Global Information Assurance Certification Paper

GCIA Practical Assignment

David Anderson

SANS Level Two

Intrusion Detection In Depth

Version 2.8

Aloha II SANS Conference

February/March 2001

Table of Contents

Table of Authorities

Assignment 1- Network Detects

Network Detect 1 – Source Quench

```
[**] ICMP Echo Request [**]
03/17-17:59:50.455340 209.86.221.32 -> yy.yy.120.158
ICMP TTL:243 TOS:0x0 ID:23185 IpLen:20 DgmLen:1500 DF
Type:8  Code:0  ID:39612   Seq:57072  ECHO

[**] ICMP Echo Request [**]
03/17-17:59:50.455451 209.86.221.32 -> yy.yy.120.158
ICMP TTL:116 TOS:0x0 ID:23186 IpLen:20 DgmLen:28
Type:8  Code:0  ID:512   Seq:47880  ECHO

[**] ICMP Echo Reply [**]
03/17-17:59:50.495401 yy.yy.120.158 -> 209.86.221.32
ICMP TTL:243 TOS:0x0 ID:36121 IpLen:20 DgmLen:1500 DF
Type:0  Code:0  ID:39612  Seq:57072  ECHO REPLY

[**] ICMP Echo Reply [**]
03/17-17:59:50.495509 yy.yy.120.158 -> 209.86.221.32
ICMP TTL:116 TOS:0x0 ID:36122 IpLen:20 DgmLen:28
Type:0  Code:0  ID:512  Seq:47880  ECHO REPLY

[**] ICMP Source Quench [**]
03/17-17:59:52.097146 209.86.221.32 -> yy.yy.120.158
ICMP TTL:243 TOS:0x0 ID:23187 IpLen:20 DgmLen:112 DF
Type:4  Code:0  SOURCE QUENCH

[**] ICMP Source Quench [**]
03/17-17:59:52.097263 209.86.221.32 -> yy.yy.120.158
ICMP TTL:243 TOS:0x0 ID:23188 IpLen:20 DgmLen:56 DF
Type:4  Code:0  SOURCE QUENCH
```

```
17:59:50.455340 user-38ldn90.dialup.mindspring.com > yy.yy.120.158:
icmp: echo request (DF) (ttl 243, id 23185)
                  4500 05dc 5a91 4000 f301 c0b4 d156 dd20
                  3fc5 789e 0800 7e52 9abc def0 0000 0000
                  0000 0000 0000 0000 0000 0000 0000 0000
                  0000 0000 0000
17:59:50.455451 user-38ldn90.dialup.mindspring.com > yy.yy.120.158:
icmp: echo request (ttl 116, id 23186)
                  4500 001c 5a92 0000 7401 8574 d156 dd20
                  3fc5 789e 0800 3af7 0200 bb08 0000 0000
                  0000 0000 0000 0000 0000 0000 0000
17:59:50.495401 yy.yy.120.158 > user-38ldn90.dialup.mindspring.com:
icmp: echo reply (DF) (ttl 243, id 36121)
                  4500 05dc 8d19 4000 f301 8e2c 3fc5 789e
                  d156 dd20 0000 8652 9abc def0 0000 0000
                  0000 0000 0000 0000 0000 0000 0000 0000
                  0000 0000 0000
17:59:50.495509 yy.yy.120.158 > user-38ldn90.dialup.mindspring.com:
icmp: echo reply (ttl 116, id 36122)
                  4500 001c 8d1a 0000 7401 52ec 3fc5 789e
                  d156 dd20 0000 42f7 0200 bb08 044e a92b
```

```
                    5010 ff00 db13 0000 0000 0000 0000
17:59:52.097146 user-38ldn90.dialup.mindspring.com > yy.yy.120.158:
icmp: source quench (DF) (ttl 243, id 23187)
                    4500 0070 5a93 4000 f301 c61e d156 dd20
                    3fc5 789e 0400 fbff 0000 0000 4500 05dc
                    8d19 4000 e701 9a2c 3fc5 789e d156 dd20
                    0000 8652 9abc
17:59:52.097263 user-38ldn90.dialup.mindspring.com > yy.yy.120.158:
icmp: source quench (DF) (ttl 243, id 23188)
                    4500 0038 5a94 4000 f301 c655 d156 dd20
                    3fc5 789e 0400 fbff 0000 0000 4500 001c
                    8d1a 0000 6801 5eec 3fc5 789e d156 dd20
                    0000 42f7 0200
```

1. Source of Trace

This trace was generated from my home network.

2. Detect was generated by:

This Alert detect was generated with the Snort intrusion detection system. A standard rule set was used. Ruleset date 3/4/2001. Additional information was collected with WinDump 3.4a6.

3. Probability the source address was spoofed:

While the detected host address is valid, the address could also be spoofed. However, if the address were spoofed, there would be little reason to precede the ICMP Source Quench with the echo request.

4. Description of attack:

First considered a Denial of Service (DoS) Attack against ICMP, this may only be reconnaissance for information. The host address 209.86.221.32 resolves to user-38ldn90.dialup.mindspring.com.

5. Attack mechanism:

Source quench has the ability to slow communications from the target host there by creating a DoS. There were not enough packets delivered to accomplish a DoS in this case. This more likely is an attempt at system or network fingerprinting.

6. Correlations:

There has still been no explanation as to the purpose of the echo followed by the source quench. Correlations related to this attack are listed below. The consensus from reviewing the information below indicates recon.

Guy Bruneau from Canada http://www.sans.org/y2k/031500-2300.htm
Ken Williams http://www.sans.org/y2k/122799-17.htm
Arrigo from London http://www.sans.org/y2k/030200.htm
Arrigo from London http://www.sans.org/y2k/021000-2300.htm
Arrigo from London http://www.sans.org/y2k/020500.htm
Denmark, University of Copenhagen http://www.sans.org/y2k/022100-1130.htm
Denmark, University of Copenhagen http://www.sans.org/y2k/022800.htm

7. Evidence of active targeting:

This attack was targeted at a specific address.

8. Severity:

```
(Critical + Lethal) – (System + Network Countermeasures) = Severity
```

Criticality = **3** - Half of the systems on the network are critical. If the exploit was successful, systems could be compromised. Some trust relationships exist between the systems.

Lethality = **1** - There is an internal application generating malicious traffic. There is a successful compromise of a system. There is the potential for the compromise of other systems.

System countermeasures = **5** – Critical systems are secure and full patches with host firewall. Other systems are less secure and not protected with a host firewall. Because there is some trust relationships between the systems, this vulnerability could be spread to critical systems. However, the host based tools we're not configured to protect against this specific Trojan.

Network countermeasures = **3** – This traffic was received at the network border router. Limited protection is available for this router without disabling ICMP completely. However, the router does filtering of such traffic for the internal network.

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

9. Defensive recommendation:

The router has been upgraded to a stateful inspection firewall that does reject most incoming ICMP while allowing outgoing ICMP to function.

10. Multiple choice test question:

This detect shows

a) reconnaissance for information.
b) a failed echo request.
c) a Denial of Service (DoS) Attack against ICMP.
d) an ICMP buffer overflow attempt.

a

Network Detect 2 – SMB Wildcard Name

```
The firewall has blocked Internet access to your computer (NetBIOS
Name) from xx.xx.103.73 (NetBIOS Name).
```

```
Time: 3/29/2001 22:43:18
```

A snort analysis of the WinDump file follows:

```
03/29-23:27:24.214321 xx.xx.103.73:137 -> 192.168.1.25:137 UDP TTL:118
TOS:0x0 ID:6973 IpLen:20 DgmLen:78
Len: 58
E6 94 00 10 00 01 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41                 AAAAAAAAAA
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/29-23:27:25.713124 xx.xx.103.73:137 -> 192.168.1.25:137 UDP TTL:118
TOS:0x0 ID:6975 IpLen:20 DgmLen:78
Len: 58
E6 98 00 10 00 01 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41                 AAAAAAAAAA
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/29-23:27:27.215023 xx.xx.103.73:137 -> 192.168.1.25:137 UDP TTL:118
TOS:0x0 ID:6976 IpLen:20 DgmLen:78
Len: 58
E6 9A 00 10 00 01 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41                 AAAAAAAAAA
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1.Source of Trace.

This trace was generated from my home network.

2. Detect was generated by:

This detect was generated by Zone Alarm running on one of the computer on my network. WinDump 3.4a6 log files provided follow up data.

3. Probability the source address was spoofed:

The host address is probably valid. The NetBIOS handshake requires valid addresses to complete. If the connection were for recon, a valid address would be necessary to recover the information.

4. Description of attack:

SMB services allow for file sharing over the network, including the Internet. This is the normal method for Windows systems to share objects. This is an attempted SMB Wildcard Name connection. This exploit has the ability to enumerate system and network information. The registered owner of the address block of which this address belongs is Telefonica Data Espana - IPNET MANAGEMENT - Madrid, Spain.

5. Attack mechanism:

An excellent decoding of the SMB wildcard name packet was described in the SANS *Intrusion Detection FAQ Port 137 Scan* by Bryce Alexander[1].

> A decode of the Netbios data in the first packet reveals the following:
>
> Bytes 0 & 1: Xid
> Value: 00 D4 (this value increments with each new query)

[1] http://www.sans.org/newlook/resources/IDFAQ/port_137.htm

Bytes 2 & 3: Opcode NMflags & Rcode
Value: 00 10 = request, query, broadcast/multicast

Bytes 4 & 5: QDcount (number of name queries in packet)
Value: 00 01 = 1 name query

Bytes 6 to 11: ANcount, NScount, ARcount
Value: 00 00 00 00 00 00 = Not used in this frame.

Byte 12: Size of name field
Value: 0x20 = decimal value 32 (next 32 bytes used for name)

Bytes 13 to 45: Name field
Value 43 4b 41 41 41...(ETC.) This is the ascii string CKAAAAA... in the packet. It is a mangled name done by splitting the hex value of each character into two parts(nibbles) and then adding 0x41 to each nibble. In this packet the name is an asterisk "*" followed by nulls. The hex value of * is 2A, splitting and adding it would become: (2+41=43) and (A+41=4B) The Ascii Value of these two results is "CK". The remaining nulls added to 41 remain 41 or "A"

Byte 46 Null field delimeter

Bytes 47 & 48 Question_type
Value: 00 21 = Node Status request (nbstat).

Bytes 49 & 50 Question Class
Value: 00 01 = Internet Class.

This particular trace was crafted by using the windows command: NBTSTAT -A (Target IP Address)

An anonymous, if permitted, connection can be created as follows:

```
net use \\sysname\IPC$ "" \user:""
```

The NBTSTAT command can be used to extract SMB associated information from the target once a connection has been established. Scripts can be used to enumerate SMB information, even when restrict anonymous is set to 1. The new network.vbs (and it's derivatives) Internet worm may exploit SMB information (see: http://www.cert.org/incident_notes/IN-2000-02.html)[2].

6. Correlations:

No correlations for the host 213.97.103.73 were discovered on the SANS website. The host was also not identified on jttp://www.incidents.org Consensus Intrusion Database for the last 30 days.

A detailed description of issues related to SMB are described at http://www.sans.org/newlook/resources/IDFAQ/port_137.htm

CAN-1999-0519 - Description A NETBIOS/SMB share password is the default, null, or missing. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0519

[2] http://www.sans.org/newlook/resources/IDFAQ/port_137.htm Port 137 Scan; Bryce Alexander

TCP/IP for Intrusion Detection and Firewalls, The SANS Institute, page 7-22.

SMB wildcard name related correlations are available at the following:
http://www.sans.org/y2k/practical/Eric_Hacker.html#anchor9566546
http://www.sans.org/y2k/111000.htm
http://www.sans.org/y2k/111700.htm
http://www.sans.org/y2k/082800.htm
http://www.sans.org/y2k/090800.htm
http://www.sans.org/y2k/081200-1300.htm

7. Evidence of active targeting:

This exploit/reconnaissance works against a specific host or network group.

8. Severity:

```
(Critical + Lethal) – (System + Network Countermeasures) = Severity
```

Criticality = **4** - Half of the systems on the network are critical. If the exploit was successful, systems could be compromised. Some trust relationships exist between the systems.

Lethality = **3** – Password, system and, account could be made available that has potential to aid in the compromise of network systems.

System countermeasures = **5** – Critical systems are secure and full patched with host firewall. Other systems are less secure but protected with a host firewall that blocks un-trusted traffic.

Network countermeasures = **5** – The network is protected from un-trusted SMB access at both the network border and at the host.

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

9. Defensive recommendation:

No modifications are necessary. SMB traffic is blocked at the border router. Traffic that slips through is blocked at the host by the host firewall.

10. Multiple choice test question:

In this detect the string CKAAAAAAAAAAA

a) identifies the destination system
b) is a search for windows names
c) is a search for the crow Trojan
d) exploits a windows file access vulnerability

b

Network Detect 3 – ICMP Nmap2.36BETA or HPING2 Echo or ?

```
[**] ICMP Nmap2.36BETA or HPING2 Echo  [**]
03/19-15:26:51.956799 192.168.1.25 -> 192.168.1.1
ICMP TTL:255 TOS:0x0 ID:7424 IpLen:20 DgmLen:28
Type:8  Code:0  ID:256   Seq:256  ECHO
. . .
[**] ICMP Nmap2.36BETA or HPING2 Echo  [**]
03/20-19:50:06.626195 192.168.1.25 -> 192.168.1.1
ICMP TTL:255 TOS:0x0 ID:7424 IpLen:20 DgmLen:28

Type:8  Code:0  ID:256   Seq:256  ECHO
```

1.Source of Trace.

This trace was generated from my home network.

2. Detect was generated by:

This Alert detect was generated with the Snort intrusion detection system. A standard rule set was used. Ruleset date 3/4/2001. Additional information was collected with windump 3.4a6.

3. Probability the source address was spoofed:

The source address was a valid address for the systems on the network.

4. Description of attack:

Snort detected an ICMP Nmap2.36BETA or HPING2 Echo. HPING is available only for UNIX type systems not Windows[3]. NMAP is also available for these platforms and for available for Windows[4]. The captured alerts definitely contained crafted packets as the IP ID, **`ID:7424,`** was identical even though the packets were detected 28 hours apart.

5. Attack mechanism:

An investigation was conducted to identify the source of the suspect traffic. As a Trojan was suspected, Trojan Defence Suite v3.0.0 Beta 4b[5] was run on the suspect system.

The results are displayed in Figure 1. RAT Remote Administrator 2.0a was discovered on the suspect system[6]. Remote Administration Tool - RAT can be active on ports 1095-1099 & 2989 (UDP).

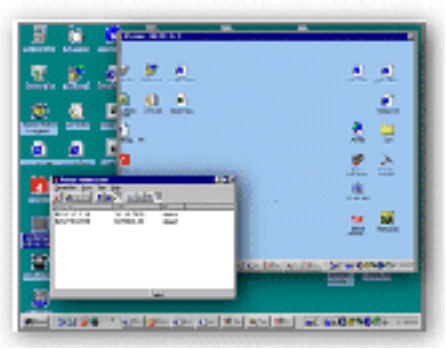


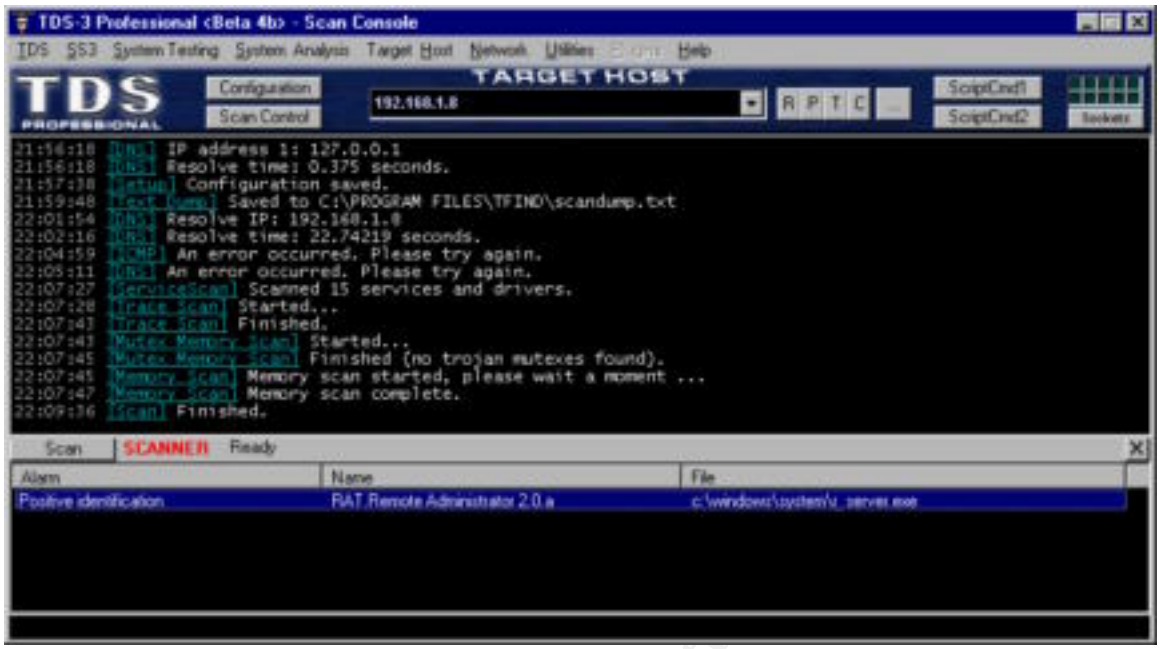
Figure 1 - TDS Trojan Detect

[3] http://www.kyuzz.org/antirez/oldhping.html

[4] http://www.insecure.org/nmap/index.html#intro

[5] http://tds.diamondcs.com.au/

[6] http://www.famatech.com/



6. Correlations:

http://www.insecure.org/nmap/
http://www.kyuzz.org/antirez/oldhping.html
http://www.eaglenet.org/antirez/hping2.html
http://www.famatech.com/

No other instances were found on the net regarding this tool.

7. Evidence of active targeting:

Specific systems were targeted.

8. Severity:

```
(Critical + Lethal) – (System + Network Countermeasures) = Severity
```

Criticality = **4** - Half of the systems on the network are critical. If the exploit was successful, systems could be compromised. Some trust relationships exist between the systems.

Lethality = **5** - There is an internal application generating malicious traffic. There is a successful compromise of a system. There is the potential for the compromise of other systems.

System countermeasures = **2** – Critical systems are secure and full patches with host firewall. Other systems are less secure and not protected with a host firewall. Because there is some trust relationships between the systems, this vulnerability could be spread to critical systems. However, the host based tools we're not configured to protect against this specific Trojan.

Network countermeasures = **1** – This traffic is generated inside the network router. Limited protection is provided. The router was not filtering for the specific Trojan discovered.

Severity = **6** = (4 + 5) - (2 + 1)

9. Defensive recommendation:

Hosts were scanned for resident Trojans Detected Trojans were removed. Host based firewalls were installed on all systems on the network. Network users, and their "friends", were instructed in the dangers of installing remote access software because it is thought to be "really" cool.

NOTE: Network countermeasures are not effective against foot-net traffic.

10. Multiple choice test question:

In this alert . . .

a) the TCP ID is normal
b) the TCP ID is crafted
c) the Seq is crafted
d) b & c

d

Network Detect 4 – NetBus Attack

```
*** Alert from NETGEAR *** [0030AB04B2CE]

05/05/2001 18:55:43.320 -     NetBus Attack Dropped -
      Source:24.240.33.66, 1688, WAN -    Destination: yy.yy.120.158,
12345, LAN -       -
```

Corresponding Firewall log entries associated with the attack.

