hacker owns this server. Because there is only traffic going to and from this port with no other correlations, I would assume that it is probably 1. The web server is doing global server load balancing.

My assumption was correct. After searching the GIAC web site. I found this response after an administrator from headhunter.net was contacted.

> Aug 4, 2000 205.128.11.157
> Response ("The probes are sent from our geographic load balancing devices, trying to determine your proximity and latency to our different locations. This is by design.")

Host **my.net.1.8**:
This host on your network has been the center of nmap attacks in the past and it continues to be the center of attacks. Most of the nmap pings are from source port 80(http) or 53(DNS) to ports 80(http) or 53(DNS). This is done because many firewalls allow ports 80 and 53 through them.

Recommendation:
Nmap scans are primarily reconnaissance. Watch for any other types of alerts that go along with this.

2.3.4.2.9 Queso fingerprint

142 alerts with this signature among the files:
Earliest such alert at **04:27:59**.343599 *on 09/26*
Latest such alert at **16:10:36**.268157 *on 11/22*

Queso fingerprint	29 sources	58 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.3.161.193	45	45	2	2
195.115.7.2	22	22	1	1
129.242.219.27	19	24	18	22
64.80.63.121	15	15	9	9
24.163.42.82	8	8	1	1

Top 5 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	11	1	4
my.net.227.10	5	13	1	2
my.net.227.118	4	6	1	3

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "Queso Fingerprint"; flags: S12;)

This signature is looking for external traffic to any internal host with flags S,1 and 2 set.

Information about attack:
A remote user has used the Queso tool to determine the OS fingerprint of the server. This can be a false positive because of the Explicit Congestion Notification (ECN) proposed standard. ECN is a standard proposed by the IETF that will cut down on network congestion and routers dropping packets by using flags 1 and 2. Because Queso also uses these flags, it could make this a false positive.

Correlation:
On our previous report we found 54 alerts making this alert increased by 262%.

Host **24.3.161.193**: Official name: **cc287787-b.union1.nj.home.com**
Registrant:
Home Network (HOME-DOM)
425 Broadway St.
Redwood City, CA 94063 US
@Home Network (NETBLK-ATHOME) ATHOME
24.0.0.0 - 24.23.my.net
@Home Network (NETBLK-NJ-COMCAST-UNION-1) NJ-COMCAST-UNION-1
24.3.160.0 - 24.3.175.255

This host was also seen in our last report. This machine had the top number of alerts (20). As we can see this machine has increased by over 100%. It has also been seen on Sep 29 in the GIAC posting at http://www.sans.org/y2k/100200.htm for the same traffic.
All Traffic is going to 2 hosts:
My.net.145.9 port 110(pop3)
My.net.253.112 port 443(https/SSL)

Host **129.242.219.27**: Official name: **nonet.td.org.UiT.No**
University of Tromso (NET-UITNET)
N-9001 Tromso NORWAY
Netname: UITNET
Netblock: 129.242.0.0 - 129.242.my.net

We have also seen this host performing numerous wingate attempts.

09/26-10:40:22.147119 [**] WinGate 1080 Attempt [**] 129.242.219.27:3285-> my.net.206.254:1080
09/26-16:22:36.048566 [**] WinGate 1080 Attempt [**] 129.242.219.27:1245-> my.net.206.254:1080
10/05-14:41:43.659469 [**] WinGate 1080 Attempt [**] 129.242.219.27:1339-> my.net.60.8:1080
10/20-20:18:33.763632 [**] WinGate 1080 Attempt [**] 129.242.219.27:3782-> my.net.53.133:1080
10/23-17:36:10.880372 [**] WinGate 1080 Attempt [**] 129.242.219.27:3962-> my.net.225.178:1080
10/28-17:08:22.282509 [**] Queso fingerprint [**] 129.242.219.27:3721-> my.net.222.50:23
10/28-22:40:42.546522 [**] Queso fingerprint [**] 129.242.219.27:3216-> my.net.97.181:113
10/30-11:55:31.927807 [**] Queso fingerprint [**] 129.242.219.27:3169-> my.net.60.38:23
10/30-15:37:30.479585 [**] Queso fingerprint [**] 129.242.219.27:4655-> my.net.215.150:23
10/31-05:35:01.742339 [**] Queso fingerprint [**] 129.242.219.27:3681-> my.net.98.119:1080
10/31-07:29:04.668481 [**] Queso fingerprint [**] 129.242.219.27:2787-> my.net.219.30:1080
10/31-15:03:58.385633 [**] Queso fingerprint [**] 129.242.219.27:4075-> my.net.60.11:1080
10/31-19:11:48.174953 [**] Queso fingerprint [**] 129.242.219.27:3585-> my.net.208.134:1080
11/01-23:45:54.325018 [**] Queso fingerprint [**] 129.242.219.27:2844-> my.net.210.246:1080
11/04-20:37:51.624439 [**] Queso fingerprint [**] 129.242.219.27:4268-> my.net.203.170:1080
11/10-14:18:26.690898 [**] Queso fingerprint [**] 129.242.219.27:1190-> my.net.53.153:1080
11/10-21:29:38.826875 [**] Queso fingerprint [**] 129.242.219.27:2705-> my.net.98.213:23
11/14-01:36:56.084925 [**] Queso fingerprint [**] 129.242.219.27:3674-> my.net.218.14:113
11/16-00:36:17.682642 [**] Queso fingerprint [**] 129.242.219.27:4528-> my.net.97.172:1080
11/16-13:05:59.510460 [**] Queso fingerprint [**] 129.242.219.27:2576-> my.net.60.38:23
11/17-22:29:44.504676 [**] Queso fingerprint [**] 129.242.219.27:1889-> my.net.218.134:1080
11/19-10:59:03.175139 [**] Queso fingerprint [**] 129.242.219.27:1465-> my.net.98.106:1080
11/19-12:52:28.371298 [**] Queso fingerprint [**] 129.242.219.27:1372-> my.net.97.176:23
11/22-11:31:27.940073 [**] Queso fingerprint [**] 129.242.219.27:3486-> my.net.105.120:23

