Global Information Assurance Certification Paper

Faud Khan

GCIA Practical

February 19, 2001

Assignment 1 – Network Traces

Network Trace 1

Time	Src IP	Src Port	Dst IP	Dst Port
11:55:55	192.116.240.24	1306	my.net.com.10	21
11:55:55	192.116.240.24	1312	my.net.com.16	21
11:55:55	192.116.240.24	1313	my.net.com.17	21
11:55:55	192.116.240.24	1314	my.net.com.18	21
11:55:55	192.116.240.24	1315	my.net.com.19	21
11:55:55	192.116.240.24	1316	my.net.com.20	21
11:55:55	192.116.240.24	1317	mynet.com.21	21
11:55:55	192.116.240.24	1318	mynet.com.22	21
11:55:55	192.116.240.24	1319	mynet.com.23	21
11:55:55	192.116.240.24	1320	mynet.com.24	21
11:55:55	192.116.240.24	1321	mynet.com.25	21
11:55:55	192.116.240.24	1322	mynet.com.26	21
11:55:55	192.116.240.24	1323	mynet.com.27	21
11:55:55	192.116.240.24	1324	mynet.com.28	21
11:55:55	192.116.240.24	1325	mynet.com.29	21
11:55:55	192.116.240.24	1326	mynet.com.30	21

1. Source of Trace:
This trace was taken from a log file from one of our Internet firewalls during November 2000. As these logs are generated from a CheckPoint firewall, they give us just enough detail to identify suspicious traffic. For this scan, I have included the following fields only: time, source IP, source port, destination IP, and destination port.

2. Detect was Generated By:
This detect was generated by exporting the firewall logs using the fw logexport command to create a colon delimited file which is then imported to Excel. For these files I have concentrated on the all rejected and dropped entries.

3. Probability the Source Address was Spoofed:
This scan indicates that the information sought requires a response. That being the case, I doubt the address was spoofed.

4. Description of the attack:
This trace illustrates an individual who scanned our entire Internet address range in search of a ftp server.

5. Attack mechanism:
In this case, our entire Internet address range was scanned, which indicates that a tool or script was used. This type of scan could have been accomplished by nmap.

6. Correlations:

This type of scan is common and doesn't pose a direct threat other than to perform reconnaissance on our site. If the attacker had determined our brand of firewall, in a previous scan, he/she would systematically try to determine weaknesses during subsequent scans.

By using http://whois.arin.net/whois/index.html, I discovered that the address was listed on RIPE NCC http://www.ripe.net/index.html. Next, I was able to determine that this address belonged to an organization called Z.A.G. Industries LTD, based out of Israel. From their web site, they seem to carry a line of storage solutions for home and business.

Worried that this site could be compromised, I have consistently monitored for this address' reappearance but not other attempts have been made.

The attacker could have been searching for an ftp server in the hopes to exploit CVE-2000-0813, (See Appendix A) a known vulnerability related to the ftp service in CheckPoint firewalls.

7. Evidence of active targeting:
There is clear evidence of active targeting since the target was our entire address range. If the target had been sporadic address ranges, I may have concluded otherwise.

8. Severity:
The severity of this attack is: -5

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

(0 + 4) – (5 + 4) = -5

Criticality = 0 This server is not critical to our business
Lethality = 4 This is a reconnaissance scan
System Countermeasure = 5 We do not have an ftp server
Network Countermeasure = 4 The firewall does not allow ftp access as we do not have an ftp server.

9. Defensive recommendations:
Configure the ftp server to not allow anonymous access. ID's would be created for a single usage only, as required. At most, an ID would expire within 24 hours of creation. Basically, it would allow enough time for a user to connect, upload or download the file(s), and logoff. If the ID and password were sniffed, they would only be valid for that day which significantly reduces the window of opportunity to attack our network resources.

If you are using a CheckPoint VPN1/Firewall-1 then ensure that PASV FTP is only enabled if necessary. Configure the FTP Security Server to handle the PASC FTP connections if you require FTP service. Ensure all the operation system is patched especially if you are using stateful inspection of passive FTP.