```
05/05/2001 18:55:43.320 NetBus Attack Dropped 24.240.33.66, 1688, WAN
yy.yy.120.158, 12345, LAN

05/05/2001 18:55:43.480 TCP connection dropped 24.240.33.66, 1689, WAN
yy.yy.120.158, 1080, LAN 'Socks' 0
```

1.Source of Trace.

This trace was generated from my home network.

2. Detect was generated by:

Netgear FR314 Firewall Router Alert.

3. Probability the source address was spoofed:

The attack was an attempt to connect to a NetBus server. This requires a valid IP address.

4. Description of attack:

NetBus is a Trojan horse attack for Windows systems. This is an attempt to connect to a NetBus server. Host address 24.240.33.66 resolves to 24-240-33-66.hsacorp.net. The host was active at the time of the attack.

```
Pinging 24.240.33.66 with 32 bytes of data:
Reply from 24.240.33.66: bytes=32 time=125ms TTL=114
```

5. Attack mechanism:

NetBus utilizes a client-server architecture where the server program is installed on the target system. A client is used to connect to these NetBus servers[7]. Once the NetBus Trojan code is executed on a victim computer, the attacker can perform illicit activities including the execution of applications (possibly with local system access). NetBus server is started when the system is booted. Additional information is available at:

http://advice.networkice.com/advice/phauna/rats/netbus/default.htm
http://www.sans.org/infosecFAQ/malicious/netbus.htm

6. Correlations:

No supporting WinDump data was available as WinDump was only logging on the inside of the firewall at the time of this attack. The firewall blocked all packets on the outside of the network. The following, in addition to many other search results, have identified similar NetBus connection attempts.

http://www.sans.org/y2k/012001.htm
http://www.sans.org/y2k/101100.htm
http://www.sans.org/y2k/100300.htm
http://www.sans.org/y2k/101000.htm

A search for host 24.240.33.66 returned no results.

7. Evidence of active targeting:

This attack was directed at my network IP address. This is only effective when specifically targeted.

8. Severity:

```
(Critical + Lethal) – (System + Network Countermeasures) = Severity
```

Criticality = 4 - Half of the systems on the network are critical. If the exploit was successful, systems could be compromised. Some trust relationships exist between the systems.

Lethality = 5 - The successful connection to a NetBus server constitutes compromise of the system. Additional systems may be compromised from inside the firewall.

[7] http://www.sans.org/infosecFAQ/malicious/netbus.htm; Chris A. Hayden

System countermeasures = 3 – Critical systems are secure and full patches with host IDS and firewall. Other systems are less secure but not critical. Because there is some trust relationships between the systems, this vulnerability could be spread to critical systems.

Network countermeasures = 5 - The firewall blocked the connection for this scan before any targets could be reached.

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

9. Defensive recommendation:

This attack is detected and rejected at the border firewall. However, critical systems should be configured to detect and circumvent this attack because of its criticality.

10. Multiple choice test question:

This NetBus attack

a) was part of a multi-tiered attack.
b) was dropped because the socks port didn't match.
c) was dropped because of destination port 12345
d) a & c

d

Network Detect 5 – TCP FIN scan

```
*** Alert from NETGEAR *** [0030AB04B2CE]

5/06/2001 13:45:02.576 -      Probable TCP FIN scan -
      Source:209.247.133.21, 80, WAN -    Destination: yy.yy.120.158,
5062, LAN -        -
```

The firewall log for this alert was also available.

```
Time   Message   Source   Destination   Notes

 05/06/2001 13:45:02.576 Probable TCP FIN scan 209.247.133.21, 80, WAN
yy.yy.120.158, 5062, LAN
```

1.Source of Trace.

This trace was generated from my home network.

2. Detect was generated by:

Netgear FR314 Firewall Router Alert.

3. Probability the source address was spoofed:

The attack attempts to conduct a TCP FIN scan. This requires a valid IP address for recon information to be returned to the attacker.

4. Description of attack:

A TCP FIN scan is a stealth scanning method used by attackers to find listening ports on the target system without being detected.

5. Attack mechanism:

A TCP FIN, or Stealth FIN, scan will send a FIN packet to each port on the target system. These packets have the ability to circumvent some firewalls and IDS protections. They may also not be logged in some cases as they purpose is to terminate connections[8].

The host 209.247.133.21 resolves to gslb-pa.bmarts.com. The host was active and responding at the time of the attack.

```
Pinging 209.247.133.21 with 32 bytes of data:
Reply from 209.247.133.21: bytes=32 time=15ms TTL=243
```

6. Correlations:

Several Correlations for FIN scans were located on the SANS web site. However, this specific host was not located.

http://www.sans.org/y2k/020101.htm
http://www.sans.org/y2k/022101-1300.htm
http://www.sans.org/y2k/012900.htm
http://www.sans.org/y2k/050200.htm
http://www.sans.org/y2k/050200.htm
http://www.sans.org/y2k/110200.htm

7. Evidence of active targeting:

This scan was detected on my network IP address. This address could have been specifically targeted, or the scan could have also been part of a sweep of the network segment.

8. Severity:

```
(Critical + Lethal) – (System + Network Countermeasures) = Severity
```

Criticality = **2** - Half of the systems on the network are critical. If the scan was successful are accessing the internal network, system vulnerabilities could be uncovered.

Lethality = **1** - The scan in and of itself is not detrimental.

System countermeasures = **4** – Critical systems are secure and full patched. Other systems are less secure but not critical.

Network countermeasures = **5** - The firewall blocked the connection for this scan before any targets could be reached.

[8] Intrusion Signatures and Analysis; Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick – pg. 345

Severity = -6 = (2 + 1) - (4 + 5)

9. Defensive recommendation:

No modifications are necessary because these types of scans are detected and rejected at the border firewall. Critical systems have host based IDS operating.

10. Multiple choice test question:

This detect is . . .

a) a scan looking for services listening on port 80.
b) a scan looking for the listening FIN service.
c) a scan looking for services listening on 5062.
d) closing the scan connection.

c)

Assignment 2 - Describe the State of Intrusion Detection

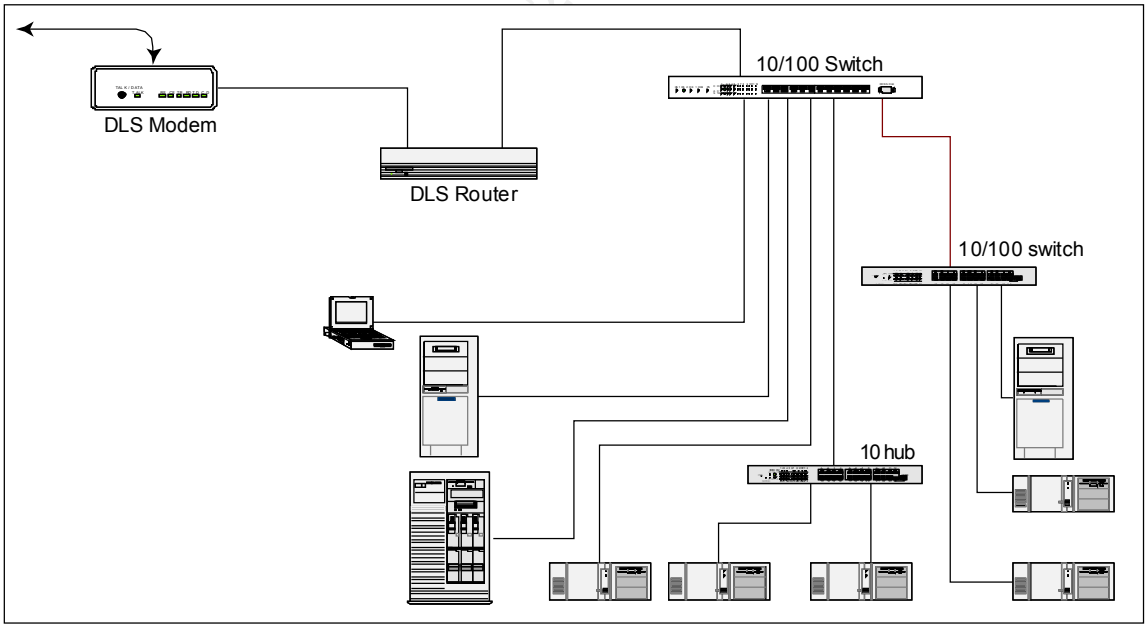
Securing the Home Front – Keeping unsolicited traffic out…

Introduction

Several papers have appeared on the SANS web site[9] over the last couple weeks describing methods to protect a home network from attack when connected with an always-on connection to the internet. While they contain much useful and accurate information, none individually contain a solution to a secure & monitored network. Securing a home computer or home network requires two important steps. First, the proper equipment is required with secure installation. Secondly, monitoring must take place to validate the operation of the equipment. Like a large cooperate network, a layered security model[10] is required to secure the home or small office (SOHO) network.

Always on DLS and cable started replacing the dial-up connections that were lucky to remain connected for periods of an hour. As soon as DSL was stable and available we signed up. The virus protection on the system was kept up to date. In the new world of always on, current virus protection is not enough to keep the systems secure. Keeping unsolicited network traffic on the outside of our home network evolved into a significant project.

Figure 2 - Initial DSL Network Configuration



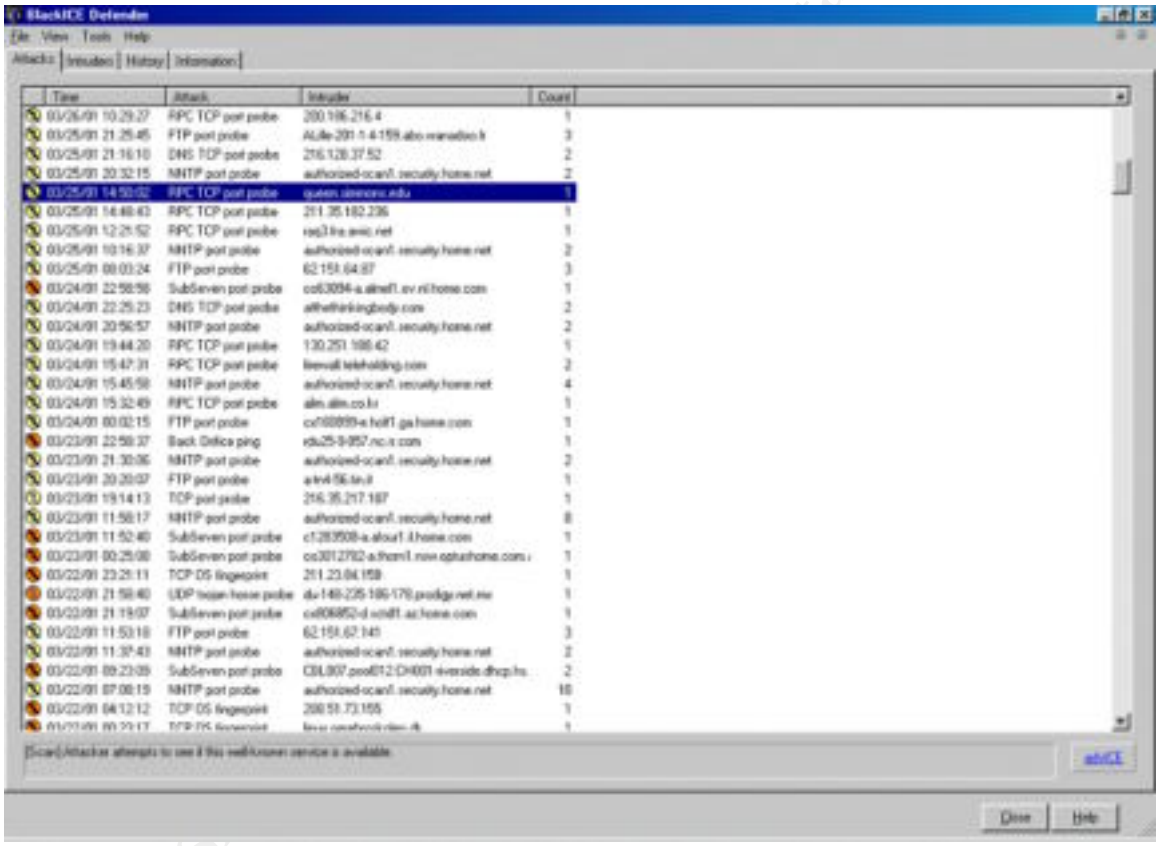
[9] http://www.sans.org/infosecFAQ/homeoffice/homeoffice_list.htm

[10] http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm

The First Attempt at Home Network Connectivity

Life was good in the beginning… I installed the fast, always on, DSL with an Arescom EasyRider Pro[11] ADSL router connecting the home network to the outside world via dslams and ATM and other good stuff. All seemed well. There was Network Address Translation (NAT) to protect the systems inside the router, which some call a firewall. The NAT was considered to allow outgoing traffic and block incoming traffic that was not mapped through to an internal host. The network configuration looked like Figure 2. Sites such as http://www.grc.com verified that the network was secure from outside traffic. Or so one might believe. This is still the most common network configuration for a home network. An always on, connection wired directly to the Internet is likely to be as exciting as that shown in Figure 3.

Figure 3 - Attack Detects With Direct Connection to the Modem



While the attacks directed at our systems behind the NAT router didn't resemble those shown in Figure 3, I was surprised to find a significant number of connection attempts being blocked at the host when Zone Alarm was installed on the desktop systems. Especially alarming were the large number of SMB connection attempts that Zone Alarm was blocking that originated outside of the router. The router was configured to block this traffic. Traffic on the windows ports (135, 137-139, and 445) were configured, in the router, to go to the bit bucket. The installation of BlackICE Defender lead to the

[11] http://www.arescom.com

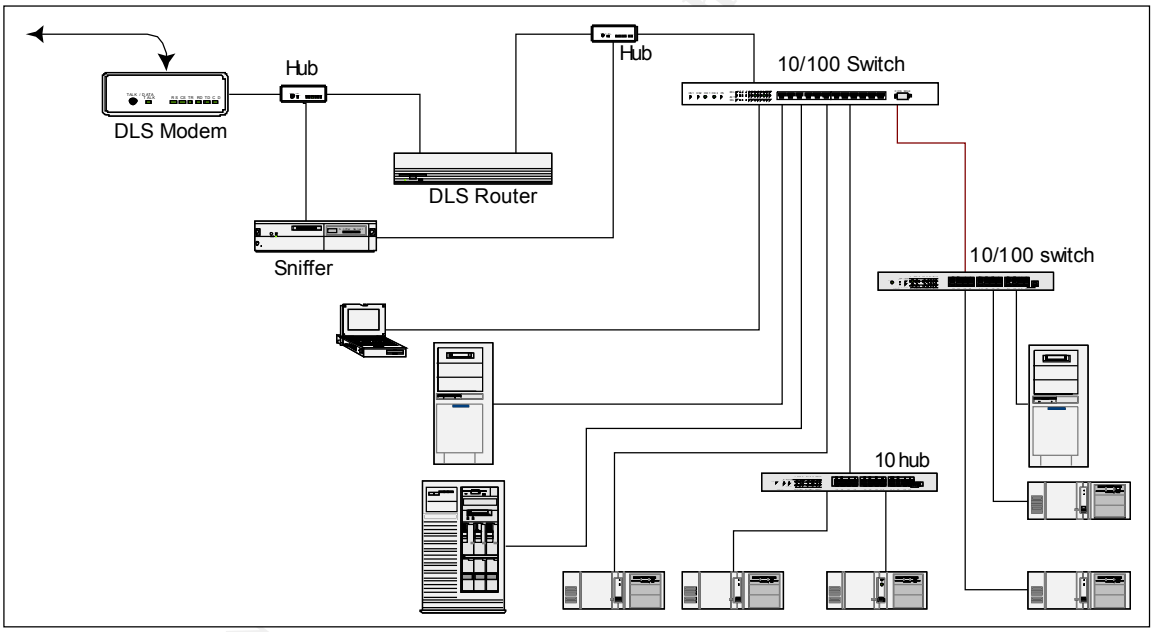
discovery of more interesting traffic. For some reason traffic was still finding its way through the NAT router. But what was the traffic that was slipping though the cracks?

Adding the $200 IDS

The IDS Hardware

To understand the flow of traffic on the network, it was reconfigured to include Intrusion Detection System (IDS) tools. The $200 IDS was assembled and installed on the network. The updated network configuration is displayed in Figure 4. An aging Pentium 200 system was configured with a couple of network cards and a couple of hubs. This will add one of the parts that are missing in most of the published solutions described earlier. The IDS to monitor the operation of and traffic carried on the network. While this falls outside the capability of the average home user, and probably beyond the interest of most capable computer users, the IDS plays a key role in operating a secure SOHO network.

Figure 4 - Router Driven Network with IDS



Adding the IDS Software

With the hardware in place, it was time to round up the software. Two components were required. The Intrusion Detection Software, and a network flight recorder and traffic monitoring tool.

Not having the significant funds to field Real Secure on a home network, I installed SNORT (http://www.snort.org). SNORT is a packet sniffer/logger that can be used as a lightweight network intrusion detection system. Snort uses rules based logging and can perform protocol analysis, content searching/matching and can be used to detect attacks

and probes[12]. Snort requires the installation libpcap drivers to operate. For a detailed analysis of snort, see: *An Analysis of the Snort Network Intrusion Detection System* by Mark D. Tollison http://www.sans.org/infosecFAQ/intrusion/snort2.htm

For monitoring network traffic, not having an up to date Linux box, I installed WinDump. WinDump is the Windows port of the UNIX network sniffer/analyzer. The current port for windows is based on tcpdump version 3.5.2[13]. Like SNORT, WinDump requires the installation of libpcap drivers.

Operating the IDS

Even the rather slow, by today's standard anyway, 200mhz does a good job of sniffing packets off of the two network cards an writing them to disk. There is very little packet loss with one interface monitoring the 10MB input from the DSL modem and the 100MB feeding the network out of the router. Three options are available on the location to monitor with SNORT; inside the firewall, outside the firewall, or both. With NAT enabled, most of the SNORT rules are unable to provide much useful detection. The only traffic that is able to do much with it the traffic directed to the public address. Viable options are then inside the firewall or both. Even the limited system that I installed is able to handle running two instances of both SNORT and WinDump, listening on both interfaces. The tools were now available to monitor and analyze the traffic slipping into the local network.