Recommendation:
Queso scans are primarily reconnaissance. Watch for any other types of alerts that go along with this.

2.3.4.2.10 SMB Name Wildcard

208 alerts with this signature among the files:
Earliest such alert at **11:19:08**.075062 *on 10/01*
Latest such alert at **09:27:51**.910085 *on 11/22*

SMB Name Wildcard	33 sources	33 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
my.net.101.160	83	83	1	1
141.157.99.21	33	33	1	1
169.254.184.161	24	24	9	9
141.157.98.201	20	22	1	2
my.net.98.154	5	5	4	4

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.101.192	83	485	1	20
my.net.6.15	53	59	2	7
my.net.101.53	9	9	5	5
my.net.101.117	7	7	3	3
my.net.101.153	7	7	4	4

Information about attack:
SMB Wildcard alerts indicate a query for netbios information when only an IP address is known, and typically can be regarded as a reconnaissance effort when coming from an external IP address.

Correlation:
On our previous report we found 338 alerts making this alert decreased by 39%.

Host: **my.net.101.160**: This is an internal address that is either compromised or misconfigured. This host was also sending out traffic in our last report. The traffic has gone down, but there is still a substantial amount of traffic coming from it.

Host **141.157.99.21**: Official name: **adsl-141-157-99-21.bellatlantic.net**

Host **169.254.184.161**:

For use with Link Local Networks
Information Sciences Institute
University of Southern California
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6695
Netname: LINKLOCAL
Netblock: 169.254.0.0 - 169.254.my.net

Host **141.157.98.201**: Official name: **adsl-141-157-98-201.bellatlantic.net**

Host: **my.net.98.154**: This is also an internal address that is either compromised or misconfigured. This host however was not sending out traffic in our last report.

Recommendation:
Find out why there is still traffic coming from these internal hosts and make sure there are no misconfigured smb workstations.

2.3.4.2.11 Null scan!

277 alerts with this signature among the files:
Earliest such alert at **10:58:55**.817608 *on 09/26*
Latest such alert at **20:33:10**.371736 *on 11/22*

Null scan!	199 sources	192 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.113.148.32	8	8	1	1
128.253.247.116	8	13	2	2
24.112.150.20	8	9	1	1
128.195.229.11	7	7	2	2
24.200.14.91	5	5	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.105.120	8	17	1	7
my.net.218.46	8	11	2	4
my.net.214.166	8	10	1	3
my.net.227.10	7	13	1	2
my.net.210.238	5	10	2	6

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "IDS4/probe-null_scan"; seq: 0; ack: 0; flags: 0;)

Information about attack:
A TCP frame has been seen with a sequence number of zero and all control bits are set to zero. This frame should never be seen in normal TCP operation. An attacker may be scanning your system by sending these specially formatted frames to see what services are available.
For more information about this alert, please see the following web site.
http://www.whitehats.com/info/IDS04

Correlation:
On our previous report we found 181 alerts making this alert increased by 35%. The source and destination addresses have also changed. There are no reoccurring attacks between reports. Null Scans however are very popular. Here is a log from the GIAC web page http://www.sans.org/y2k/020800-2300.htm.

[**] Null scan! [**]

02/01-03:10:20.015000 195.231.146.190:1899 -> 192.0.212.70:6699

[**] Null scan! [**]

02/01-03:14:16.605248 132.230.178.52:1565 -> 192.0.208.14:4759

Host **128.53.247.116**: Official name: **tls16.resnet.cornell.edu**
Here is more information about the host, as you can see it came from a dorm room at Cornell University.