10. Multiple choice test question:
What is PASV mode ftp?

a. The server opens a TCP connection back to the client in order to transfer data
b. The server opens a UPD connection back to the client in order to transfer data
c. The client opens a UPD connection to the server in order to transfer data
d. The client opens a TCP connection to the server in order to transfer data

Answer: d

Network Trace 2

```
[**] IDS246 - MISC - Large ICMP Packet [**]
12/28-17:12:24.097245 attacker.net -> my.network.com
ICMP TTL:247 TOS:0x0 ID:54277  DF
ID:48282   Seq:61662  ECHO
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
31 00 00 00 60 3A 11 40 58 15 07 08 58 15 07 08  1...`:.@X...X...
00 40 00 00 00 00 00 00 01 00 00 00 01 00 00 00  .@..............
01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ................
19 00 00 00 06 00 00 00 44 00 00 00 00 00 00 00  ........D.......
00 00 00 00 18 00 00 00 A1 04 00 00 F0 01 BD 9C  ................
C0 64 E4 9C 70 93 B8 9E 60 31 C0 9F F8 58 87 A0  .d..p...`1...X..
E8 82 99 A1 F8 0D 94 A2 E8 06 5F A3 F0 E8 73 A4  ..........._...s.
E8 E8 3E A5 F0 CA 53 A6 E8 CA 1E A7 F0 EC 2D AA  ..>...S.......-.
E8 8E DE AA 70 AB FC AB E8 70 BE AC 70 8D DC AD  ....p....p..p...
E8 52 9E AE 50 53 BC AF C0 11 7E B0 50 35 9C B1  .R..PS....~.P5..
40 2E 67 B2 50 17 7C B3 40 10 47 B4 50 F9 5B B5  @.g.P.|.@.G.P.[.
40 F2 26 B6 50 DB 3B B7 40 D4 06 B8 D0 F7 24 B9  @.&.P.;.@.....$.
40 B6 E6 B9 D0 D9 04 BB C0 D2 CF BB D0 BB E4 BC  @...............
C0 B4 AF BD D0 9D C4 BE C0 96 8F BF D0 7F A4 C0  ................
C0 78 6F C1 D0 61 84 C2 C0 5A 4F C3 D0 43 64 C4  .xo..a...ZO..Cd.
C0 3C 2F C5 50 60 4D C6 C0 1E 0F C7 50 42 2D C8  .</.P`M.....PB-.
E0 FB 60 D2 F0 E4 75 D3 E0 DD 40 D4 F0 C6 55 D5  ..`...u...@...U.
E0 BF 20 D6 F0 A8 35 D7 E0 A1 00 D8 F0 8A 15 D9  .. ...5.........
60 A8 0E DA 70 A7 FE DA 60 8A EE DB 70 89 DE DC  `...p...`...p...
60 82 A9 DD 70 6B BE DE 60 64 89 DF 70 4D 9E E0  `...pk..`d..pM..
60 46 69 E1 70 2F 7E E2 60 28 49 E3 70 11 5E E4  `Fi.p/~.`(I.p.^.
60 0A 29 E5 F0 2D 47 E6 E0 26 12 E7 F0 0F 27 E8  `.)..-G..&....'.
E0 F2 16 E9 F0 F1 06 EA E0 D4 F6 EA F0 D3 E6 EB  ................
E0 B6 D6 EC F0 B5 C6 ED 60 D3 BF EE 70 D2 AF EF  ........`...p...
60 B5 9F F0 70 B4 8F F1 60 97 7F F2 70 96 6F F3  `...p...`...p.o.
60 79 5F F4 70 78 4F F5 60 5B 3F F6 70 5A 2F F7  `y_.pxO.`[?.pZ/.
E0 77 28 F8 70 3C 0F F9 E0 59 08 FA F0 58 F8 FA  .w(.p<...Y...X..
E0 3B E8 FB F0 3A D8 FC E0 1D C8 FD F0 1C B8 FE  .;...:..........
E0 FF A7 FF F0 FE 97 00 E0 E1 87 01 F0 E0 77 02  ..............w.
60 FE 70 03 70 FD 60 04 60 E0 50 05 70 DF 40 06  `.p.p.`.`.P.p.@.
60 C2 30 07 70 C1 20 08 60 A4 10 09 70 A3 00 0A  `.0.p. .`...p...
60 86 F0 0A 70 85 E0 0B E0 A2 D9 0C 70 67 C0 0D  `...p.......pg..
E0 84 B9 0E F0 83 A9 0F E0 66 99 10 F0 65 89 11  .........f...e..
E0 48 79 12 F0 47 69 13 E0 2A 59 14 F0 29 49 15  .Hy..Gi..*Y..)I.