```
The firewall has blocked Internet access to your computer (NetBIOS
Name) from xx.xx.103.73 (NetBIOS Name).

Time: 3/29/2001 22:43:18
```

A snort analysis of the WinDump file follows:

```
03/29-23:27:24.214321 xx.xx.103.73:137 -> 192.168.1.25:137 UDP TTL:128
TOS:0x0 ID:6973 IpLen:20 DgmLen:78
Len: 58
E6 94 00 10 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41                     AAAAAAAAAA
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+==+=+=+=+=+=+=+=+=+=+=+=+
```

Additionally, a large number of port scans slipped through the NAT. Was there a reasonable priced way to reduce this traffic?

KEEP OUT! – Adding a Stateful Inspection Firewall

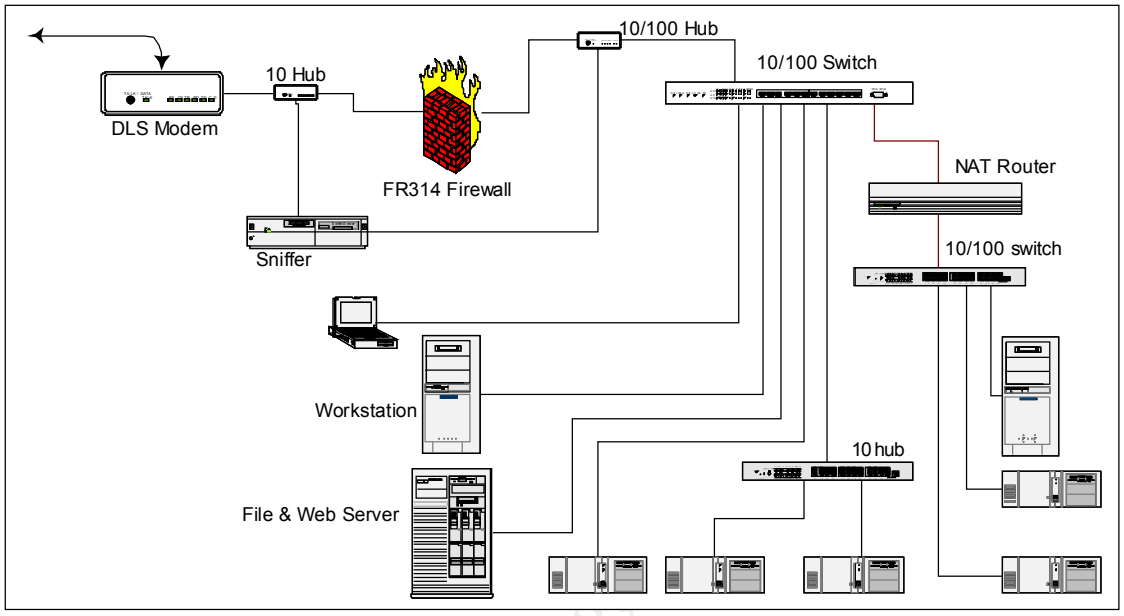
The Arescom EasyRider Pro had been on the front door for over a year and a half. It has served well. However, new products were coming available. Real firewalls are now available with stateful packet inspection for under $500. Two caught my eye; the SonicWALL SOHO2 (~$400) and the Netgear FR314 (~$300 – for a limited time ~$200 with CompUSA and Netgear rebates).

[12] http://www.snort.org/what_is_snort.htm; Martin Roesch,

[13] http://netgroup-serv.polito.it/windump/

The additional features of the SOHO2 couldn't justify the additional cost for the planned use I had. The FR314 was installed at the front door of the network as shown in Figure 5.

Figure 5 - Firewall Driven Network with IDS



The FR314 significantly reduced the amount of unwanted traffic slipping into the local network. Some examples are as follows:

- Malicious packets are dropped.
- Spoofed packets are dropped.
- UDP port scans are dropped.
- Several other scans are dropped.
- Several Trojan attacks are dropped.
- Several DoS attacks are dropped.
- SMB traffic is dropped.
- For those that want it, parental controls with content filtering capability

There would have to be a down side. While the firewall is easy to configure, there is very limited ability to configure custom rules for traffic through the firewall. For $300, you don't get to have the "rules" tab. Much of this limitation can be overcome by placing a router behind the firewall. The logging provided by a firewall may be sufficient in some cases to eliminate the need for additional monitoring outside the firewall. That need would be determined by ones paranoia level.

Summary

Now the SOHO is a well-protected and monitored fortress with many layers to protect it. A summary of the configuration of the secured network follows:

- A stateful packet inspection firewall at the front door.
- A network intrusion detection system.
- A network flight recorder (monitoring traffic inside and outside the firewall).
- A host based IDS on critical systems (the exposed server for instance).

- Current virus protection.
- Fully patched operating systems.
- Logging and monitoring on systems that are capable.
- Host based firewalls on all systems.
- A router that can be configured to provide some additional filtering
- Soon to come, vulnerability scanning.

Now when the SNORT alerts of the BlackICE alarms fire, it is usually something to get excited about. Like this morning when BlackICE and SNORT light up when the worm described in CERT Advisory CA-2001-11 sadmind/IIS Worm visited the web server.SNORT was nice enough to record the following:

```
[**] spp_http_decode: IIS Unicode attack detected [**]
05/08-02:28:28.408799 xx.xx.209.49:47316 -> yy.yy.120.158:80
TCP TTL:239 TOS:0x0 ID:16758 IpLen:20 DgmLen:135 DF
***AP*** Seq: 0xF218C71A  Ack: 0x14E3C110  Win: 0x2238  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The next step is to update the Linux box so that the Nessus vulnerability scanner[14] is operational. Can't finance the operation of the ISS vulnerability scanner either. This fills in another critical layer in the layered defense of the SOHO fortress…

It is possible to create a reasonably secure home network with effective intrusion detection. All of this and it only cost a few hundred dollars. Thanks to freeware, shareware, homeware, Open Source rebates, and some reasonably prices commercial software and hardware. Remember, just because your paranoid, doesn't mean that someone isn't out to get ya (or your system in this case)…

References

Books and Papers

Network Intrusion Detection; An Analyst's Handbook; Stephen Northcutt, Judy Novak

The Practical Intrusion Detection Handbook; Paul E. Proctor

An Analysis of the Snort Network Intrusion Detection System by Mark D. Tollison
http://www.sans.org/infosecFAQ/intrusion/snort2.htm

http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm

The Need for Multi-layered Defenses on the Personal PC
http://www.sans.org/infosecFAQ/homeoffice/defenses.htm

Connecting Your Home LAN to the Internet – Securely Andrew S. Baker March 27, 2001
http://www.sans.org/infosecFAQ/homeoffice/home_LAN.htm

Cable/DSL Router and Personal Firewall: Belt and Suspenders? Mike McCabe February 14, 2001 http://www.sans.org/infosecFAQ/homeoffice/cable.htm

[14] http://www.nessus.org

How Complicated Is Home Protection? Dale Hillman November 23, 2000
http://www.sans.org/infosecFAQ/homeoffice/protection.htm

A Hardware Based Firewall Option for the SOHO (Small Office/Home Office) User. A look into the LINKSYS Etherfast Cable/DSL Router. Scott Kisser December 4, 2000
http://www.sans.org/infosecFAQ/homeoffice/option.htm

Products

SNORT http://www.snort.org

WIN32 Graphic Interface for Snort – http://www.xato.net/downloads

WinDump http://netgroup-serv.polito.it/windump/

Zone Alarm http://www.zonelabs.com/

BlackICE http://www.networkice.com

Nessus http://www.nessus.org/

Netgear FR314 http://www.netgear.com/product_view.asp?xrp=4&yrp=12&zrp=82

SonicWALL SOHO2 http://www.sonicwall.com/products/soho/index.html

Assignment 3 - "Analyze This" Scenario

Security Analysis for GIAC Enterprises

Prepared by *David Anderson*
Soon to be certified GCIA Intrusion Detection Analyst
No Hole Too Small
A Computer Security Services Company

Introduction

Our organization, *No Hole Too Small* (here after called vendor), has been asked to provide a bid for security services to *GIAC Enterprises* (here after called customer). The first step in the process of generating the bid is an analysis of the security of the customers network.

GIAC Enterprises is an e-business startup that sells electronic fortune cookie sayings. The vendor was provided with one month's worth of data from a Snort system with what is believed to be a fairly standard rulebase. Unfortunately, from time to time, the power has failed or the disk was full the vendor was not provided with data for all days covered by the monitoring.

The vendor was tasked with analyzing the data provided. The vendor was asked to be especially alert for signs of compromised systems or network problems. An analysis report was requested.

Data Overview

The Vendor was provided with four compressed files containing the data for analysis. These files are approximately 15MB in size. Once uncompressed this provided 98 files comprising 155 MB of data for the analyst to process. Dates were missing from the data set. Limited information was provided concerning the methods used to collect the data.

Analysis Overview

Due to the large155 MB dataset provided by the customer and the short time period available for analysis, a detailed analytical review of each event in the data set would be impossible. Therefore, a focused review of critical issues was conducted in addition to a detailed overview of the security issues contained in the data set.

The first step was to organize the large dataset so that it was useful. The available files were review for content structure and organization. They were prioritized by file type as follows: alerts, scan, and then OOS.

The files were prepared for importation into a FoxPro database. The IP:port information was split into separate fields in the databases. The following procedure was used.

```
* procedure SPLITIP.PRG
USE e:\sanscert\part3\alerts.dbf EXCLUSIVE
browse
goto top
replace all s_port with substr(source,at(":",source)+1)
replace all d_port with substr(dest,at(":",dest)+1)
replace all source with substr(source,1,at(":",source)-1)
replace all dest with substr(dest,1,at(":",dest)-1)
browse
use
```

The following steps were used to clean up the entries in database

```
make new table with  portscans and Watchlist
SELECT *;
 FROM alerts;
 WHERE AT("spp_portscan",Alerts.alert) > 0;
 INTO TABLE spp_portscan.dbf

SELECT *;
 FROM alerts;
 WHERE AT("Watchlist",Alerts.alert) > 0;
 INTO TABLE watchlist.dbf

SELECT *;
 FROM alerts;
 WHERE AT("scan",Alerts.alert) > 0;
   OR (AT("NMAP",Alerts.alert) > 0);
   OR (AT("fingerprint",Alerts.alert) > 0);
 INTO TABLE scans.dbf

remove portscans, scans  and Watchlists from rest alert table

delete for AT("spp_portscan:",Alerts.alert) > 0
delete for AT("Watchlist",Alerts.alert) > 0
delete for AT("scan",Alerts.alert) > 0
delete for AT("fingerprint",Alerts.alert) > 0
delete for AT("NMAP",Alerts.alert) > 0
pack

Extract spp portscan detections from spp table
SELECT *;
 FROM spp_portscan;
 WHERE AT("DETECTED",Spp_portscan.alert) > 0;
 ORDER BY Spp_portscan.source

replace all source with substr(alert,at("from",alert)+5)
replace all source with  substr(source,1,at("(",source)-1)
```

The following were the result of this processing:

```
490498 combined alert records before split
 26920 alert records after split
  5336 Tiny Fragment records after split
 53294  scan records after split
108317 watchlist records after split
296477 spp_portscan records after split
   154 Broadcast records after split
```

Now we have a more manageable dataset to review. A similar approach was used to process the search records into the database for evaluation. This created approximately 1.3 million records from the scan files. Grep was used to extract information from concatenated versions of the data files. Excel was used as an additional analysis tool.

Data Analysis

Alert Analysis

Alert Analysis Summary

There were a total of 32265 detected alerts indicating possible hostile activity. This excludes scanning activity that will be addressed separately. 32 MY.NET hosts generating 1002 alerts were detected as sources for alerts. The remaining 31154 alerts were generated from 686 external addresses. All of the alerts were collected on the companies' network using SNORT with what seem to be a standard ruleset.
Table 1 outlines a summary of the SNORT alerts detected on the companies' network. Table 2 identifies and summarizes the primary host sources causing alerts on the companies' network. Likewise, Table 3 identifies the primary destination hosts that were identified in alerts. Table 4 lists the primary target ports of the detected alerts. The scan files contain 1312807 records that were imported into FoxPro for evaluation with some help from Perl.

Table 1 - Alert Summary

Alert	Total	External	Internal
Totals	32256	31154	1002
DNS udp DoS attack described on unisog	16146	16146	0
Tiny Fragments	5336	5329	7
Connect to 515 from outside	4238	4238	0
WinGate 1080 Attempt	2234	2234	0
Attempted Sun RPC high port access	2048	2048	0
SNMP public access	591	173	418
Russia Dynamo - SANS Flash 28-jul-00	546	104	442
SMB Name Wildcard	513	437	76
SUNRPC highport *access!*	204	204	0
Connect to 515 from inside	159	0	159
TCP SMTP Source Port traffic	100	100	0
Back Orifice	77	77	0
External RPC call	59	59	0
SITE EXEC - Possible wu-ftpd exploit - GIAC000623	3	3	0
Happy 99 Virus	1	1	0
STATDX UDP attack	1	1	0

Table 2 - Top 10 Alert Source IP Addresses

Internal SourceHosts	Records	External SourceHosts	Records	Resolved Name
MY.NET.205.138	442	209.67.50.203	16132	futuresite.register.com
MY.NET.70.38	137	141.211.176.99	2236	vishuman28.us.itd.umich.edu
MY.NET.97.244	74	216.119.15.88	1273	216-119-15-88.o1.jps.net
MY.NET.162.201	71	209.217.166.69	713	Verio, Inc. Englewood, CO
MY.NET.97.155	60	205.188.153.100	569	fes-d004.icq.aol.com
MY.NET.101.160	58	205.188.153.108	492	fes-d012.icq.aol.com
MY.NET.98.134	40	205.188.153.106	397	America Online, Inc Sterling, VA
MY.NET.97.52	33	128.46.156.231	161	ece156-dhcp-2.ecn.purdue.edu
MY.NET.97.168	33	205.188.153.104	154	fes-d008.icq.aol.com
MY.NET.97.133	26	205.188.153.101	149	fes-d005.icq.aol.com

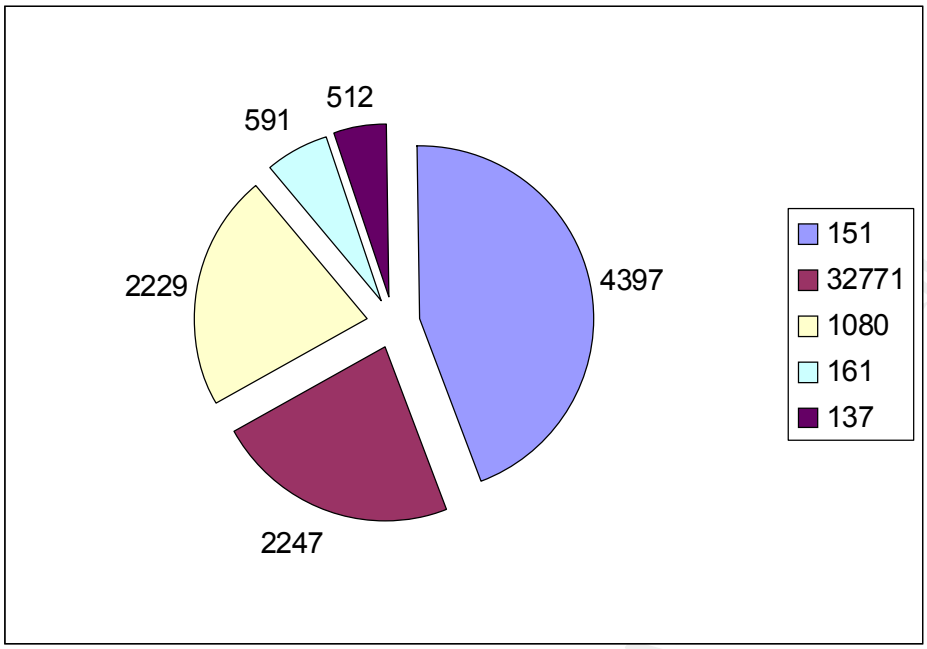
Table 3 - Top 10 Destination Hosts IP Addresses