Registrant:
Cornell University (CORNELL-DOM)
Cornell Information Technologies
Network Operations Center 100 CCC
Ithaca, NY 14853 US
Domain Name: CORNELL.EDU
Netname: CCS-NET
Netblock: 128.253.0.0 - 128.253.my.net

This host was also seen with other alerts. As you can see from the following log, this host first did several null scans against host my.net.227.10 ports 3516 and 4053 and then did a queso scan. You can also see that the source port for most of the packets is either 3932 or 2720 which tells us that it is a crafted packet.

```
09/27-06:29:50.123638 [**] Null scan! [**] 128.253.247.116:3932-> my.net.227.10:3516
09/27-06:31:53.537498 [**] Null scan! [**] 128.253.247.116:3932-> my.net.227.10:3516
09/27-06:47:53.927904 [**] Null scan! [**] 128.253.247.116:3932-> my.net.227.10:3516
09/27-06:48:11.609172 [**] Null scan! [**] 128.253.247.116:3932-> my.net.227.10:3516
09/27-07:00:24.679328 [**] Null scan! [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:08:11.831023 [**] Queso fingerprint [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:29:27.932023 [**] Null scan! [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:31:17.992797 [**] Queso fingerprint [**] 128.253.247.116:26-> my.net.227.10:2720
09/27-07:39:10.634903 [**] Null scan! [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:39:46.418105 [**] Queso fingerprint [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:46:58.309049 [**] Queso fingerprint [**] 128.253.247.116:2720-> my.net.227.10:4053
09/27-07:53:19.530143 [**] Queso fingerprint [**] 128.253.247.116:0-> my.net.227.10:2720
11/13-03:15:55.888279 [**] Null scan! [**] 128.253.247.116:20-> my.net.218.34:1376
```

After searching the GIAC website we also found this host doing the following scan:
Sep 29 06:49:47 128.253.247.116:1388 -> MY.NET.219.250:3799 NOACK **S****U

Recommendation:
Watch null scans to see if they correlate with any other alerts. Make sure that no trojans are installed on these workstations.

2.3.4.2.12 SNMP public access

402 alerts with this signature among the files:
Earliest such alert at **11:17:47**.004982 *on 10/01*
Latest such alert at **17:32:56**.420810 *on 11/19*

SNMP public access	19 sources	1 destinations

Top 5 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

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.101.192	402	485	19	20

Snort Signature:
alert UDP any any -> any 161 (msg: "SNMP public access"; content: "public";).

Information about attack:
This attack is probably not an attack but a snmp device sending a trap back to the network manager.

Correlation:
On our previous report we found 922 alerts making this alert decreased by 57%. The source hosts are probably sending traps back to a snmp server at my.net.101.192.

Recommendation:
Make sure the host.deny and host.allow files are properly configured on host my.net.101.192 to receive traps from only specified hosts. Also, it would be wise to change the community name to something different then "public".

2.3.4.2.13 Back Orifice

1680 alerts with this signature among the files:
Earliest such alert at **15:01:27**.048398 *on 10/01*
Latest such alert at **03:16:06**.961852 *on 11/21*

Back Orifice	39 sources	931 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
62.136.90.120	306	306	189	189
63.46.46.143	291	291	291	291
203.148.182.108	111	111	100	100
213.43.69.72	99	99	91	91
203.155.130.111	79	79	72	72

Top 5 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.97.142	6	8	3	5
my.net.98.82	6	8	4	6
my.net.98.81	6	9	5	8

Snort Signature:
alert UDP $EXTERNAL any -> $INTERNAL 31337 (msg: "Back Orifice";)

Information about attack:
This event indicates an attempt to connect to the default port for the Back Orifice trojan. This is a probe and does not necessarily indict compromise.
Back Orifice 2000 (BO2K) is advertised as "a best-of-breed network administration tool, granting sysadmins access to every Windows machine on their network. Using Back Orifice 2000, network administrators can perform typical desktop support duties without ever leaving their desk (5)." But is it really an administrative tool? Why would an administration tool provide stealth installation techniques?
For more information about Back Orifice, please refer to the following web site:
http://www.sans.org/infosecFAQ/malicious/back_orifice.htm

Correlation:
On our previous report we found 0 alerts making this alert increased by 100%. We have seen lots of international traffic of attackers scanning for machines that are infected with back orifice.
After searching the GIAC web site, I found similar traffic during the same time period.
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.c.170:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.c.225:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.d.237:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.d.244:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.e.52:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.e.166:31337 UDP
Oct 6 21:57:05 128.186.123.79:1745 -> a.b.e.243:31337 UDP

Host **62.136.90.120** : Official name: **modem-120.dextroamphetam.dialup.pol.co.uk**
route: 62.136.0.0/15
descr: Planet Online Limited
descr: The White House
descr: Melbourne St.
descr: Leeds LS2 7PS United Kingdom
origin: AS5388
mnt-by: AS5388-MNT
changed: matthew@planet.net.uk 19990521
source: RIPE

Host: **63.46.46.143** : **1Cust143.tnt2.sierra-vista.az.da.uu.net**
Registrant:
UUNET Technologies, Inc. (UU-DOM)
3060 Williams Drive Ste 601
Fairfax, VA 22031
USA
Domain Name: UU.NET
Netname: NETBLK-UUNET97DU
Netblock: 63.0.0.0 - 63.63.my.net
Maintainer: UUDA

Host: **203.148.182.108** :
inetnum: 203.148.160.0 - 203.148.191.255
netname: ANET-TH
descr: A-Net Co., Ltd.
descr: ISP
country: TH
admin-c: PR2-TH
rev-srv: ns.a-net.net.th
address: A-Net Co.,Ltd
address: 23 Charoen Nakorn 14Rd.
address: Klongsan, Bangkok Thailand