E0 0C 39 16 F0 0B 29 17 60 29 22 18 F0 ED 08 19  ..9...).`)".....
60 0B 02 1A 70 0A F2 1A 60 ED E1 1B 70 EC D1 1C  `...p...`...p...
60 CF C1 1D 70 CE B1 1E 60 B1 A1 1F F0 00 76 20  `...p...`.....v
60 93 81 21 F0 E2 55 22 E0 AF 6A 23 F0 C4 35 24  `..!..U"..j#..5$
E0 91 4A 25 F0 A6 15 26 E0 73 2A 27 70 C3 FE 27  ..J%...&.s*'p..'
E0 55 0A 29 70 A5 DE 29 E0 37 EA 2A 70 87 BE 2B  .U.)p..).7.*p..+
60 54 D3 2C 70 69 9E 2D 60 36 B3 2E 70 4B 7E 2F  `T.,pi.-`6..pK~/
60 18 93 30 F0 67 67 31 60 FA 72 32 F0 49 47 33  `..0.gg1`.r2.IG3
```

```
60 DC 52 34 F0 2B 27 35 60 BE 32 36 F0 0D 07 37  `.R4.+'5`.26...7
E0 DA 1B 38 F0 EF E6 38 E0 BC FB 39 F0 D1 C6 3A  ...8...8...9...:
E0 9E DB 3B 70 EE AF 3C E0 80 BB 3D 70 D0 8F 3E  ...;p..<...=p..>
E0 62 9B 3F 70 B2 6F 40 60 7F 84 41 70 94 4F 42  .b.?p.o@`..Ap.OB
60 61 64 43 70 76 2F 44 60 43 44 45 70 58 0F 46  `adCpv/D`CDEpX.F
60 25 24 47 F0 74 F8 47 60 07 04 49 F0 56 D8 49  `%$G.t.G`..I.V.I
60 E9 E3 4A F0 38 B8 4B E0 05 CD 4C F0 1A 98 4D  `..J.8.K...L...M
E0 E7 AC 4E F0 FC 77 4F E0 C9 8C 50 70 19 61 51  ...N..wO...Pp.aQ
E0 AB 6C 52 70 FB 40 53 E0 8D 4C 54 70 DD 20 55  ..lRp.@S..LTp. U
E0 6F 2C 56 70 BF 00 57 60 8C 15 58 70 A1 E0 58  .o,Vp..W`..Xp..X
60 6E F5 59 70 83 C0 5A 60 50 D5 5B F0 9F A9 5C  `n.Yp..Z`P.[...\
60 32 B5 5D F0 81 89 5E 60 14 95 5F F0 63 69 60  `2.]...^`.._.ci`
E0 30 7E 61 F0 45 49 62 E0 12 5E 63 F0 27 29 64  .0~a.EIb..^c.')d
E0 F4 3D 65 70 44 12 66 E0 D6 1D 67 70 26 F2 67  ..=epD.f...gp&.g
E0 B8 FD 68 70 08 D2 69 E0 9A DD 6A 70 EA B1 6B  ...hp..i...jp..k
60 B7 C6 6C 70 CC 91 6D 60 99 A6 6E 70 AE 71 6F  `..lp..m`..np.qo
60 7B 86 70 F0 CA 5A 71 60 5D 66 72 F0 AC 3A 73  `{.p..Zq`]fr..:s
60 3F 46 74 F0 8E 1A 75 E0 5B 2F 76 F0 70 FA 76  `?Ft...u.[/v.p.v
E0 3D 0F 78 F0 52 DA 78 E0 1F EF 79 F0 34 BA 7A  .=.x.R.x...y.4.z
E0 01 CF 7B 70 51 A3 7C E0 E3 AE 7D 70 33 83 7E  ...{pQ.|...}p3.~
E0 C5 8E 7F 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01  ................
00 01 00 01 00 01 00 01 00 01 00 00 C0 C7 FF FF  ................
01 00 00 00 B0 B9 FF FF 00 04 00 00 45 44 54 00  ............EDT.
45 53 54 00 00 00 00 00 79 01 00 00 FF FF FF FF  EST.....y.......
44 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  D...............
A0 14 07 08 00 00 00 00 02 00 00 00 04 00 00 00  ................
F0 0D 07 08 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 44 00 00 00 F2 0D 07 08 00 00 00 00  ....D...........
00 00 00 00 00 00 00 00 01 00 00 00 70 0E 07 08  ............p...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

1. Source of the Trace:
The traffic was captured by tcpdump, which we had configured on a system outside our firewall.

2. Detect was generated by:
This trace was an outtake of Snort v1.6.3 using the full rule set. It was triggered by the following rule:

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"IDS246 - MISC -
Large ICMP Packet"; dsize: >800;)
```