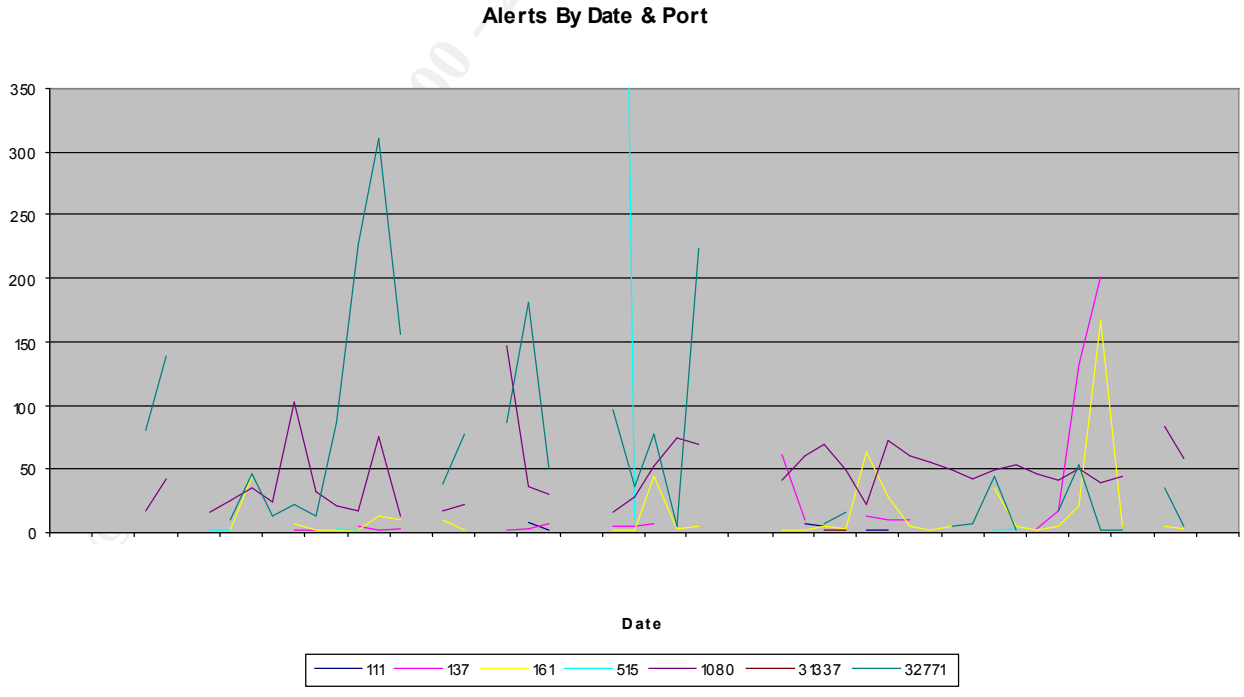
Internal Destinations	3827	External Destinations	11	
MY.NET.1.3	5411	194.87.6.38	442	38.6.87.194.dynamic.dol.ru
MY.NET.1.4	5390	216.181.129.185	9	PrimusDSL, Inc. Sterling, VA
MY.NET.1.5	5331	64.23.4.67	3	chimay.skynetweb.com
MY.NET.213.158	657	212.187.65.135	3	c65135.upc-c.chello.nl
MY.NET.222.218	433	128.8.3.106	3	bay6.umd.edu
MY.NET.100.209	405	129.155.192.99	2	Sun Microsystems, Inc. Mountain View, CA
MY.NET.99.104	404	24.13.123.8	1	cc61691-a.abdn1.md.home.com
MY.NET.101.192	374	151.196.73.119	1	Bell Atlantic Reston, VA
MY.NET.130.86	260	148.243.214.7	1	na-148-243-214-7.na.avantel.net.mx
MY.NET.97.213	225	131.204.205.101	1	Auburn University Auburn University, AL

Table 4 - Target Port Summary

Port	Records
53	16132
151	4397
32771	2247
1080	2229
161	591
137	512
2478	442
6699	104
25	96
31337	77
111	59

Figure 6 - Significant Alert Destinations





Alert Analysis Details

DNS udp DoS attack described on unisog

Probability the source address was spoofed

In order for this attack to work, the IP address must be spoofed[15].

Description of attack

The attack uses DNS to execute a packet flooding Denial of Service (DoS) attack. This DoS attack started on 01/06/2001 at 18:30:02.600073 and continued until 20:00:01.567114. There were 16146 detects by SNORT related to this attack. All of the 16132 DNS UDP DoS detects originated from a single host, 209.67.50.203 (futuresite.register.com). One-half of the total alert detects were generated by this specific attack. A small sample of the alert records is shown below.

```
01/06-20:00:00.939018  [**] DNS udp DoS attack described on unisog
[**] 209.67.50.203:20065 -> MY.NET.1.5:53

01/06-20:00:00.968516  [**] DNS udp DoS attack described on unisog
[**] 209.67.50.203:28054 -> MY.NET.1.4:53

01/06-20:00:01.567114  [**] DNS udp DoS attack described on unisog
[**] 209.67.50.203:23516 -> MY.NET.1.3:53
```

Evidence of Active Targeting

This attack targets DNS servers. Three of the companies' addresses were targeted in this attack. MY.NET.1.3, MY.NET.1.4, and MY.NET.1.5. These servers appear to be DNS servers for the company.

Attack Mechanism

This attack is initiated by sending numerous UDP DNS requests with a spoofed source IP address. The DNS responses are returned to the spoofed IP address[16]. The holder of the spoofed IP address is the unlucky victim as is the case with many other IP spoof Dos attacks. The nameserver acts as the middleman in this attack amplifying traffic in the process. As in many other attacks where the source IP address is spoofed the real source of the attack is difficult if not impossible to identify.

The DNS response can have a 538 byte, or larger, answer can cause significant traffic. With the approximate 3 DNS inbound packets per second estimated traffic flow can excede45 Mb/s of traffic[17]. More detailed information describing this attack is available at:

- Report Date: January 11, 2001 http://www.sans.org/y2k/011101.htm
- DoS attacks using the DNS ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos

---

[15] ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos, DoS attacks using the DNS

[16] http://www.cert.org/incident_notes/IN-2000-04.html CERT® Incident Note IN-2000-04

[17] http://www.sans.org/y2k/011101.htm, Report Date: January 11, 2001 - 1000

- CERT® Incident Note IN-2000-04 http://www.cert.org/incident_notes/IN-2000-04.html

Correlations

This attack had not been discovered in earlier investigation of the companies' security. No CVE entries or candidates were located. Information was located from both AUSCERT (ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos) and CERT (http://www.cert.org/incident_notes/IN-2000-04.html).

The first locatable information concerning this attack was described on Unisorg (http://www.theorygroup.com/Archive/Unisog/2001/msg00005.html). It described as a steady stream (~220/min/DNS server) of DNS requests originating from 209.67.50.203[18]. The admin for this address indicated that they are not the source but the target of a DoS attack seeing 60 - 90 Mb data stream toward 209.67.50.203. Additional information from this thread is available at:

- http://www.theorygroup.com/Archive/Unisog/2001/msg00033.html
- http://www.theorygroup.com/Archive/Unisog/2001/msg00008.html
- http://www.theorygroup.com/Archive/Unisog/2001/msg00007.html
- http://www.theorygroup.com/Archive/Unisog/2001/msg00018.html
- http://www.theorygroup.com/Archive/Unisog/2001/msg00011.html
- http://www.theorygroup.com/Archive/Unisog/2001/msg00029.html

The most descriptive correlation comes from *GIAC Report Date: January 09, 2001 – 1300*, http://www.sans.org/y2k/010901-1300.htm. An excerpt is included trace records and is listed here.

> *(Joe Matusiewicz)*[19]
> *Futuresite.register.com is the victim of a DoS attack. Someone is spoofing their source address and sending queries to DNS servers all over the Net. My traces look like this:*
>
> ```
> 2001/1/8 12:59:02.177788 209.67.50.203.6151 >
> my.dns.server1.53: 24585+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.311022 209.67.50.203.4894 >
> my.dns.server2.53: 3293+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.583484 209.67.50.203.24933 >
> my.dns.server3.53: 9234+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.617994 209.67.50.203.26315 >
> my.dns.server42.53: 39809+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.747418 209.67.50.203.5737 >
> my.dns.server1.53: 38829+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.752486 209.67.50.203.27229 >
> my.dns.server3.53: 60955+ MX?  aol.com. (25) (DF)
> 2001/1/8 12:59:02.774917 209.67.50.203.15825 >
> ```
>
> *I was getting them at a rate of 29,000 an hour against 4 DNS servers. In the beginning they were bouncing off my firewall but now my border*

[18] http://www.theorygroup.com/Archive/Unisog/2001/msg00005.html, National Radio Astronomy Observatory, Ph: 804 296 0327

[19] http://www.sans.org/y2k/010901-1300.htm, Report Date: January 09, 2001 - 1300

router just sends them to the bit bucket. I called Exodus.com and they told me that the register.com admins put an incoming filter on their border.

Here are some additional CVEs related to DNS:

CVE-1999-0048 CVE-1999-0024	CVE-1999-0299 CVE-1999-0275	CVE-1999-0184 CVE-1999-0010	CVE-1999-0274

Defensive recommendation

The general method used to stop this traffic has been to block traffic from 209.67.50.203. Some networks have blocked traffic from the subnet 209.67.50.0. Additionally, Also, an egress filtering should be enabled to help ensure that the companies network does not initiate an attack like this[20].

More detailed information is available from AUSCERT ALERT AL-1999.004 (ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos). It provides, in addition to other information, details on the configuration of BIND version 8. Additional information may also be found at:

- http://www.cert.org/advisories/CA-96.21.tcp_syn_flooding.html
- ftp://ftp.auscert.org.au/pub/mirrors/ftp.isi.edu/in-notes/rfc2267.txt
- http://www.cert.org/incident_notes/IN-2000-04.html
- http://www.sans.org/y2k/010901.htm
- http://www.sans.org/y2k/011101.htm

Tiny Fragments

Probability the source address was spoofed

Some source IP may be valid while others could possibly be spoofed. There isn't sufficient data or time available to justify further investigation.

Description of attack

Tiny Fragment traffic is created when the TCP packets are fragmented smaller that "normal" for operating systems and routers usage.

Of the total 5336, 48.5% of the detects were generated by the top five external host IP addresses. Shown below in Figure 7 are the primary source IP addresses for the tiny fragments traffic. A small sample of the alert records extracted via `grep "Tiny " scanall.txt` is shown below.

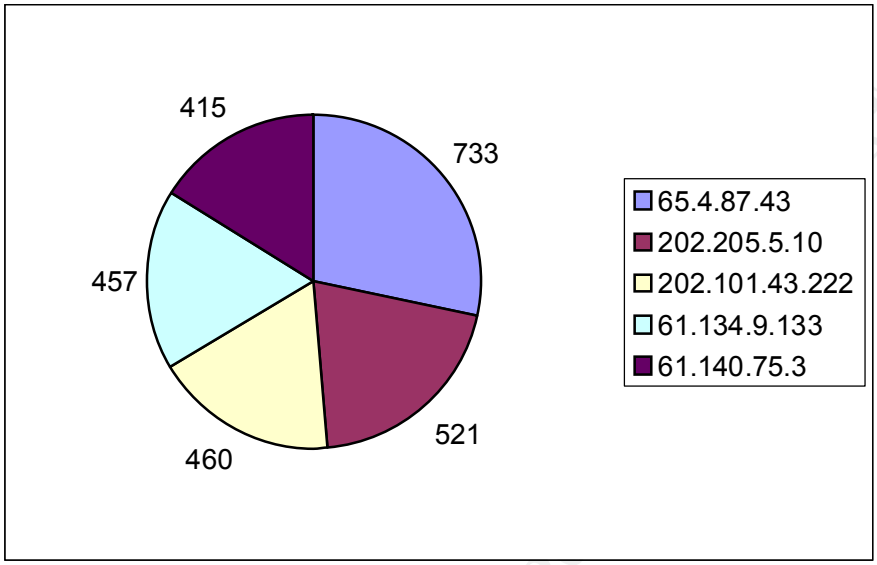
```
01/04-18:21:32.656548  [**] Tiny Fragments - Possible Hostile
Activity [**] 61.140.75.4 -> MY.NET.1.10

01/04-18:21:54.296324  [**] Tiny Fragments - Possible Hostile
Activity [**] 202.108.43.152 -> MY.NET.1.8
```

[20] http://www.sans.org/y2k/011101.htm, Report Date: January 11, 2001 - 1000

Seven of the tiny fragment detects were generated from the local host MY.NET.219.122. All of the outbound traffic for the Tiny Fragments generated from MY.NET.219.122 was targeted at 208.162.62.208 (Chassis2harc2-ppp39.alaweb.com owned by Covington Electric/Alaweb Andalusia, AL).

Figure 7 - Primary Tiny Fragments Source IP Addresses



Evidence of Active Targeting

There appears to be some active targeting of tiny fragments. Nearly all, 96.29%, of the tiny fragments traffic was targeted at three MY.NET hosts, with 59.63% bound for MY.NET.1.8. Targeted host details are displayed in Table 5.

Table 5- Primary Tiny Fragments Destination IP Addresses

Source Address	Alerts	% Of Total
MY.NET.1.8	3235	59.63%
MY.NET.1.10	1262	23.26%
MY.NET.217.162	727	13.40%

Attack mechanism

While possible to occur for normal traffic transport, tiny fragments are generally indicative of hostile traffic. Tiny Fragment traffic can be used for DoS attacks, to attempt to bypass intrusion detection systems, and to communicate in a covert channel[21].

Correlations

[21] Network Intrusion Detection: An Analyst's Handbook; Stephen Northcut, Judy Novak –pg47,246

Correlations were found in the OOS files that, while unable to specifically identify tiny fragments, identified the use of crafted packets. Examples are shown here.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/09-17:38:45.371358 65.26.4.145:48 -> MY.NET.217.162:6699
TCP TTL:110 TOS:0x0 ID:21999  DF
21SFR**U Seq: 0x6330EC6   Ack: 0xC96B0114   Win: 0x5010
TCP Options => EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
01/05-10:37:34.044997 194.234.48.26:21 -> MY.NET.217.162:21
TCP TTL:27 TOS:0x0 ID:39426
**SF**** Seq: 0x519B7EF3   Ack: 0x2BBEABB0   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/28-20:21:49.698103 139.130.61.206:109 -> MY.NET.217.162:109
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x60D655C6   Ack: 0x397F5CF2   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

There were also supporting records in the scan files. An example is shown here.

```
Dec 10 06:03:40 147.8.182.157:109 -> MY.NET.1.10:109 SYNFIN **SF****
```

There are correlations for SANS Analysis Reports:
http://www.sans.org/y2k/122900.htm Report Date: December 29, 2000 – 1000
http://www.sans.org/y2k/052400-1300.htm - Detects Analyzed 5/24/00
http://www.sans.org/y2k/012301.htm - Report Date: January 23, 2001 - 1400
Correlations from http://www.sans.org/y2k/121900.htm (David Hoelzer)
Additionally, there are several correlations of tiny fragments traffic and prior reviews of the companies' security. The number if tiny fragments alerts appears to be increasing.
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Robert_Currie.doc
http://www.sans.org/y2k/practical/Markus_DeShon.html
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Crist_Clark_GCIA.html
http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_5.__Tiny
http://www.sans.org/y2k/practical/Eric_Hacker.html#_Toc490920406
http://www.sans.org/y2k/practical/Jeffrey_Taylor_GCIA.html
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc

Defensive recommendation

The hosts MY.NET.1.8, MY.NET.1.10, and MY.NET.217.162 have records identifying them as the source of tiny fragments and are possibly compromised. They should be checked for the presence of installed Trojan or backdoors.

Connect to 515 from outside & inside

Probability the source address was spoofed

Traffic is recon for vulnerable hosts and/or connection attempts to invoke the exploit. Source IP addresses are likely valid.

Description of attack

LPRng is a replacement print service for the BSD lpd printing service. It contains multiple format string vulnerabilities that will allow remote users to execute arbitrary code on vulnerable systems. A subset of the port 515 connect scan records extracted via `grep ":515 " scanall.txt` is shown below.

```
Dec 16 21:08:57 209.217.166.69:4199 -> MY.NET.2.127:515 SYN **S*****
Dec 16 21:08:57 209.217.166.69:4201 -> MY.NET.2.129:515 SYN **S*****
Dec 16 21:08:57 209.217.166.69:4202 -> MY.NET.2.130:515 SYN **S*****
Dec 16 21:08:57 209.217.166.69:4208 -> MY.NET.2.136:515 SYN **S*****
Dec 16 21:08:59 209.217.166.69:4752 -> MY.NET.4.170:515 SYN **S*****
Dec 16 21:08:59 209.217.166.69:4808 -> MY.NET.4.226:515 SYN **S*****

Dec 20 21:58:38 MY.NET.163.17:2178 -> 148.243.214.7:515 SYN **S*****
```

Two types of alerts were detected by snort related to port 515 connect. 4238 detects for connection attempts to port 515 from outside and 159 detects for connection attempts to port 515 from the inside. For all of the external 515 connection alerts, 99% originated from the hosts listed in Table 6.

Table 6 - Primary Source IP Address for External 515 Connect

Source Address	Alerts	Resolved Name
141.211.176.99	2236	vishuman28.us.itd.umich.edu
216.119.15.88	1273	216-119-15-88.o1.jps.net
209.217.166.69	713	Verio, Inc. Englewood, CO

For all of the internal 515 connection alerts, 92% originated from the hosts listed in Table 7. This traffic could be valid

One interesting source port, MY.NET.163.17, had 515 connections to an outside host address; 148.243.214.7. It resolves to na-148-243-214-7.na.avantel.net.mx.