Host: **213.43.69.72**: Official name: **NAS-213-43-69-72.ixir.com**
Registrant:
ixir (IXIR3-DOM)
Dogus Holding, Istinye Yokusu
Istanbul, 0 80860
TR
inetnum: 213.43.0.0 - 213.43.128.255
netname: IXIR
Domain Name: IXIR.COM

Host: **203.155.130.111** : Official name: **l130ppp111.ksc.net.th**
domain: KSC.NET.TH
descr: Changing NS which has authority to manage domain
company: Internet KSC Co.,Ltd
address: 333 Laksi-Plaza Tower I, 12nd Fl.
address: Changwata Rd,Donmuang
city: Bangkok
inetnum: 203.155.128.0 - 203.155.135.255

Recommendation:
Watch traffic to see if any hosts get a lot of traffic or correlations with other alerts.

2.3.4.2.14 Broadcast Ping to subnet 70

1811 alerts with this signature among the files:
Earliest such alert at **14:48:07**.021725 *on 10/03*
Latest such alert at **03:52:13**.369033 *on 11/17*

Broadcast Ping to subnet 70	215 sources	1 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
193.231.169.166	88	88	1	1
193.226.60.179	55	55	1	1
193.231.220.101	50	50	1	1
213.154.131.131	49	49	1	1
193.231.220.71	43	43	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.70.255	1811	1811	215	215

Snort Signature:
Alert icmp any any -> my.net.70.255 any (msg: “Broadcast Ping to subnet 70”;)

Information about attack:
If this address responds to pings then it can be used in a smurf attack.

Correlation:
On our previous report we found 0 alerts making this alert increased by 100%. We also found no correlation to these hosts.

Host: **193.231.169.166** :
inetnum: 193.231.169.0 - 193.231.169.255
netname: MEDIASAT
descr: Media Sat S.A.
country: RO

Host: **193.226.60.179** :
inetnum: 193.226.60.0 - 193.226.60.255
netname: ANATOMIE-NET
descr: Universitatea Ovidius - Facultatea de Medicina - Catedra de anatomie
country: RO

Host: **193.231.220.101** : Official name: **ppp220101.fx.ro**
Host: **193.231.220.71** : Official name: **ppp220071.fx.ro**
inetnum: 193.231.208.0 - 193.231.223.255
netname: FX-NET
descr: FX Internet - One Trading Group
descr: Burebista 1, bl. D15, sc. 3
descr: Bucuresti 3, Romania

Host: **213.154.131.131** : Official name: **ns.endzone.ro**

inetnum: 213.154.131.0 - 213.154.134.255
netname: PCNET
descr: PCNET - ATM-ADSL Network
country: RO

This name server is probably compromised by a hacker. There is no reason why a name server would be sending pings to a broadcast address.

Recommendation:
Very Interesting traffic. The top 5 source addresses are all from Romania. Configure screening router to not allow packets destined for this broadcast address.

2.3.4.2.15 Attempted Sun RPC high port access

2542 alerts with this signature among the files:
Earliest such alert at **08:34:21**.306733 *on 09/26*
Latest such alert at **20:58:24**.675341 *on 11/22*

Attempted Sun RPC high port access	20 sources	33 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
205.188.153.108	628	628	4	4
205.188.153.107	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

Top 5 Destinations receiving this attack signature

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

Information about attack:

Attempts to access RPC ports are of a concern because there are several well-known buffer overflow vulnerabilities in various RPC programs. Port map is usually consulted to determine what programs are running on the host before attempting to exploit a vulnerability in one of the programs that is reported.

Correlation:
On our previous report we found 2094 alerts making this alert decreased by 18%.

Host **205.188.153.107** : Official name: **fes-d011.icq.aol.com**
Host **205.188.153.108** : Official name: **fes-d012.icq.aol.com**
Host **205.188.153.109** : Official name: **fes-d013.icq.aol.com**
Host **205.188.153.116** : Official name: **fes-d020.icq.aol.com**
Host **205.188.153.101** : Official name: **fes-d005.icq.aol.com**
These addresses are all from AOL's program ICQ.

America Online, Inc (NETBLK-AOL-DTC)
22080 Pacific Blvd
Sterling, VA 20166 US
Netname: AOL-DTC
Netblock: 205.188.0.0 - 205.188.my.net

I would like to refer back to our previous report where we gave you the following information about this activity:

Almost all the high port accesses come from ICQ servers and the rest of the source ports are not known trojan ports. At the following URL we have evidence of an ICQ worm, which would produce a connection profile similar to this one: http://archives.neohapsis.com/archives/bugtraq/1999-q3/1514.html. At this URL Blue Boar, who moderates the Vuln-Dev mailing list at Securityfocus.com, describes the ICQ worm's workings. Further, we find more details about an ICQ trojan at http://www.simovits.com/trojans/tr_data/y463.html and at http://www.canada.cnet.com/news/0-1005-200-114889.html?tag=st.

Lastly, the URL http://dark-e.com/archive/trojans/icqr/index.html describes a remote access trojan called ICQ relay, which runs on Windows systems. While no ICQ trojans could be located that masquerade as ICQ for Linux or Unix, it is surely only a matter of time and is likely already out there in the wild somewhere.