3. Probability the source address was spoofed:
There is a high probability that the address was spoofed to prevent detection. This type of request does not return any useful information.

4. Description of Attack:
A large icmp packet was sent to my firewall. This is an older method of attack and was recorded in CVE-1999-0128 (See Appendix A).

5. Attack Mechanism
The attacker used a command similar to: *ping –l 65535 my.network.com*

6. Correlations:
This detect indicates that someone was attempting to perform a DoS on my firewall. I assume that the attacker was hoping that the system had not been patched against known or older types of attacks. Non-patched systems would not be able to handle a large sized icmp packet and would crash as a result.

I performed a lookup at http://whois.arin.net/whois/index.html and determined that the source IP belonged to a large Canadian bank.

7. Evidence of active targeting:
There is evidence of active targeting since the attack attempts to knock out our firewall.

8. Severity:
The severity of this attack is: 1

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

(5 + 1) – (4 + 4) = 1

Criticality = 5 The target was our firewall
Lethality = 4 Can cause non-patched systems to crash
System Countermeasure = 4 Patched against this vulnerability
Network Countermeasure = 4 Firewall does not respond to pings.

9. Defensive Recommendations:
Ensure your systems are patched against the Ping O'Death and other older type of exploits. Just because they are older methods of exploit, does not mean they are not used anymore.

10. Multiple choice test question:

A large ICMP packet can be created with the following:

a. arp –a
b. ping –l 65510 destination.ip.address
c. ping –s
d. traceroute destination.ip.address

Answer: b

Network Trace 3

Time	Src IP	Dst IP	proto
14:50:53	216.52.125.38	mynetwork.net	icmp
14:50:53	63.251.143.2	mynetwork.net	icmp
14:50:53	63.251.120.2	mynetwork.net	icmp
14:50:53	216.52.85.194	mynetwork.net	icmp
14:50:53	216.52.172.130	mynetwork.net	icmp
14:50:53	63.251.159.2	mynetwork.net	icmp
14:50:53	64.94.163.226	mynetwork.net	icmp
14:50:53	63.251.61.6	mynetwork.net	icmp
14:50:53	216.52.189.36	mynetwork.net	icmp
14:50:53	63.251.235.226	mynetwork.net	icmp
14:50:53	216.52.153.130	mynetwork.net	icmp
14:50:53	216.52.44.194	mynetwork.net	icmp
14:50:53	216.52.110.66	mynetwork.net	icmp
14:50:53	64.94.206.66	mynetwork.net	icmp
14:51:23	216.52.125.38	mynetwork.net	domain-udp
14:51:23	63.251.143.2	mynetwork.net	domain-udp
14:51:23	63.251.120.2	mynetwork.net	domain-udp
14:51:23	216.52.85.194	mynetwork.net	domain-udp
14:51:23	216.52.172.130	mynetwork.net	domain-udp
14:51:23	63.251.159.2	mynetwork.net	domain-udp
14:51:23	64.94.163.226	mynetwork.net	domain-udp
14:51:23	63.251.61.6	mynetwork.net	domain-udp
14:51:23	216.52.189.36	mynetwork.net	domain-udp
14:51:23	63.251.235.226	mynetwork.net	domain-udp
14:51:23	216.52.153.130	mynetwork.net	domain-udp
14:51:23	216.52.44.194	mynetwork.net	domain-udp
14:51:23	216.52.110.66	mynetwork.net	domain-udp
14:51:23	64.94.206.66	mynetwork.net	domain-udp