Table 7 - Primary Source IP Address for Internal 515 Connect

Source Host	Alerts
MY.NET.70.38	137
MY.NET.98.151	9

Evidence of Active Targeting

Most traffic for this alert is scanning for a vulnerable host. No specific host stands out as being targeted.

Attack mechanism

LPRng, is a print-service now being packaged with open-source Linux distributions. LPRng has missing format string arguments in at least two calls to the syslog() function.

These function calls allow user-supplied arguments to be passed to port 515/tcp. A buffer overflow allows the execution of arbitrary code[22]. The Ramen Worm has the ability to target the LPRng printer service vulnerability.[23] The data set provided does not provide sufficient information to rule out an attack by the Ramen Worm. The primary scan IP addresses were not found in the OOS files where a Ramen signature may be detectible.

Correlations

While records were identified in both the alert and the scan files, the OOS files showed no evidence of the Port 515 Connects. Port 515 Connects from inside are identified in earlier evaluations of the companies' security. The connection attempts from outside were not seen in earlier reviews.
http://www.sans.org/y2k/practical/chris_kuethe_gcia.html#2.10.
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc

Additional information concerning the Port 515 Connects is available at the locations listed below:
http://www.kb.cert.org/vuls/id/382365
http://www.cert.org/advisories/CA-2000-22.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0917
http://www.sans.org/y2k/the_compromise.htm
http://www.sans.org/newlook/alerts/port515.htm - Alert: Increased probes to TCP port 515
http://www.sans.org/y2k/040901-1500.htm

http://www.sans.org/y2k/041201-1500.htm

Scan files were also correlated with the alert records with the following SQL

```
SELECT *;
 FROM scan1fix;
 WHERE Scan1fix.d_port == "515"
```

CVE-2000-0917 - Format string vulnerability in use_syslog() function in LPRng 3.6.24 allows remote attackers to execute arbitrary commands[24].

BUGTRAQ – 20000925 - Format strings: bug #2: LPRng

http://www.cert.org/advisories/CA-2000-22.html - CERT® Advisory CA-2000-22 Input Validation Problems in LPRng

Defensive recommendation

The reason for outgoing port 515 traffic from MY.NET.163.17 should be identified.

---

[22] https://www.kb.cert.org/vuls/id/382365 - Vulnerability Note VU#382365

[23] http://www.sans.org/infosecFAQ/malicious/ramen.htm The Ramen Worm and its use of rpc.statd, wu-ftpd and LPRng Vulnerabilities in Red Hat Linux

[24] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0917

Security patches should be applied or LPRng should be upgraded to a non-vulnerable version. Block access to printer service on port 515/tcp using firewall or packet-filtering technologies.

WinGate 1080 Attempt

Probability the source address was spoofed

The WinGate connection attempts are to invoke the exploit. Source IP addresses are likely valid.

Description of attack

WinGate is a software package that allows a Local Area Network (LAN) to share a single Internet connection via Proxy and NAT[25]. Sample alert records extracted via `grep "WinGate" SnortAall.txt` is shown below.

```
01/16-19:54:21.253143  [**] WinGate 1080 Attempt [**]
216.179.0.32:1460 -> MY.NET.98.227:1080

01/16-20:46:56.356065  [**] WinGate 1080 Attempt [**]
216.179.0.32:1914 -> MY.NET.97.105:1080

01/16-20:55:04.551061  [**] WinGate 1080 Attempt [**]
216.179.0.32:2507 -> MY.NET.97.93:1080

01/16-21:05:13.059699  [**] WinGate 1080 Attempt [**]
216.179.0.32:3257 -> MY.NET.60.38:1080
```

The hosts listed in Table 8 were the primary hosts attempting a WinGate attempt. While they were the primary hosts they only totaled less than 10% of the total 2234 alerts for WinGate connection attempts.

Table 8 - Primary WinGate Connect Attempt Hosts

Source Address	Alerts	Resolved Name
212.72.75.236	64	ONLINE-KIOSK GmbH
212.73.162.30	40	tiger.swepipe.com
209.61.189.49	37	pluto.planetwebspace.com
216.152.64.142	30	Java.ca.us.webchat.org
216.152.64.211	27	Finance.webmaster.com

Attack mechanism

Connections are not logged by default configuration. The default configuration also allows WinGate to accept any incoming connections. Intruders can use WinGate to

[25] http://wingate.deerfield.com/

effectively hide their true IP addresses during attacks[26]. WinGate also installs without a password allowing attackers to redirect connections without authentication[27].

Correlations

WinGate connection attempts have been seen in numerous reviews of the companies' security in the past. They are listed here:

http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Markus_DeShon.html
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Robert_Currie.doc
http://www.sans.org/y2k/practical/Eric_Hacker.html
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm#assign3
http://www.sans.org/y2k/practical/Bill_Royds.zip
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/David_Thibault_GCIA.html#ANALYZE_THIS
http://www.sans.org/y2k/practical/John_Best.htm#assign3

Additional WinGate information is available from CERT and SANS. Links to some are included here:

http://www.cert.org/vul_notes/VN-98.03.WinGate.html - CERT Vulnerability Note VN-98.03
Report Date: March 28, 2001 – 1200 http://www.sans.org/y2k/032801-1200.htm
GIAC- Detects Analyzed 5/28/00 - http://www.sans.org/y2k/052800-1100.htm
GIAC - Detects Analyzed 8/13/00 - http://www.sans.org/y2k/081300.htm

Defensive recommendation

The connections attempts to WinGate are probably benign as WinGate is not likely in use on the network because of the network size and configuration. The use of WinGate should probably be avoided on the companies' network unless it in necessary. If used, WinGate connection logging must be enabled. The necessary proxies should be bound to the machine's internal IP address. WinGate v2.1 version has the ability to install using a more secure default configuration[26].

SNMP public access

Probability the source address was spoofed

The host addresses are to be expected valid, as the SNMP connection requires a valid connection.

Description of attack

[26] http://www.cert.org/vul_notes/VN-98.03.WinGate.html

[27] CVE-1999-0291 - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0291

SNMP (Simple Network Management Protocol) is used to monitor and administer many network devices and computers. A number of internal hosts are still to try to access host MY.NET hosts using default public SNMP settings. A new added threat appears in this review in that there external hosts attempting public SNMP access. Purdue University appears to want to help the company manage its resources. A subset of the SNMP alert records extracted via `grep "SNMP" SnortAall.txt` is shown below.

```
01/12-01:42:52.645350  [**] SNMP public access [**]
MY.NET.162.201:1819 -> MY.NET.50.154:161

01/12-01:42:53.845474  [**] SNMP public access [**]
MY.NET.162.201:1819 -> MY.NET.50.154:161

01/12-09:17:50.224557  [**] SNMP public access [**]
128.183.38.30:1032 -> MY.NET.154.26:161

:01/12-09:27:50.250923  [**] SNMP public access [**]
128.183.38.30:1032 -> MY.NET.154.26:161
```

Listed in Table 9 are the top hosts that created 80% of the alerts. The targeted hosts are listed in Table 10.

Table 9 - Top Public SNMP Connection Attempt Hosts

Source Host	Alerts
128.46.156.231 ece156-dhcp-2.ecn.purdue.edu	161
MY.NET.97.244	74
MY.NET.162.201	71
MY.NET.97.155	60
MY.NET.98.134	40
MY.NET.97.168	33
MY.NET.97.52	33

Table 10 - Targeted MY.NET SNMP Hosts

MY.NET.14.1	MY.NET.100.99
MY.NET.50.154	MY.NET.101.192
MY.NET.100.143	MY.NET.154.26
MY.NET.100.206	

Attack mechanism

SNMP uses an unencrypted "community string" for its authentication. Most SNMP equipment is delivered with the default community string "public". This leaves such equipment open for compromise. Equipment in such a state can easily be attacked using many of the common tools available for SNMP hardware management.

Correlations

This has been repeatedly referenced in earlier reports.
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Robert_Currie.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Bill_Royds.zip

This item is number 10 on the list of The Ten Most Critical Internet Security Threats (http://www.sans.org/topten.htm)

CVE Entries:

Default or blank SNMP community name (public) - CAN-1999-0517
Guessable SNMP community name - CAN-1999-0516
Hidden SNMP community strings - CAN-1999-0254, CAN-1999-0186

Defensive recommendation

Purdue University should be contacted about the status of ece156-dhcp-2.ecn.purdue.edu. The host may be compromised.

If the company does not absolutely require SNMP, it should be disabled to remove many security threats[28]. If SNMP is required appropriate modifications must be made to the hardware to correct the poor naming in use.

Russia Dynamo - SANS Flash 28-jul-00

Probability the source address was spoofed

There appears to be a stable communication channel between the two hosts involved. The Host IP is valid.

Description of attack

All of the traffic for the alert is between MY.NET.205.138:6699 and 194.87.6.38:2478. 194.87.6.38:2478 resolves to 38.6.87.194.dynamic.dol.ru and is registered to Demos Company Ltd. Moscow Russia. It is also possible that this is a false positive and the traffic is Napster traffic. Napster is known to use port 6699 as its data channel. The following sample was extracted from the alert file via `grep "Russia" SnortAall.txt`.

```
12/08-16:09:05.164572 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 ->194.87.6.38:2478
```

[28] http://www.sans.org/topten.htm

```
12/08-16:09:14.532328 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
194.87.6.38:2478 -> MY.NET.205.138:6699

12/08-16:09:18.221557 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478

12/08-16:09:20.714259 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478

12/08-16:09:24.108584 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
```

Evidence of Active Targeting

This traffic appears isolated between the two hosts involved.

Attack mechanism

This appears to be a communication channel between the two hosts described above.

Correlations

There were no indications of questionable traffic for the two IP addresses involved in this traffic in either the scan files of the OOS files.

Without having the snort rule available, it is difficult to understand specifically what the trigger was. However, when reviewing the data grepped from the scan files involved with port 6699, it would be nearly impossible to classify all of this traffic as normal Napster traffic:

```
Dec 7 06:34:20 24.112.199.246:2113 -> MY.NET.204.114:6699 INVALIDACK
*1*FR*A* RESERVEDBITS
Dec 7 07:28:44 149.151.195.233:6699 -> MY.NET.215.166:1971 FULLXMAS 2*SFRPAU
RESERVEDBITS
Dec 7 07:29:04 149.151.195.233:6699 -> MY.NET.215.166:1971 FULLXMAS 2*SFRPAU
RESERVEDBITS
Dec 7 07:29:05 149.151.195.233:0 -> MY.NET.215.166:6699 FULLXMAS 2*SFRPAU
RESERVEDBITS
Dec 7 15:38:12 129.171.170.225:2334 -> MY.NET.212.78:6699 NOACK **S****U
Dec 7 20:08:30 24.65.255.98:6699 -> MY.NET.205.246:1104 VECNA 2****P**
RESERVEDBITS
Dec 7 21:18:59 24.23.121.89:6699 -> MY.NET.98.181:1044 INVALIDACK 21SFR*A*
RESERVEDBITS
Dec 7 21:57:32 24.200.184.120:1047 -> MY.NET.223.134:6699 UNKNOWN *1*F*PA*
RESERVEDBITS
Jan 1 11:00:14 209.255.209.109:1056 -> MY.NET.140.151:6699 SYN **S*****
Jan 1 14:57:15 MY.NET.201.94:1150 -> 130.111.153.104:6699 SYN **S*****
Jan 1 18:08:41 194.208.82.186:6699 -> MY.NET.201.122:4997 UNKNOWN *1**RPA*
RESERVEDBITS
Jan 1 23:34:05 216.232.33.71:6699 -> MY.NET.218.214:1550 NULL ********
Jan 1 23:35:07 216.232.33.71:6699 -> MY.NET.218.214:1550 INVALIDACK **S***AU
```

There were no correlations available for this detect. The SANS Flash 28-jul-00 which was identified in the alert was unobtainable at this time.

Defensive recommendation

The system MY.NET.205.138 should be evaluated to see which services are running on port 6699. Napster should be rules out as a source for this traffic. If there is no valid reason for this traffic, MY.NET.205.138 should be considered compromised.

SMB Name Wildcard

Probability the source address was spoofed

It is likely that the majority of the addresses in these alerts are valid IP involved in Windows/Samba SMB traffic.

Description of attack

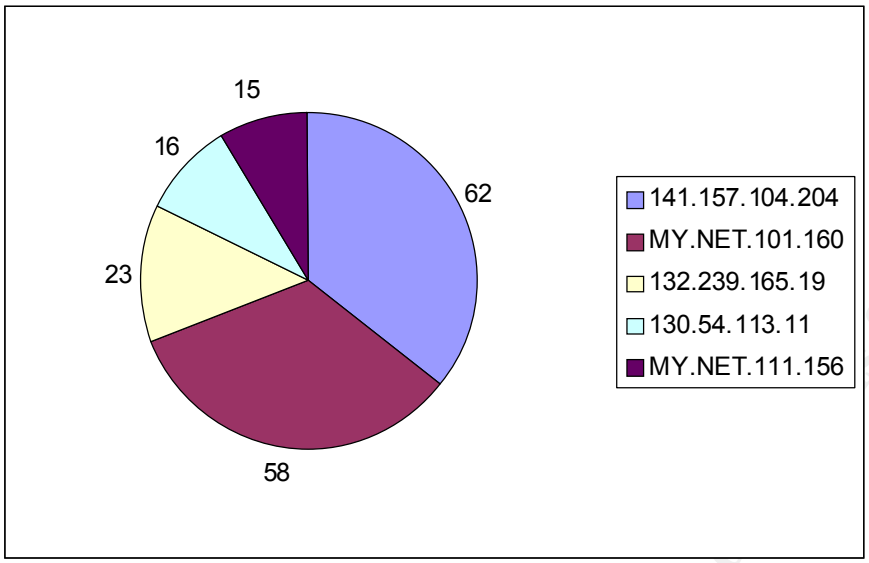
SMB services allow for file sharing over the network, including the Internet. This is the normal method for Windows systems to share objects. With Windows systems, all resources are a name as compared to UNIX, where all resources are a file. The SMB Wildcard is a NetBIOS name query and this probe is probably a prelude to an SMB connection. Traffic between port 137 and port 137 is common on a network with Windows systems, or systems using Samba.

`grep "SMB" SnortAall.txt` was used to grab this sample from the alert file:

```
01/11-20:39:55.613704  [**] SMB Name Wildcard [**]
130.207.201.28:137 -> MY.NET.154.252:137
01/11-20:39:57.110017  [**] SMB Name Wildcard [**]
130.207.201.28:137 -> MY.NET.154.252:137
01/11-20:59:32.959656  [**] SMB Name Wildcard [**]
130.153.158.82:137 -> MY.NET.183.171:137
01/11-20:59:34.459129  [**] SMB Name Wildcard [**]
130.153.158.82:137 -> MY.NET.183.171:137
01/11-20:59:51.086183  [**] SMB Name Wildcard [**]
130.153.158.82:137 -> MY.NET.183.171:137
```

40% of the SMB wild card traffic was generated the five hosts identified in Figure 8. The two MY.Net hosts can likely be disregarded and considered non-hostile hosts. Their traffic is likely normal Windows chatter.

Figure 8- SMB Wildcard Hosts



Attack mechanism

When configured insecurely (the out of the box installation), NetBIOS allows the enumeration of sensitive information from NT systems, exposes critical system files, and may give full file system access. NetBIOS over TCP/IP can allow this access from any host connected to the Internet[29].

Intruders are actively exploiting Windows networking shares that are, in many cases inadvertently, made available for connections across the Internet[30].

An anonymous connection can be created as follows:

```
net use \\sysname\IPC$ "" \user:""
```

A typical connection looks like:

```
[**] SMB Name Wildcard [**]
05/10-18:08:05.359797 badguy.com:137 -> goodguy.com:137 UDP TTL:119
TOS:0x0 ID:45361 Len: 58
00 D4 00 00 00 01 00 00 00 00 00 00 20 43 4B 41 ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 ..[31]
```

The NBTSTAT command can be used to learn names associated with a target. The new network.vbs (and it's derivatives) Internet worm may exploit SMB information (see: http://www.cert.org/incident_notes/IN-2000-02.html)[31].

[29] http://www.sans.org/topten.htm

[30] http://www.cert.org/incident_notes/IN-2000-02.html

[31] http://www.sans.org/newlook/resources/IDFAQ/port_137.htm Port 137 Scan; Bryce Alexander

Correlations

Network Detect 2 – SMB Wildcard Name
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Eric_Hacker.html#anchor9566546
http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_8.__SMB

CERT® Incident Note IN-2000-02; http://www.cert.org/incident_notes/IN-2000-02.html
CVE candidate CAN-1999-0519. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0519

This item is number 7 on the list of The Ten Most Critical Internet Security Threats (http://www.sans.org/topten.htm).
http://www.sans.org/y2k/051300.htm
http://www.sans.org/y2k/071100.htm
http://www.sans.org/y2k/040100.htm
http://www.sans.org/y2k/061500.htm
http://www.sans.org/y2k/041100.htm
http://www.sans.org/y2k/042900.htm
http://www.sans.org/y2k/051800.htm
http://www.sans.org/y2k/050500.htm
http://www.sans.org/y2k/082800.htm
http://www.sans.org/y2k/052800-1130.htm
http://www.sans.org/y2k/111000.htm
http://www.sans.org/y2k/042400.htm
http://www.sans.org/y2k/081200-1300.htm
http://www.sans.org/y2k/111700.htm
http://www.sans.org/y2k/033000.htm
http://www.sans.org/y2k/honeypot_catch.htm

Defensive recommendation

Enable restrict anonymous on windows NT/2000 systems. This will require a valid account to retrieve wildcard SMB information. However, information can still be retrieved by anonymous users if the host name is know (scripts can also retrieve bulk information) unless restrict anonymous is set to level 2. Level 2 is only available with Windows 2000. Restrict anonymous is set to level 2 may cause interaction issues with earlier version of Windows and Samba.