The evidence here suggests a problem with ICQ, since ICQ has no business connecting to Rusersd. When turned on, Rusersd will announce what users are logged onto a Unix system, and provide a facility that is not used by ICQ (and if it is, it shouldn't be). The destination systems are most likely to be Linux systems that are running the Linux version of ICQ for KDE, since Windows systems don't come equipped with rusersd. Chat services that allow file transfers, such as Wrapster, ICQ, IRC and AIM, should ideally be proxied through servers with DCC turned off to prevent the spread of trojan files through them.

2.3.4.2.16 TCP SMTP Source Port traffic

2893 alerts with this signature among the files:
Earliest such alert at **13:10:15**.618101 *on 10/23*
Latest such alert at **20:09:16**.403626 *on 11/19*

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	1789	2068	1789	2048
24.7.227.215	1096	1148	1096	1144
194.67.168.11	6	6	6	6
194.88.77.240	2	2	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.104.129	2	2	2	2
my.net.60.134	2	2	2	2
my.net.142.23	2	4	2	4
my.net.26.94	2	5	2	5
my.net.112.208	2	3	2	3

Snort Signature:
alert TCP $INTERNAL 25 -> $EXTERNAL any (msg: "TCP SMTP Source Port traffic";)

Information about attack:
Attackers try to disguise as smtp traffic because a lot of screening routers allow SMTP traffic into their mail servers.

Correlation:
On our previous report we found 922 alerts making this alert decreased by 313%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **211.46.110.81** :

inetnum: 211.42.0.0 - 211.51.my.net
netname: KRNIC-KR-23
descr: KRNIC
descr: Korea Network Information Center

Host **24.7.227.215** :

@Home Network (NETBLK-ATHOME) ATHOME
24.0.0.0 - 24.23.my.net
@Home Network (NETBLK-BB1-RDC2-TX-2) BB1-RDC2-TX-2
24.7.224.0 - 24.7.239.255

Host **194.67.168.11** :

inetnum: 194.67.168.8 - 194.67.168.15
netname: RELSOFT
descr: Relsoft network. Web portal.
descr: RMT hosting
country: RU

Host **194.88.77.240** : Official name: **monopoly.fulham.vi.net**

Registrant:
VIRTUAL INTERNET DIRECT LIMITED (VI14-DOM)
ELYSIUM HOUSE, 126-128 NEW KINGS ROAD
LONDON, SW6 4LZ, UK
Domain Name: VI.NET
inetnum: 194.88.76.0 - 194.88.79.255
netname: LONDON1-DIAL-POOL2
descr: Level 3 Communications: Managed Modem address space
country: GB

Recommendation:
Make sure all SMTP daemons in the above list are configured properly.

2.3.4.2.17 WinGate 1080 Attempt

4727 alerts with this signature among the files:
Earliest such alert at **00:00:52**.873106 *on 09/26*
Latest such alert at **23:32:20**.988483 *on 11/22*

WinGate 1080 Attempt	550 sources	2637 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
63.193.210.208	1883	1883	1837	1837
208.194.161.155	217	217	100	100
198.63.2.192	179	179	9	9
204.117.70.5	149	149	35	35
64.86.5.250	136	136	68	68

Top 5 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	123	124	5	6
my.net.60.11	74	77	43	46
my.net.60.8	66	72	37	43
my.net.60.16	38	40	22	23

Snort Signature:
alert tcp $EXTERNAL_NET !53 -> $HOME_NET 1080 (msg:"MISC-WinGate-1080-Attempt";flags:S;)

Information about attack:
Someone is scanning your system to see if it is running SOCKS. This may be a hacker that desires to "bounce" traffic through your system at other people. It may also be a chat server trying to determine if someone is indeed bouncing through your system to chat anonymously.

Correlation:
On our previous report we found 6193 alerts making this alert decreased by 24%.

Host **216.176.130.250**: Official name**: finger-for-port-scan-info-at-hebron.in.us.dal.net**
Registrant:
DALnet (DAL2-DOM)
6755 Mira Mesa Blvd. Ste. 123, #130
San Diego, CA 92121 US
Domain Name: DAL.NET
This host was no longer in the top 5 but it was seen as a top 5 in the previous report. It still was seen but with only 7 attempts. All 7 servers were not any of the previous servers that were scanned. By the name and the registrant, it is probably an irc server that is fingering the host after it connects to the irc network dal.net

Host **63.193.210.208**: Official name: **adsl-63-193-210-208.dsl.snfc21.pacbell.net**
Pacific Bell Internet NetCenter (PB401-ORG) trouble@PBI.NET
303 Second Street Suite 830
San Francisco, CA 94107
1-800-4NETPBI (463-8724) Fax- - (415) 442-4999
ADSL BASIC-rback7-snfc21 (NETBLK-SBCIS990913-39) SBCIS990913-39
63.193.210.0 - 63.193.211.255
With www.samspade.org I was also able to use their safe browser to take a look at this machine and I found a Linux web server that still has the manuals and default information. It also has an old version of php installed, which is probably vulnerable to attacks. This is probably a computer of a not-so bright attacker who was looking for a Wingate to browse the Internet anonymously.