1. Source of Trace:

This was taken from our Internet firewall. I noticed this traffic back in November and December of 2000. I have not seen too much of it lately. This trace is in the format of time; source IP; destination IP; destination port.

2. Detect was generated by:

This detect was generated by exporting the firewall logs using the fw logexport command to create a colon delimited file which was then imported to Excel. For these files, I have concentrated on the all rejected and dropped entries.

3. Probability the source address was spoofed:

There is a low probability that the addresses are spoofed as they seem to be requesting dns-udp.

4. Description of Attack:

This attack used a script or tool to send a multitude of ICMP and DNS packets at our firewall. The source IP's were repeated for both floods. The dns portion always occurred 30 seconds after the icmp packets. The frequency of this pattern was approximately 30 times daily.

5. Attack Mechanism:

I had difficulty determining the attack mechanism since I was not able to find an exploit that encompassed both icmp and dns packets. I was however able to locate an exploit on rootshell for a script called doomdns. Doomdns attempts a smurf style flood, sending dns requests using spoofed addresses.

The icmp floods could have been generated by any number of tools, including nmap. The icmp packets were sent to a single IP address - not a range.

6. Correlations:
My first objective was to resolve all the addresses in the list using a whois lookup. All addresses resolved to either InterNAP Network Services or Speedera.

Here are the results of the search at http://whois.arin.net/whois/index.html.

Speedera (NETBLK-PNAP-NYM-SPDERA-DC-02)
4800 Great America Parkway
Santa Clara, CA 95054
US

Netname: PNAP-NYM-SPDERA-DC-02
Netblock: 64.94.163.224 - 64.94.163.255

Coordinator:
Operations Center, InterNAP Network (INO3-ARIN) noc@INTERNAP.COM
206.256.9500 (FAX) 206.256.9580

Record last updated on 19-Sep-2000.
Database last updated on 10-Feb-2001 18:25:02 EDT.

InterNAP Network Services (NETBLK-PNAP-05-2000)
Two Union Square
601 Union St., Suite 1000
Seattle, WA 98101
US

Netname: PNAP-05-2000
Netblock: 64.94.0.0 - 64.95.255.255
Maintainer: PNAP

Coordinator:
Operations Center, InterNAP Network (INO3-ARIN) noc@INTERNAP.COM
206.256.9500 (FAX) 206.256.9580

Domain System inverse mapping provided by:

NS1.PNAP.NET 206.253.194.65
NS2.PNAP.NET 206.253.194.97

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 09-Jan-2001.
Database last updated on 10-Feb-2001 18:25:02 EDT.

I then used www.google.com to determine what business this organization might be in order to determine what could be causing this activity.

After reading information about their service, I learned that Speedera offers web load balancing. For example, if you were a customer with a site hosted with Speedera, they would place copies of your site throughout the world. When users want to access a particular site, they are routed to the closest web site hosting your pages, in order to reduce network access time, while providing full redundancy.

Due to a mis-configuration or a compromised system, my site was seen as a Speedera host site, and therefore was constantly being polled for availability. As part of the failover process, I am sure it was attempting to determine if the other sites were available.

7. Evidence of Active Targeting:
There is no evidence of active targeting since this traffic was not attempting anything malicious. It was just flooding my site with the icmp and dns requests.