Windows traffic should be block at the boarder router. This should eliminate most external SMB Name Wildcard issues.

Targeted MY.NET hosts should be tested for weak or null passwords. Systems with such passwords should be carefully inspected to verify their security. This would to the 101 hosts contacted by the top three source hosts.

In addition to review the security of the Windows, the UNIX systems should have their NFS usage reviewed.

External RPC call & Sun RPC high port access/attempt

Probability the source address was spoofed

The addresses are valid. A valid address is required to initiate the TPC connection. For the recon traffic, a valid address is necessary to return the recon information collected.

Description of attack

These alerts are triggered by access to port 111 (the portmapper service) or UDP port 32771 (rpcbind). Information can be retrieved that can be used to target known vulnerabilities in RPC related services.

Examples of the three type of alerts related to RPCs that were detected are displayed below as extracted from the alert file via `grep "RPC" SnortAall.txt`.

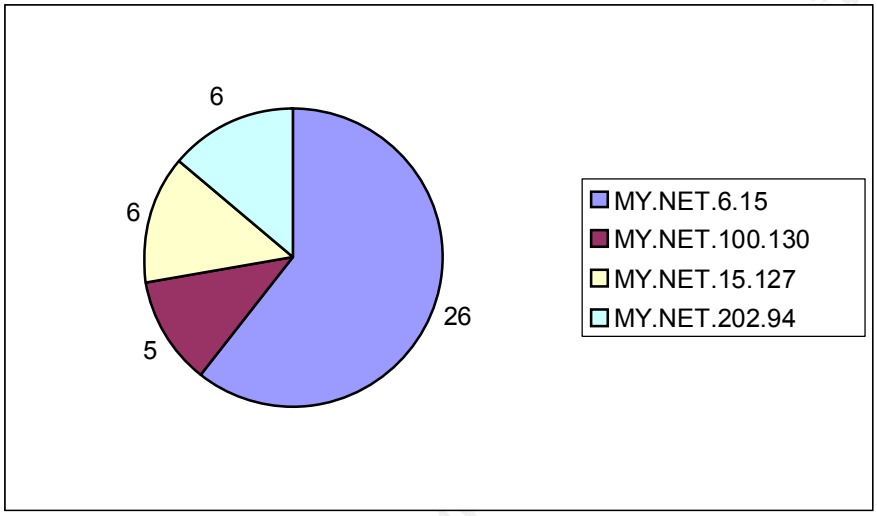
```
01/18-20:12:23.068148  [**] External RPC call [**]
202.84.134.141:748 -> MY.NET.6.15:111
01/18-20:12:23.672941  [**] External RPC call [**]
202.84.134.141:748 -> MY.NET.6.15:111
01/18-20:12:46.806033  [**] External RPC call [**]
202.84.134.141:615 -> MY.NET.15.127:111
01/18-20:16:20.752084  [**] External RPC call [**]
202.84.134.141:718 -> MY.NET.100.130:111
01/18-16:14:20.851226  [**] Attempted Sun RPC high port access [**]
205.188.153.102:4000 -> MY.NET.105.115:32771
01/18-16:18:21.395469  [**] Attempted Sun RPC high port access [**]
205.188.153.102:4000 -> MY.NET.105.115:32771
01/18-16:26:21.299216  [**] Attempted Sun RPC high port access [**]
205.188.153.102:4000 -> MY.NET.105.115:32771
01/18-16:26:36.828690  [**] Attempted Sun RPC high port access [**]
205.188.153.102:4000 -> MY.NET.105.115:32771
01/05-11:19:08.063764  [**] SUNRPC highport access! [**]
128.169.50.34:21 -> MY.NET.5.11:32771
01/05-11:19:08.068073  [**] SUNRPC highport access! [**]
128.169.50.34:21 -> MY.NET.5.11:32771
01/05-11:19:08.158010  [**] SUNRPC highport access! [**]
128.169.50.34:21 -> MY.NET.5.11:32771
01/05-11:19:08.323482  [**] SUNRPC highport access! [**]
128.169.50.34:21 -> MY.NET.5.11:32771
```

Four external hosts generated 61% of the external RPC calls. They are shown in Table 11- Top External RPC Access Hosts. Four MY.NET hosts received 66% External RCP access traffic. They are identified in Figure 9.

Table 11- Top External RPC Access Hosts

Accessing Host	Alerts	Lookup name / Owner
148.228.125.215	13	Benemerita Universidad Autonoma de Puebla Puebla, Puebla MX
195.116.66.14	8	Fabryka Wodek POLMOS w Lancucie Poland
206.210.80.6	8	Stargate Industries, LLC Pittsburgh, PA
63.11.25.117	7	1Cust117.tnt1.yakima.wa.da.uu.net

Figure 9 - Top External RCP Access Targets



Of the total SUN RPC highport Access, 90 % were generated from the hosts listed in Table 12.

Table 12 – SUN RPC highport Access Source Hosts

Accessing Host	Alerts
205.188.153.139	91
24.180.202.45	35
64.4.13.74	19

Table 13 - Primary SUNRPC highport accessed hosts

Accessing Host	Alerts
MY.NET.98.199	91
MY.NET.99.51	35
MY.NET.213.158	19

92.6% of the attempted high port accesses were from the hosts listed in Table 14.

Table 14 - Primary Sun RPC high port attempt hosts

Attempting Host	Alerts
205.188.153.100	569
205.188.153.108	492
205.188.153.106	397
205.188.153.104	154
205.188.153.101	149
205.188.153.102	73
205.188.153.105	63

Attack mechanism

External RPC call, Sun RPC highport access and Attempted Sun RPC high port access alerts are all related to RPC services on UNIX systems.[32]. rpcbind listens on high numbered port 32771. This port is generally not filtered, as is the default port 111. This allows the bypassing of packet filters, such as TCP wrappers, and the security that these filters provide. There are many exploits connected with RPC services[33]. Successful use of these exploits generally result in root comprise of the system. Below is an apparent exploit utilizing the vulnerabilities presented by unsecured RPC access and associated services.

```
01/06/01 05:04:21.793408 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.829933 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.830004 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.888825 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.888876 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.919235 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:45.761356 External RPC call 206.210.80.6 3832 MY.NET.15.127 111
01/06/01 05:08:19.304357 External RPC call 206.210.80.6 1751 MY.NET.100.130 111
01/06/01 06:39:35.583605 STATDX UDP attack 206.210.80.6 1074 MY.NET.6.15 32776
```

[32] http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_2.__RPC; Dale Ross

[33] http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RPC

Correlations

Correlations in both the scan and OOS files were identified that are related to the port 111 alert records. They are listed below:

From the OOS files

```
01/11-20:02:28.312092 MY.NET.217.158:111 -> 193.253.209.167:2340
```

From the scan files

```
Dec 20 15:05:33 148.228.125.215:1843 -> MY.NET.133.104:111 SYN
**S*****
Dec 20 15:05:33 148.228.125.215:1850 -> MY.NET.133.111:111 SYN
**S*****
Dec 20 15:05:33 148.228.125.215:1884 -> MY.NET.133.141:111 SYN
**S*****
Dec 29 19:44:58 63.11.25.117:1661 -> MY.NET.6.15:111 SYN **S*****
Dec 29 19:44:59 63.11.25.117:2 -> MY.NET.6.15:111 FIN ***F****
Dec 29 19:44:59 63.11.25.117:5 -> MY.NET.6.15:111 VECNA *****P**
Dec 21 08:42:35 MY.NET.1.5:53 -> 192.48.96.19:32771 UDP
Dec 21 08:42:35 MY.NET.1.5:53 -> 192.48.96.19:32771 UDP
Dec 21 08:42:35 MY.NET.1.5:53 -> 192.48.96.19:32771 UDP
Jan  3 15:19:03 MY.NET.70.163:36356 -> 24.3.45.174:32771 SYN **S*****
```

Correlations in the scan files were identified that are related to the port 32771 alert records. Issuing the command `grep ":32771 " oosall.txt` was unable to locate any additional information in the OOS files. Information identified is listed below:

Additional information about port 32771 traffic was identified to host MY.NET.202.94. This interaction was not captured in the alert records.

```
Dec 30 21:12:18 216.99.200.242:24713 -> MY.NET.202.94:32771 SYN **S*****
Dec 30 21:12:21 216.99.200.242:24713 -> MY.NET.202.94:32771 SYN **S*****
Dec 30 21:37:38 216.99.200.242:24618 -> MY.NET.202.94:32771 SYN **S*****
Dec 30 21:37:41 216.99.200.242:24618 -> MY.NET.202.94:32771 SYN **S*****
Dec 30 21:37:51 216.99.200.242:26684 -> MY.NET.202.94:32771 SYN **S*****
Dec 30 21:37:57 216.99.200.242:26684 -> MY.NET.202.94:32771 SYN **S*****
```

RPCs have been an issue in prior reviews of the companies' security. Important instances are identified below:

http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc

Additional important information related to RPC services is indicated below:

http://www.sans.org/y2k/trouble_RPCs.htm - The trouble with RPCs - Stephen Northcutt

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0189 - Solaris rpcbind listens on a high numbered UDP port, which may not be filtered since the standard port number is 111. Additional correlations for RPC[34]:

CVE-1999-0228	CVE-1999-0003	CVE-1999-0974	CVE-1999-0320
CVE-1999-0687	CVE-1999-0212	CVE-1999-0008	CVE-1999-0969
CVE-1999-0900	CVE-1999-0208	CVE-1999-0353	

Defensive recommendation

The companies' hosts identified in Table 13 and Figure 9 should re review for possible compromise due to the many exploits related to the RPC services. Like with the SMB access, precautions should be taken to block the external access to RPC services at the network border. Special security precautions should be utilized in any case where such services must be available from outside.

TCP SMTP Source Port traffic

Probability the source address was spoofed

Mail delivery requires a valid IP address.

Description of attack

This alert appears to be triggered by external mail traffic originating from port25. It is not in the current SNORT rule set. The current rule set looks for outgoing traffic on port 25 and interprets it as an indication of mail relay.

A sample of the SMTP source port 25 traffic was extracted us issuing the command `grep "SMTP" SnortAall.txt`. The results are displayed below:

```
12/12-07:23:36.587711  [**] TCP SMTP Source Port traffic [**]
213.74.161.214:25 -> MY.NET.5.27:1002
01/03-16:35:10.148560  [**] TCP SMTP Source Port traffic [**]
165.112.79.25:25 -> MY.NET.253.42:25
01/03-16:35:10.627013  [**] TCP SMTP Source Port traffic [**]
165.112.79.25:25 -> MY.NET.253.42:25
01/03-16:35:13.611045  [**] TCP SMTP Source Port traffic [**]
165.112.79.25:25 -> MY.NET.253.42:25
01/03-16:35:13.663130  [**] TCP SMTP Source Port traffic [**]
165.112.79.25:25 -> MY.NET.253.42:25
```

Two hosts generated 95 % of all the traffic triggering this alert. They are displayed in Table 15.

[34] http://www.sans.org/y2k/CVE.htm

Table 15 - Primary SMTP Source port traffic Hosts

Source Host	Alerts	Resolved Name
63.11.25.117	84	1Cust117.tnt1.yakima.wa.da.uu.net
165.112.79.25	11	vismed.nida.nih.gov

Attack mechanism

The SMTP transmission channel is a TCP connection established between the sender process port and the receiver process port. This single full duplex connection is used as the transmission channel. This protocol is assigned the service port 25[35].This could be possible mail relay traffic, or attempts to channel mail traffic through the companies' mail servers for some reason. This could possibly be legitimate traffic based on the name resolution. But, in sufficient data has been supplied to determine the validity of this traffic.

Correlations

http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Markus_DeShon.html

Defensive recommendation

Unless there is a specific purpose for providing access to the companies' mail servers from outside sources, traffic to the mail servers should be blocked at the boarder router. If there are legitimate users that need this access, rules can be created to allow only this specific traffic.

Back Orifice

Probability the source address was spoofed

The IP addresses were not likely to be spoofed. These appear to be attempts to connect to a Back Orifice server.

Description of attack

Back Orifice is a remote control utility with extensive capabilities. It operates on Windows systems. Back Orifice operates as a client/server. The server is run on the victim system. It can be easily installed via email attachments or newsgroup downloads.

A sample of the Back Orifice alerts is displayed below:

```
12/09-22:25:08.039128  [**] Back Orifice [**] 209.94.199.202:31338 -
> MY.NET.60.36:31337
```

[35] http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc0821.html

```
12/09-22:25:08.379764  [**] Back Orifice [**] 209.94.199.202:31338 -
> MY.NET.60.152:31337
12/09-22:25:08.829984  [**] Back Orifice [**] 209.94.199.202:31338 -
> MY.NET.60.185:31337
12/09-22:25:09.119468  [**] Back Orifice [**] 209.94.199.202:31338 -
> MY.NET.60.212:31337
12/09-22:25:09.130663  [**] Back Orifice [**] 209.94.199.202:31338 -
> MY.NET.60.216:31337
```

Of all of the Back Orifice alerts, 85.7% of the alerts were generated from three hosts. The targeting hosts are identified in Table 16.

Table 16 - Back Orifice Alert Targeting Hosts

Source Host IP	Alerts	Domain Name
209.94.199.202	32	cuscon1096.tstt.net.tt
62.136.71.93	20	modem-93.lawrencium.dialup.pol.co.uk
209.94.199.143	14	cuscon1037.tstt.net.tt

Evidence of Active Targeting

The hostile hosts are not targeting a specific host. They are searching for a Back Orifice server.

Attack mechanism

Back Orifice is small self-installing remote control utility. Executing the server on any windows machine installs the server. The executable is placed into the system where it will not interfere with other running applications. Back Orifice can also be attached to any windows executable that will run normally after installing the server. It does not show up in the task list. Back Orifice is loaded when the computer starts. The filename that it runs as is configurable.[36]

Back Orifice typically listens on port 31337 TCP/UDP with the server running on port 31338. The new version Back Orifice 2000 can be expected on ports 8787,54320, and 54321.[37]

Correlations

There were no records located in the OOS files that were related to the Back Orifice alerts. However, many related recorded were located in the scan files. A sample is included below.

```
Dec 29 19:45:46 63.11.25.117:2009 -> MY.NET.140.188:31337 SYN
**S*****
Dec 29 19:45:52 63.11.25.117:2042 -> MY.NET.140.137:31337 SYN
**S*****
Dec 29 19:45:55 63.11.25.117:2062 -> MY.NET.140.104:31337 SYN
**S*****
```

[36] http://www.bo2k.com/indexwhatis.html

[37] http://www.sans.org/newlook/resources/IDFAQ/oddports.htm

```
Dec 29 19:46:00 63.11.25.117:2083 -> MY.NET.140.248:31337 SYN
**S*****
Dec 29 19:46:10 63.11.25.117:2124 -> MY.NET.140.113:31337 SYN
**S*****
Dec 29 19:46:19 63.11.25.117:2147 -> MY.NET.140.92:31337 SYN
**S*****
Dec 29 19:46:25 63.11.25.117:2172 -> MY.NET.140.220:31337 SYN
**S*****
Jan  1 00:40:52 147.208.171.139:3747 -> MY.NET.98.131:31337 SYN
**S*****
```

There is no data to indicate that the Back Orifice alerts were anything other than attempts to connect to a Back Orifice server. The OOS files contained no data related to this alert. The scan files showed additional attempts to connect to Back Orifice servers. On e critical item of data was uncovered while searching the scan files. Records were discovered that showed MY.NET.70.163 attempting connections on port 31337. This indicates either a company employee using Back Orifice, or the system is compromised and being used to attempt Back Orifice connections.

Previous evaluations of the companies' security have shown Back Orifice connection attempts. They are available here:

http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Bill_Royds.zip
http://www.sans.org/y2k/practical/Robert_Currie.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Marc_Bayerkohler_GCIA.html#Trace_4__Back_Orifice_Scan
http://www.sans.org/y2k/021800.htm

There is additional information related to Back Orifice available at these locations:

http://www.cert.org/vul_notes/VN-98.07.backorifice.html - CERT Vulnerability Note VN-98.07
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0660
http://www.sans.org/infosecFAQ/malicious/back_orifice.htm

Defensive recommendation

The host MY.NET.70.163 should be investigated immediately and the issue of its port 31337 resolved. The other company hosts with Back Orifice connection attempts should be reviewed for the presence of Back Orifice.

SITE EXEC - Possible wu-ftpd exploit - GIAC000623

Probability the source address was spoofed

The three hosts attempting the wu-ftpd exploit are valid.

Description of attack

This attack is an exploit that if successful allows root access to the system. The alert record is listed here:

```
11/26-17:30:50.939661  [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 24.23.255.246:4507 -> MY.NET.130.98:21
12/16-12:21:46.219962  [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 209.162.94.11:4584 -> MY.NET.156.127:21
12/21-15:26:29.595664  [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 64.217.116.106:1684 -> MY.NET.97.162:21
```

The primary source hosts and target hosts are identified in Table 17.

Table 17 - wu-ftpd exploit Source & Target Hosts

Source Host	Resolved Name / Reg. Owner	Target Host
209.162.94.11	Verio, Inc.	MY.NET.156.127
24.23.255.246	cm47580-a.ftwrth1.tx.home.com	MY.NET.130.98
64.217.116.106	adsl-64-217-116-106.dsl.hstntx.swbell.net	MY.NET.97.162

Attack mechanism

wu-ftp uses the C *strcpy()* function to copy a string from one variable to another. It is vulnerable to a buffer overflow because it fails to perform any input bound checking [38].

The Ramen Worm also has the ability to target the wu-ftpd service vulnerability[23].