Host **208.194.161.155**: Official name: **proxy.monitor.twisted.ma.us.dal.net**
Registrant:
DALnet (DAL2-DOM)
6755 Mira Mesa Blvd. Ste. 123, #130
San Diego, CA 92121 US
Domain Name: DAL.NET
By the name and the registrant, I would assume that this computer is checking to see if the host has wingate installed. Wingate is a popular way to connect to the irc anonymously.

Host **198.63.2.192** :
Verio, Inc. (NET-VRIO-198-063)
8005 South Chester Street
Englewood,, CO 80112 US
Netname: VRIO-198-063
Netblock: 198.63.0.0 - 198.66.my.net
Miscellaneous unknown host.

Host **204.117.70.5** : Official name: **security.enterthegame.com**
Registrant:
Mystical Creations (ENTERTHEGAME-DOM)
P.O. Box 11991
Lexington, KY 40579-1991 US
Domain Name: ENTERTHEGAME.COM
Enterthegame.com is a gaming irc server. Therefore this is probably also a irc server checking to see if the host has wingate installed.

Host **64.86.5.250** : Official name: **proxy3.monitor.dal.net**
Registrant:
DALnet (DAL2-DOM)
6755 Mira Mesa Blvd. Ste. 123, #130
San Diego, CA 92121 US
Domain Name: DAL.NET
Another irc server checking for a wingate.

Recommendation:
Make sure Wingate is not installed on any of these hosts. If it is, make sure it is properly configured.

2.3.4.2.18 Watchlist 000222 NET - NCFC

8093 alerts with this signature among the files:
Earliest such alert at **01:43:43**.866602 *on 09/26*
Latest such alert at **21:27:46**.757337 *on 11/22*

Watchlist 000222 NET-NCFC	45 sources	26 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
159.226.45.3	6296	6296	8	8
159.226.91.20	1147	1147	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

Top 5 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	1293	1296	7	9
my.net.253.43	460	588	17	21
my.net.253.42	155	171	12	20
my.net.253.41	120	214	16	21

Information about attack:
These are addresses that we are watching for suspicious activity and they need to be watched closer. There is some serious suspicious activity coming from these hosts.

Correlation:
On our previous report we found 19478 alerts making this alert decreased by 60%.

Host **159.226.45.3**: Official name: **aphy.iphy.ac.cn**
The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
Netname: NCFC
Netblock: 159.226.0.0 - 159.226.my.net
This host has increased traffic significantly, but it still has suspicious activity. Take a look at the following trace. These packets are definitely crafted. They all have the same source and destination port.

```
09/28-23:02:23.208956 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3599-> 255.255.253.42:25
09/28-23:02:33.725458 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3599-> 255.255.253.42:25
09/28-23:02:33.864378 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3599-> 255.255.253.42:25
09/28-23:03:03.751847 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3599-> 255.255.253.42:25
09/28-23:03:03.763811 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:3599-> 255.255.253.42:25
```

Host: **159.226.91.20**:

The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
Netname: NCFC
Netblock: 159.226.0.0 - 159.226.my.net

This host has some serious suspicious activity. Take a look at the following trace. These packets are definitely crafted. They are all from the same source port with the same destination port for a few packets, and then they stop. Then start again 2 weeks later with the same source and destination port.

09/27-08:20:08.411335 [**] Watchlist 000222 NET-NCFC [**] 159.226.91.20:4740-> 255.255.253.43:25
09/27-08:20:34.497214 [**] Watchlist 000222 NET-NCFC [**] 159.226.91.20:4740-> 255.255.253.43:25
10/09-20:54:44.259470 [**] Watchlist 000222 NET-NCFC [**] 159.226.91.20:3205-> 255.255.253.42:25
10/09-20:54:44.259470 [**] Watchlist 000222 NET-NCFC [**] 159.226.91.20:3205-> 255.255.253.42:25
10/09-20:55:05.182490 [**] Watchlist 000222 NET-NCFC [**] 159.226.91.20:3205-> 255.255.253.42:25

Hosts **my.net.253.41-43**: These hosts have decreased traffic significantly since last month.

Recommendation:
Continue to watch for suspicious activity that is on this watch list. If it continues to show no interesting activity, you might want to consider turning off this watch list.

2.3.4.2.19 Watchlist 000220 IL-ISDNNET - 990517

29757 alerts with this signature among the files:
Earliest such alert at **01:14:52**.325234 *on 09/26*
Latest such alert at **14:58:55**.189582 *on 11/22*

Watchlist 000220 IL-ISDNNET-990517	58 sources	104 destinations

Top 5 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

Top 5 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	1462	1	4

Information about attack:
These are addresses that we are watching for suspicious activity.

Correlation:
On our previous report we found 19478 alerts making this alert decreased by 60%.
Host **212.179.95.5** : Official name: **cable-95005.bezeqint.net**
Host **212.179.27.6** : Official name: **clnt-27006.bezeqint.net**
Host **212.179.79.2**
Host **212.179.44.115** : Official name: **bzq-44-115.bezeqint.net**
Host **212.179.72.226**

Registrant:
Bezeq International (BEZEQINT2-DOM)
40 Hashacham St.
Petach Tikva, Israel 49170
inetnum: 212.179.95.0 - 212.179.99.255
netname: CABLE-XPRMNT
descr: Cable-Modem-Experiment
country: IL

Cable modems from Israel.

The following are traces from the above hosts:

4 different signatures are present for *my.net.211.146* as a destination
1 instances of *SYN-FIN scan!*
1 instances of *Queso fingerprint*
2 instances of *Null scan!*
4810 instances of *Watchlist 000220 IL-ISDNNET-990517*

10/04-11:46:03.475588 [**] SYN-FIN scan! [**] 63.195.56.20:21-> my.net.211.146:21
11/04-01:59:00.495308 [**] Queso fingerprint [**] 133.46.212.81:28-> my.net.211.146:1738
11/04-06:53:58.388774 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.5:2012-> my.net.211.146:4922
11/04-15:19:39.764305 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.5:3288-> my.net.211.146:4922
11/05-04:47:27.303528 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.95.5:1263-> my.net.211.146:4922

This definitely looks like signs of a backdoor. It starts off with a syn-fin scan, then a Queso fingerprint and then continues on unknown port 4922 over 4800 packets.

2 different signatures are present for *my.net.223.98* as a destination
2 instances of *SYN-FIN scan!*
3938 instances of *Watchlist 000220 IL-ISDNNET-990517*

09/30-13:29:25.706832 [**] SYN-FIN scan! [**] 160.78.49.191:53-> my.net.223.98:53
10/07-11:19:57.852887 [**] SYN-FIN scan! [**] 163.10.19.34:21-> my.net.223.98:21
10/08-09:22:28.762440 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.44.115:1057-> my.net.223.98:6699
10/08-09:22:33.623535 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.44.115:1057-> my.net.223.98:6699

This definitely looks like signs of a backdoor. It starts off with a syn-fin scan and then continues on unknown port 6699 for over 3900 packets. These are also crafted packets because they have the same source and destination port.

3 different signatures are present for *my.net.206.90* as a destination
1 instances of *Null scan!*
3 instances of *SYN-FIN scan!*
3914 instances of *Watchlist 000220 IL-ISDNNET-990517*

10/02-06:45:44.160229 [**] SYN-FIN scan! [**] 208.61.4.207:9704-> my.net.206.90:9704
10/03-08:58:52.711013 [**] SYN-FIN scan! [**] 209.92.40.32:9704-> my.net.206.90:9704
10/04-11:45:36.849160 [**] SYN-FIN scan! [**] 63.195.56.20:21-> my.net.206.90:21
11/11-06:13:05.916864 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.27.6:1498-> my.net.206.90:4619
11/11-06:13:48.456742 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.27.6:1498-> my.net.206.90:4619
11/11-06:13:56.352386 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.27.6:1498-> my.net.206.90:4619

This definitely looks like signs of a backdoor. It starts off with a syn-fin scan and then continues on unknown port 4619 for over 3900 packets. These are also crafted packets because they have the same source and destination port.

1 instances of *SYN-FIN scan!*
1 instances of *WinGate 1080 Attempt*
1638 instances of *Watchlist 000220 IL-ISDNNET-990517*

10/04-11:45:22.586270 [**] SYN-FIN scan! [**] 63.195.56.20:21-> my.net.203.142:21
11/11-00:13:47.307406 [**] WinGate 1080 Attempt [**] 207.114.4.46:4602-> my.net.203.142:1080
11/13-08:32:51.335546 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:32685-> my.net.203.142:4619
11/13-08:33:25.968059 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:32685-> my.net.203.142:4619
11/13-08:33:27.053998 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:32685-> my.net.203.142:4619

This definitely looks like signs of a backdoor. It starts off with a syn-fin scan and then continues on unknown port 4619 for over 1600 packets. These are also crafted packets because they have the same source and destination port.

2 different signatures are present for *my.net.218.142* as a destination
3 instances of *SYN-FIN scan!*
1459 instances of *Watchlist 000220 IL-ISDNNET-990517*

10/02-06:47:31.162333 [**] SYN-FIN scan! [**] 208.61.4.207:9704-> my.net.218.142:9704
10/04-11:46:39.098227 [**] SYN-FIN scan! [**] 63.195.56.20:21-> my.net.218.142:21
10/14-21:13:03.728275 [**] SYN-FIN scan! [**] 130.89.229.48:53-> my.net.218.142:53
11/16-11:38:55.812945 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:13270-> my.net.218.142:4990
11/16-11:39:10.814986 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:13270-> my.net.218.142:4990
11/16-11:39:13.585859 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.79.2:13270-> my.net.218.142:4990

This definitely looks like signs of a backdoor. It starts off with a syn-fin scan and then continues on unknown port 4990 for over 1400 packets. These are also crafted packets because they have the same source and destination port.

Recommendation:
Check each of this machines for backdoors and watch this watch list closely. There looks like a lot of suspicious activity.