Correlations

Information was located in the OOS files that are related to the alert records. A sample is included below:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/13-02:55:21.107292 200.194.102.99:21 -> MY.NET.1.7:21
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x39C33F6B   Ack: 0x5D02211   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/13-02:55:21.323445 200.194.102.99:21 -> MY.NET.1.18:21
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x39C33F6B   Ack: 0x5D02211   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/13-02:55:21.441921 200.194.102.99:21 -> MY.NET.1.24:21
TCP TTL:24 TOS:0x0 ID:39426
**SF**** Seq: 0x39C33F6B   Ack: 0x5D02211   Win: 0x404
00 00 00 00 00 00                                ......
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/13-02:55:23.842127 200.194.102.99:21 -> MY.NET.1.144:21
TCP TTL:24 TOS:0x0 ID:39426
```

[38] http://www.sans.org/y2k/practical/Herschel_Gelman.html#breakdown

```
**SF**** Seq: 0x1579A075   Ack: 0x2F88AF6F   Win: 0x404
00 00 00 00 00 00
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

There were also records located in the scan files that are related to the alert files.

http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Herschel_Gelman.html#breakdown

Happy 99 Virus

Probability the source address was spoofed

The IP address was not spoofed. A valid IP address is required to transport the Happy.99 worm file through the mail server to the victim's desktop.

Description of attack

The Happy99.exe, while sometimes referred to as a virus, is a computer worm that works on Windows systems. This computer worm currently does not erase or alter files. The worm can cause network slowdowns and crash e-mail servers.

When executed, sometimes automatically depending on the system configuration, the worm opens a window titled "Happy New Year 1999 !!" and provides a fireworks display. This is intended to distract the user while the worm continues its installation. The worm sends itself to other users when the infected computer is online.

```
12/22-20:25:10.840208  [**] Happy 99 Virus [**] 63.216.198.158:2239
-> MY.NET.6.47:25
```

Attack mechanism

The Happy99.Worm can be received as an email attachment or retrieved newsgroup postings. The file is usually named Happy99.exe. The Happy99.exe file is attached as a separate email sent in conjunction with an outgoing email or newsgroup posting. Generally, it is added without the user's knowledge.

In addition, the worm does the following:[39]

- Copies itself as Ska.exe
- Extracts Ska.dll to C:\Windows\System
- Modifies the Wsock32.dll file in C:\Windows\System by copying the existing Wsock32.dll to Wsock32.ska

Correlations

http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_6.__Happy
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Robert_Currie.doc

[39] http://service1.symantec.com/sarc/sarc.nsf/html/Happy99.Worm.html Happy99.Worm

http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm

Defensive recommendation

The system MY.NET.6.47 should be checked for the presence of the Happy99.exe worm. Anti-virus detection should be deployed to prevent this worms penetration if not deployed already. There are less instances of this worm than in prior reviews of the companies' security.

STATDX UDP attack

Probability the source address was spoofed

The exploit of this vulnerability requires a valid IP address.

Description of attack

The statdx UDP attack exploits remote root vulnerability in the RPC based statd daemon. statd implements the Network Status Monitor RPC protocol to provide reboot notification for other services.[40]

206.210.80.6 (registered to Stargate Industries Pittsburgh, PA) targeting MY.NET.6.15

```
01/06/01 05:04:21.793408 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.829933 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:21.919235 External RPC call 206.210.80.6 1414 MY.NET.6.15 111
01/06/01 05:04:45.761356 External RPC call 206.210.80.6 3832 MY.NET.15.127 111
01/06/01 05:08:19.304357 External RPC call 206.210.80.6 1751 MY.NET.100.130 111
01/06/01 06:39:35.583605 STATDX UDP attack 206.210.80.6 1074 MY.NET.6.15 32776
01/06/01 06:39:35.583605 STATDX UDP attack 206.210.80.6 1074 MY.NET.6.15 32776
```

Attack mechanism

The exploit code is available at:
http://www.securiteam.com/exploits/A_new_advanced_exploit_code_for_the_string_formating_vulnerability_in_StatD.html

http://members.cotse.com/mailing-lists/bugtraq/2000/Oct/0156.html

http://security-archive.merton.ox.ac.uk/bugtraq-200008/0065.html

http://security-archive.merton.ox.ac.uk/archive-200008/0082.html

The Ramen Worm has the ability to target the statd service vulnerability[23].

Correlations

http://www.sans.org/y2k/practical/George_Bakos.html#exploit

---

40 http://www.securiteam.com/exploits/A_new_advanced_exploit_code_for_the_string_formating_vulnerability_in_StatD.html

http://www.sans.org/y2k/022801-1100.htm Report Date: February 28, 2001 - 1100
http://www.sans.org/y2k/120600-1200.htm Report Date: December 6, 2000 – 1200
http://www.sans.org/y2k/013101-1000.htm Report Date: January 31, 2001 – 1000
http://www.sans.org/y2k/021301.htm Report Date: February 13, 2001 – 0900

Defensive recommendation

Systems should be patched to eliminate this vulnerability. Consider blocking such traffic at the network border.

Scan Analysis

Scan Analysis Summary

There was much scanning activity detected on the customer network. There were a total of 91691 scan events recorded in the dataset. Of these scan events, 60846 were from an IP address external to MY.NET while 30845 originated with a MY.NET IP address. The very large number of internal source IP scans events indicated serious security issues exist on the companies' network. An overall summary of the scan activity is presented in Table 18. The primary scanning hosts are identified in Figure 10 while the top destination hosts are shown in Figure 11. Figure 12 presents the data for the top three scanned ports over the period of the monitoring. Data for the balance of the significant port scans is presented in Figure 13.

Table 18 - Scan Summary

Scan Type	Total	External Source	Internal External
Total	91691	60846	30845
SYN-FIN scan!	51192	51192	0
spp_portscan	38243	7660	30583
Null scan!	826	826	0
Queso fingerprint	710	710	0
NMAP TCP ping!	558	296	262
Broadcast Ping to subnet 70	154	154	0
Probable NMAP fingerprint attempt	8	8	0

Figure 10 - Top Scanning Source IP Addresses

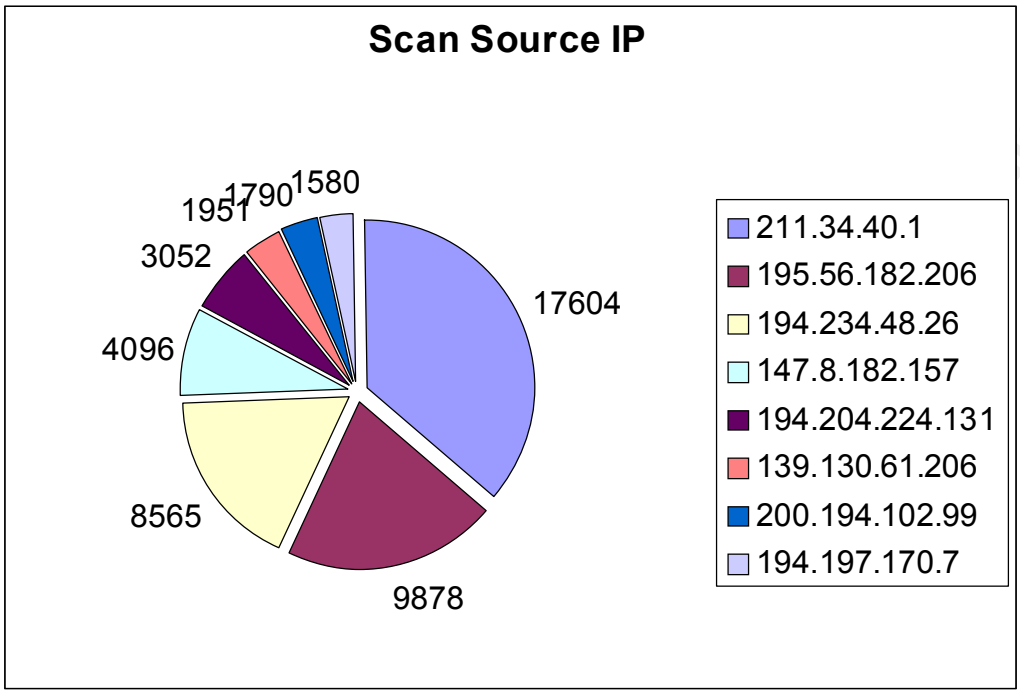


Figure 11 - Top Scan Destination Addresses

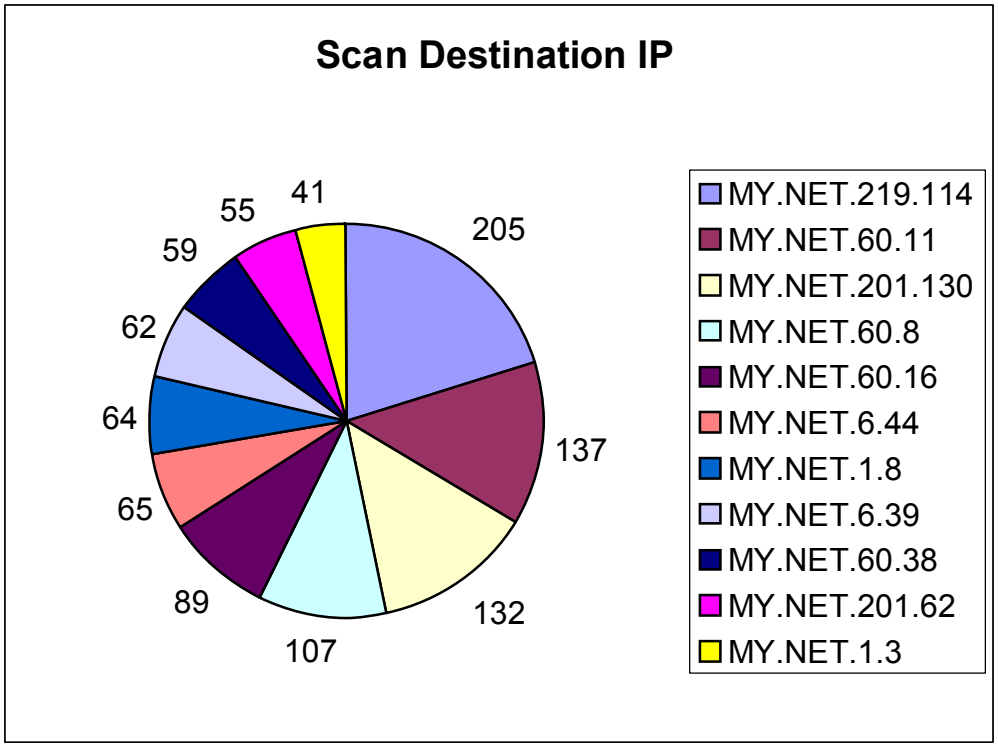


Figure 12 - Top Three scanned Ports vs. Date

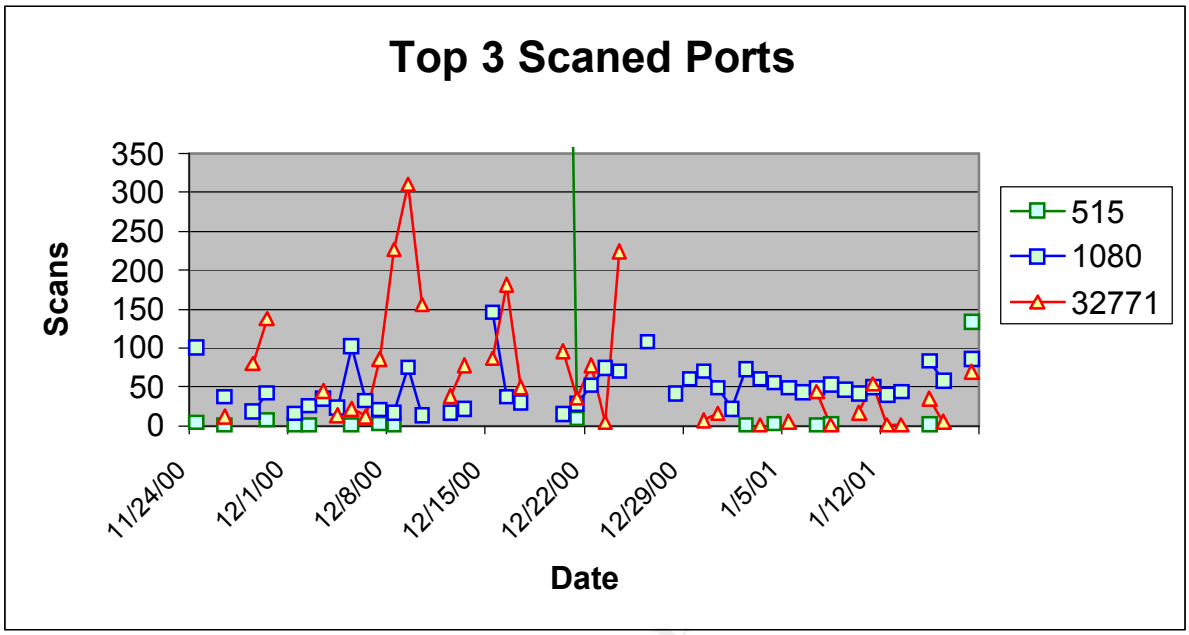
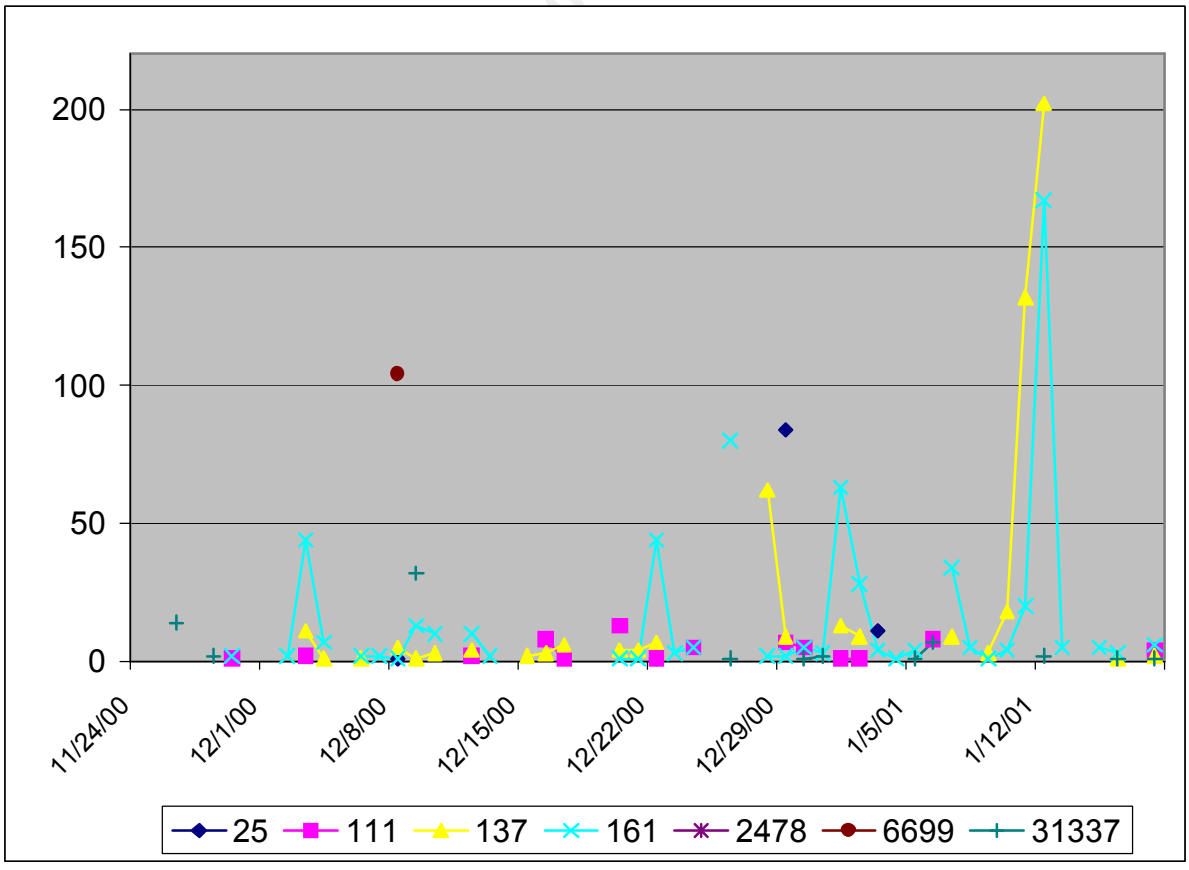


Figure 13 - Primary Ports Scanned vs. Date



Scan Analysis Details

In addition to the scans identified in the alerts, the scan files show indications of scans for the Raman worm, or Bad Blood, or SubSeven. These scans were generated from the hosts identified in Table 19. One of these hosts was a company host, MY.NET.98.238. The following was used to extract the records indication the scans in question:

```
SELECT *;
 FROM scan1fix;
 WHERE Scan1fix.d_port = "27374";
 ORDER BY Scan1fix.source
```

Additional scans were identified in the OOS files such as Xmas tree scans. The OOS files also contained a significant amount of traffic from MY.NET hosts that included abnormal flag settings. Many of there are likely scans of other hosts.

Table 19 - Significant Scanning Hosts From Scan Files

24.10.184.121	**MY.NET.98.238**
24.160.198.104	130.67.37.2
24.183.250.2	130.67.37.67
24.202.238.63	131.161.49.140
24.226.126.93	216.99.200.242
24.26.94.142	

The following excerpt is a near identical match to at Possible Ramen Worm Traces from GIAC.[41]

```
Date       Time     Source    S_port Dest        D_port Type  Flags
Jan-3-2001 11:20:20 130.67.37.2 1807 MY.NET.200.5 27374 SYN **S*****
Jan-3-2001 11:20:20 130.67.37.2 1808 MY.NET.200.6 27374 SYN **S*****
Jan-3-2001 11:20:20 130.67.37.2 1809 MY.NET.200.7 27374 SYN **S*****
Jan-3-2001 11:20:20 130.67.37.2 1810 MY.NET.200.8 27374 SYN **S*****
```

97.5% of the scanning activity was generated by the SYN-FIN scan (55.8%) and the spp_portscan (41.7%).