2.3.4.2.20 SYN-FIN scan!

53912 alerts with this signature among the files:
Earliest such alert at **13:10:30**.153412 *on 09/30*
Latest such alert at **09:33:33**.732424 *on 11/22*

SYN-FIN scan!	29 sources	25416 destinations

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
160.78.49.191	7199	7199	7199	7199
208.61.4.207	6635	6635	6635	6635
209.92.40.32	4967	4967	4967	4967
63.195.56.20	3897	3897	3897	3897
130.89.229.48	3860	3860	3860	3860

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
my.net.223.251	10	12	10	11
my.net.70.84	8	9	8	9
my.net.201.126	8	12	3	7
my.net.224.79	8	8	8	8
my.net.221.233	8	8	8	8

Snort Signature:
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "IDS198/SYN FIN Scan"; flags: SF;)

Information about attack:
A TCP probe was sent with the SYN+FIN flags set in the header. This traffic does not occur naturally and indicates an intentional probe, likely as a part of single-packet OS detection. This was once considered a stealth scan, but is now considered a VERY loud way of scanning. I guess no one has told these people yet. For more information about this Please see the following web sites :
http://www.whitehats.com/info/IDS198
http://www.insecure.org/nmap/

Correlation:
On our previous report we found 12 alerts making this alert decreased by 42%. The source and destination addresses have also changed. There are no reoccurring attacks.

Host **160.78.49.191** : Official name: **ema.chim.unipr.it**
Centro di Calcolo di Ateneo (NET-PARMANET1)
Centro di Calcolo di Ateneo
Universita` di Parma
Viale Delle Scienze
43100 PARMA - ITALIA
Netname: PARMANET
Netblock: 160.78.0.0 - 160.78.my.net

Host **208.61.4.207** : Official name: **adsl-61-4-207.mia.bellsouth.net**
Registrant:
BellSouth.net, Inc (BELLSOUTH-DOM)
1100 Ashwood Pkwy. Suite 200
Atlanta, GA 30338 US
Domain Name: BELLSOUTH.NET

Host **209.92.40.32** : Official name: **dslcv1-32.fast.net**
Registrant:
You Tools Corporation (FAST-DOM)
3864 Courtney Street ; Suite 130
Bethlehem, PA 18017-8987 US
Domain Name: FAST.NET
FASTNET-You Tools Corporation (NETBLK-NETBLK-FAST3) NETBLK-FAST3
209.92.0.0 - 209.92.my.net
FASTNET Corporation (NETBLK-DSL1-FASTNET) DSL1-FASTNET
209.92.40.0 - 209.92.47.255

Host **63.195.56.20** : Official name: **adsl-63-195-56-20.dsl.snfc21.pacbell.net**
Registrant:
Pacific Bell Internet Services (PACBELL2-DOM)
303 Second Street Suite 830
San Francisco, CA 94107
Domain Name: PACBELL.NET

Host **130.89.229.48** : Official name: cal032044.student.utwente.nl
University Twente (NET-UTNET)
Postbox 217
7500 AE Enschede
NETHERLANDS
Netname: UTNET
Netblock: 130.89.0.0 - 130.89.my.net

Recommendation:
Make sure that the scans don't lead into any other types of attacks.

Assignment 3 – Analysis Process

The first step I did was to organize all of the data into 3 different files. I did this by first unzipping the files into their own directory and then I put them into a single file with the following command on a Windows 2000 machine.

For /f "tokens=4 skip=7" %I in ('dir') do type %I>> SnortA.txt
For /f "tokens=4 skip=7" %I in ('dir') do type %I>> SnortS.txt
For /f "tokens=4 skip=7" %I in ('dir') do type %I>> OSS.txt

This gave me 3 files.

SnortA.txt	15meg	Snort Alerts
SnortS.txt	22meg	Snort Port Scans
OSS.txt	17meg	Snort

Next I ran into a problem because snortsnarf does not accept MY.NET. To go around this, I ran the files through a ported version of sed for win32 with the following commands:

Sed 's/MY.NET/my.net/g' snorta.txt >> alerts.txt
Sed 's/MY.NET/my.net/g' snorts.txt >> scans.txt

Since I now had two files that I could run though snortsnarf I installed perl for win32 and ran snortsnarf with the following command

Perl snortsnarf –dns alerts.txt
Perl snortsnarf –dns scans.txt

I then ran into a similar problem like everyone else that has tried this. I ran out of memory. I then went to a quad processor machine that had 4 gig of ram and tried it again. It was much faster and I no longer had a memory problem. I was able to get the results that were seen above.

I then used the following web sites to gather information and correlations for all the alerts:

www.snort.org	Snort application and documentations
www.sans.org	GIAC information was great for correlation
Packetstorm.securify.com	Many security applications and white papers
www.securityfocus.com	Many security applications, white papers, and most of all BugTraq
www.samspade.org	Great web site for doing whois, nslookups, and many other inet tools
www.insecure.org/nmap	Great scanning utility
http://www.isi.edu/in-notes/iana/assignments/port-numbers	This site has all of iana port numbers
www.simovits.com/nyheter9902.html	This site has a list of common trojan ports
www.google.com	Great search engine to find correlation information.
www.whitehats.com	Great site for referencing Snort alerts
http://www.silicondefense.com/snortsnarf/	Can't do this project with out this.