SYN-FIN scan

SYN-FIN scans are executed utilizing the most invalid packets that can exist. “They go against every rule applied to TCP/IP.”[42] A SIN-FIN packet starts the establishment while concurrently breaking that connection. This scan, and its related FIN, are infrequent use. There are two apparent reasons for their popularity. First, they have some ability to sneak through network protections. This ability is not as successful as in the past, but still

[41] http://www.sans.org/infosecFAQ/malicious/ramen.htm

[42] Intrusion Signatures and Analysis; Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick – pg. 345

reasonably effective in many cases. Second, Because FIN terminates a connection; it is not always logged or monitored. This activity constitutes the majority of the scanning activity, 55.8%.

Correlations

http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Markus_DeShon.html
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc

spp_portscan

A netcat scan of systems is used to identify open ports. This is generally recon prior to a future attack. Netcat can also be used to identify an available service susceptible to attack. Netcat is not as versatile as NMAP, however is very effective at identifying system vulnerabilities[43]. IT also has the capability to sneak through NAT (at least on some unpredictable basis). spp_portscan is the first runner up with 41.7% of the scanning activity.

There were 643 MY.NET hosts identified that were actively scanning other hosts. This indicates a significant security issue. These systems are either compromised, or at the hands of malicious users. There should not be that many systems conducting scans on such a wide basis. Not all hosts could be identified, but the most significant MY.NET scanning hosts are identified in Table 20. Also identified, are the top external scanning hosts. Internal hosts generated 80% of the scans!

Table 20 - Most significant MY.NET scanning Hosts

My.NET Host	Alerts	External Host	Alerts
MY.NET.217.150	6290	212.64.74.169	336
MY.NET.217.158	4935	24.7.86.215	302
MY.NET.100.230	3008	24.113.198.51	271
MY.NET.219.126	2202	216.99.200.242	270
MY.NET.253.24	2001	24.3.0.36	195
MY.NET.217.126	1491	152.163.206.134	133
MY.NET.217.182	1327	63.78.39.192	126

Correlations

http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc

[43] Intrusion Signatures and Analysis; Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick – pg. 173

Queso Fingerprint

The Queso fingerprint is used to identify the operating system of the target system. Knowing the operating system allows the attacker to determine which vulnerabilities may exist on the target system. Scan alerts shoed 710 Queso fingerprint scans of the companies' systems. Nearly 30% of these scans are between the hosts 206.65.191.129 and MY.NET.219.114. There were also a few other instances of paired scanning, but not nearly as significant as that between hosts 206.65.191.129 and MY.NET.219.114. With the exception of the operating system identification these are reasonably benign. The Queso fingerprint activity on the network was rather limited constituting approximately 1% of the scanning activity.

Correlations

http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Robert_Currie.doc

NULL scans

Null scans generate TCP packet that have no flag bits set. It is used to map out network topology. Null scans are generally precursory reconnaissance scans. They, like other recon scans, are typically followed by more directed scans and or exploits. The NULL scan activity on the network was also limited constituting approximately 1% of the scanning activity.

Correlations

http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc

NMAP scans

NMAP is designed for scanning large networks to determine hosts that are available and the services running. It is probably the most sophisticated of all of the scanning tools. NMAP supports a large number of scanning techniques[44]:

- UDP
- TCP connect()
- TCP SYN (half open)
- ICMP (ping sweep)
- FIN, ACK sweep
- Xmas Tree
- SYN sweep

[44] http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_3.__Queso

- Null scan
- And others.

In addition to the NMAP specific scans, the NULL scans may have been conducted with NMAP. NMAP could make account for up to 1.7% of the scanning activity.

Correlations

http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
http://www.sans.org/y2k/practical/Guy_Bruneau.doc
http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
http://www.sans.org/y2k/practical/Robert_Currie.doc
http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc

Figure 14 - Top Two Scan Alerts

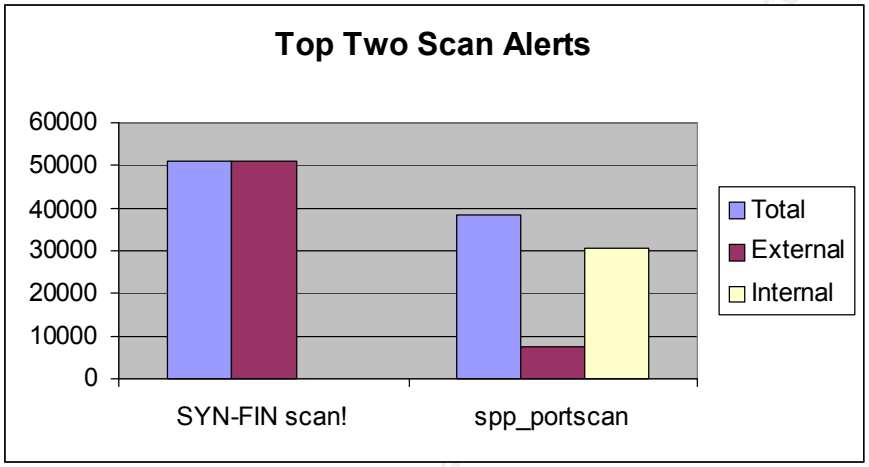
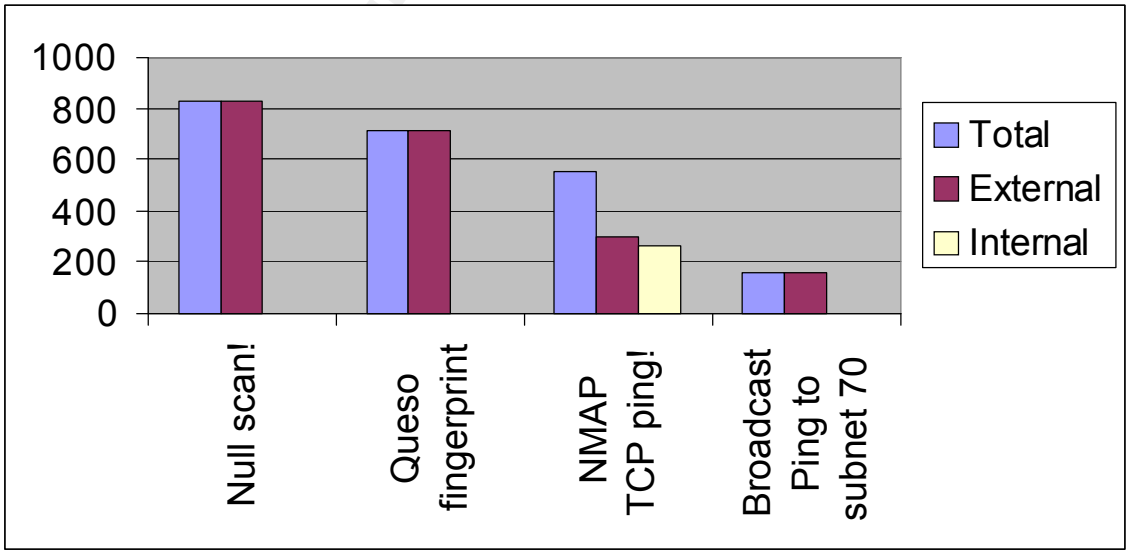


Figure 15 - Other Scans



Defensive recommendation

Measures are described in the general security improvement recommendation that should address most of the issues related to system scanning.

Watched Alert Analysis

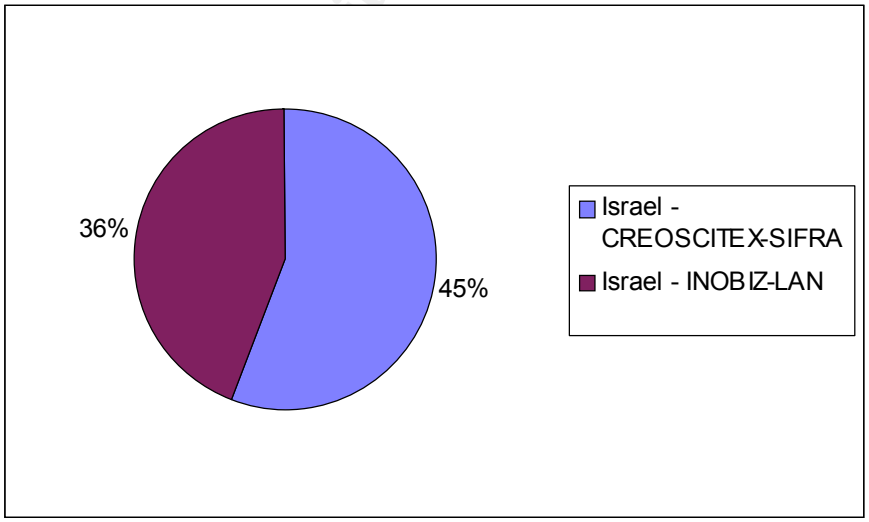
There were a significant number of alerts generated by the Watchlist 000222 NET-NCFC and Watchlist 000220 IL-ISDNNET-990517 SNORT alert rules. No specific details were provided as to the details. As evaluated in earlier reviews of the companies' security, these appear to be custom rules to watch traffic from Israel and the Computer Network Center Chinese Academy[45].

While there are 32 hosts that created alerts from the Computer Network Center Chinese Academy, they generated 2% of the alert traffic (2400 alerts) with the balance, 98%, coming from Israel (105876 alerts). Two source hosts generated 81% of the alerts. Details are shown in Table 21 and Figure 16.

Table 21 - Primary Watchlist Alerts From Israel

IP Owner	% Of Total	Alerts
Israel - Bezeq International	4%	4641
Israel - Cable-Modem-Experiment	4%	4563
Israel - CREOSCITEX-SIFRA	45%	48785
Israel - INOBIZ-LAN	36%	39015
Sub-Total	89%	97004

Figure 16 - Primary Watchlist Hosts



[45] http://www.sans.org/y2k/practical/Herschel_Gelman.html#3

Table 22 - Watchlist Summary For Primary Sources

Israel - CREOSCITEX-SIFRA	
Alerts From Host 212.179.79.2	Alerts
MY.NET.220.126	6699
MY.NET.212.38	4336
MY.NET.229.114	4876
MY.NET.225.234	4967
Israel - INOBIZ-LAN	
Alerts From Host 212.179.27.111	Alerts
MY.NET.201.222	6688
MY.NET.217.138	41038

Correlations

http://www.sans.org/y2k/practical/JoanneTreurniet.html#asst3
http://www.sans.org/y2k/practical/Herschel_Gelman.html#3
http://www.sans.org/y2k/033000-2300.htm
http://www.sans.org/y2k/032500-2200.htm
http://www.sans.org/y2k/032700-2000.htm
http://www.sans.org/y2k/032200-1700.htm
http://www.sans.org/y2k/052000.htm
http://www.sans.org/y2k/051900.htm
http://www.sans.org/y2k/043000.htm

Defensive recommendation

If there is no real purpose for traffic from the watchlisted hosts, they should be clocked at the network border. As they have been placed on a special monitoring list this should be seriously considered.

Security Improvement Recommendations

The vendor uncovered many significant network security issues on the companies' network. The vendor recommends that the company implement network security improvement actions without delay! Some consideration should be given to restricting network connectivity until some of the security measures identified herein are implemented. A layered security approach must be implemented immediately to secure the companies' network. Simply installing a firewall at the network "front door" will not secure the companies' resources. For additional information see:

http://www.sans.org
http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm

Network Intrusion Detection; An Analyst's Handbook; Stephen Northcutt, Judy Novak
The Practical Intrusion Detection Handbook; Paul E. Proctor

A layered approach such as listed below is required to secure the companies' network resources.

1. Improve router security (router filtering & ACLs).
2. Install a firewall and the network border with appropriate filtering.
3. Scan the network for compromised and vulnerable systems.
4. Implement scheduled system vulnerability scanning.
5. Implement host system security measures (IDS and firewalls).
6. Implement auditing and monitoring measures.
7. Deploy network based Intrusion Detection Systems (IDS).
8. Implement appropriate measures from http://www.sans.org/topten.htm.
9. Develop an Incident Response Plan. (Include attacking the attacker).
10. Develop a Security Policy for the company.

Why should the company go through all of the effort? Others best say some things. Here is the opinion of an independent third party:

> *"Using multiple layers in a security model is the most effective method of deterring unauthorized use of computer systems and network services. Every layer provides some protection from intrusion, and the defeat of one layer may not lead to the compromise your whole organization."*[46]

Each of the defensive recommendation identified throughout this review should be addressed and implemented as appropriate. Significant improvements can be made to system security by addressing the issues identified in the SANS Top Ten List. See http://www.sans.org/topten.htm for details. With all of the DNS scanning activity the company should verify that its DNS servers are secure and protected appropriately. The list of identifiable DNS servers is listed in Table 23.

Table 23 - Companies DNS Servers

MY.NET.1.3
MY.NET.1.4
MY.NET.1.5

Prior to procurement and installation of a border firewall router configuration can be enhanced to add significant security improvements. Once again, consideration should be given to restricting network connectivity until these corrections are implemented. Router ACLs at the border router should specifically deny:

- Deny traffic inbound from local network addresses and other invalid (and spoofed) addresses.

[46] http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm; Peter Watson

- Deny inbound traffic for low ports 666, 1024, 1080, 1243, 1524, 2023,2565, 6667, 6711, 8080, 9989, 13000, 12345, 12346, 16969, 27374, 31337and other active Trojan ports.
- Deny improperly "flagged" TCP/IP traffic.
- Deny inbound traffic for low ports unless required
- Deny Napster and Guntilla traffic if determined to be appropriate.
- Drop connections after a reasonable timeout period.

As mentioned earlier, some plan needs developed post hast to deal with the large number of hosts that are, or are likely to be, compromised. A list of host that are all but certain to be compromised is provided in Table 24. These hosts should be appraised and corrected immediately. The lists of MY.NET host scanning other systems is significant - 644 systems. At this time, these hosts should be considered hostile. A vulnerability scanner such as Nessus (http://www.nessus.org/) or ISS Internet Scanner (http://documents.iss.net/literature/InternetScanner/is_ps.pdf) should be run against the network. Information from this scan should be used to develop a schedule to correct vulnerabilities and remove compromised systems from the network.

Table 24- MY.NET Compromised Hosts

MY.NET.1.8	MY.NET.205.138	MY.NET.98.199	MY.NET.6.15	MY.NET.98.156
MY.NET.1.10	MY.NET.163.17	MY.NET.99.51	MY.NET.100.130	MY.NET.97.234
MY.NET.217.162	MY.NET.98.238	MY.NET.213.158	MY.NET.15.127	MY.NET.98.126
			MY.NET.202.94	

While listed at the bottom of the list as action items, the development and implementation of both a security policy and Incident Response Plan should commence concurrently with the implementation of the other security measures.

References:

Network Intrusion Detection; An Analyst's Handbook; Stephen Northcutt, Judy Novak

Intrusion Signatures and Analysis; Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick

The Practical Intrusion Detection Handbook; Paul E. Proctor

TCP/IP for Intrusion Detection and Firewalls, The SANS Institute

Port 137 Scan Bryce Alexander; May 10, 2000; http://www.sans.org/newlook/resources/IDFAQ/port_137.htm;

CERT® Incident Note IN-2000-02 http://www.cert.org/incident_notes/IN-2000-02.html

Follow-up on a Honeypot Catch**;** http://www.sans.org/y2k/honeypot_catch.htm

An Analysis of the Snort Network Intrusion Detection System by Mark D. Tollison http://www.sans.org/infosecFAQ/intrusion/snort2.htm

http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm

The Need for Multi-layered Defenses on the Personal PC http://www.sans.org/infosecFAQ/homeoffice/defenses.htm

Connecting Your Home LAN to the Internet – Securely Andrew S. Baker March 27, 2001 http://www.sans.org/infosecFAQ/homeoffice/home_LAN.htm

Cable/DSL Router and Personal Firewall: Belt and Suspenders? Mike McCabe February 14, 2001 http://www.sans.org/infosecFAQ/homeoffice/cable.htm

How Complicated Is Home Protection? Dale Hillman November 23, 2000 http://www.sans.org/infosecFAQ/homeoffice/protection.htm

A Hardware Based Firewall Option for the SOHO (Small Office/Home Office) User. A look into the LINKSYS Etherfast Cable/DSL Router. Scott Kisser December 4, 2000 http://www.sans.org/infosecFAQ/homeoffice/option.htm

http://www.sans.org

http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm

The Need for Multi-layered Defenses on the Personal PC http://www.sans.org/infosecFAQ/homeoffice/defenses.htm

Guy Bruneau http://www.sans.org/y2k/practical/Guy_Bruneau.doc
Mike Bell http://www.sans.org/y2k/practical/Mike_Bell_GCIA.doc
George Bakos http://www.sans.org/y2k/practical/George_Bakos.html#exploit
Joanne Treurniet http://www.sans.org/y2k/practical/JoanneTreurniet.html#asst3
Herschel Gelman http://www.sans.org/y2k/practical/Herschel_Gelman.html#3
Joe Matusiewicz http://www.sans.org/y2k/practical/Joe_Matusiewicz_GCIA.doc
Robert Currie http://www.sans.org/y2k/practical/Robert_Currie.doc
Markus DeShon http://www.sans.org/y2k/practical/Markus_DeShon.html

Andy Siske http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm
Crist Clark http://www.sans.org/y2k/practical/Crist_Clark_GCIA.html
Dale Ross http://www.sans.org/y2k/practical/Dale_Ross_GCIA.htm#_5.__Tiny
Eric Hacker http://www.sans.org/y2k/practical/Eric_Hacker.html#_Toc490920406
David Thibault
http://www.sans.org/y2k/practical/David_Thibault_GCIA.html#ANALYZE_THIS
John Best http://www.sans.org/y2k/practical/John_Best.htm#assign3
Teri Bidwell http://www.sans.org/y2k/practical/Teri_Bidwell_GCIA.doc