8. Severity:
The severity of this attack is: 1

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

(3 + 2) – (2 + 2) = 1

Criticality = 3 The dns server is somewhat critical to our business.
Lethality = 2 The network volume was not enough to accomplish a DoS
System Countermeasure = 2 Patched to latest version
Network Countermeasure = 2 Our firewall does not respond to pings but does allow dns. As a result, we cannot protect ourselves against this type of traffic.

9. Defensive Recommendations:
Ensure icmp traffic is not allowed into your network including the DMZ (Demilitized Zone). Ensure all activity to your DNS servers is logged to ensure you are able to detect malicious activity. You may also want to place a performance agent that monitors system utilization (eg: CPU, NIC's, HD) and determine whether spikes are normal or signify a pending attack.

Our firewall did its job and prevented the icmps from entering our network.

10. Question:

When performing a zone transfer from a Primary DNS to a Secondary DNS which of the following protocols are used?

a. UDP 53
b. TCP 53
c. UDP 53 & TCP 53
d. Neither UDP 53 or TCP 53

Answer: b

Network Trace 4

21989.829000 attacker.net mynet.com UDP Source Port: 6112 Destination Port: 6112
21990.335999 attacker.net mynet.com UDP Source Port: 6112 Destination Port: 6112
21990.335999 attacker.net mynet.com UDP Source Port: 6112 Destination Port: 6112

1. Source of Trace:
I got this from a personal PC firewall. It is shown in the format of: time; source address; destination address; source port; destination port.

2. Detect was generated by:
The alert was originally created and logged by NetworkICE. It was detected as a UDP scan. The logs are created in .enc format. Ethereal was used to view the packets shown above.

3. Probability the address was spoofed:
Chances are the address was not spoofed as the attacker would like to know the results of the scan.

4. Description of attack:
Multiple attempts by a system to attach to UDP port 6112.

5. Attack Mechanism:
A script or tool that polls UDP port 6112. I checked out cve.mitre.org and rootshell.com and found nothing which describes such an attack mechanism.

6. Correlations:
Since I had never seen this port before, I searched http://www.isi.edu/in-notes/iana/assignments/port-numbers to determine what services, if any, operated on this port. I discovered that battle.net operates on this port.

I then went to www.google.com to see what I could find out about this game. Battle.net is a Dungeons and Dragons network-based game available over the net. I was able to determine that this port does use UDP 6112.

The previous holder of my IP address must have been playing battle.net and the server was attempting to determine my status.

7. Evidence of active targeting:
There is no evidence of active targeting in this instance as it is using a known network game port.

8. Severity:
The severity of this attack is: -1

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

(3 + 4) – (4 + 4) = -1

Criticality = 3 The attack was against a home PC.
Lethality = 4 If the attacker exercised this vulnerability, s/he could acquire root privileges
System Countermeasure = 4 Not using CDE on system
Network Countermeasure = 4 Firewall blocks attempts to this port and alerts me of the attempt.

9. Defensive recommendations:
Ensure gaming traffic is blocked by a firewall. Games should not be played on corporate networks due the overhead it places on network availability.

10. Multiple choice question:

If you are connecting to the Internet through a dial-up connection, is it possible to receive packets from a session that was held by the previous holder of your IP?

a. Yes, only if you are registered to the site.
b. No
c. Yes, only if you were logged on previously (within the day).
d. Yes

Answer: d

Assignment 2 – "Analyze This" Scenario

Security Analysis of GIAC Enterprises

Completed by: Faud Khan

This security analysis is performed as part of an RFP (request for proposal) for security services by Faud Khan Inc.. The customer, GIAC Enterprises, provided the source of the data for this review as Snort IDS alert logs, scan logs, and schedule logs. Previous analyses performed for GIAC enterprises were also reviewed by Faud Khan Inc,, before conducting this analysis.

Due to power failures and hard drive space availability, the logs received do not represent a complete picture of the traffic sent to and received by the customer site. GIAC did not disclose any information pertaining to its network architecture, security/usage policies and/or procedures, or security controls (electronic or otherwise).

Part 1 – Overview of Findings:

The major alerts recorded include the following:
Watchlists; WinGate; SYN-FIN scan; TCP SMTP Source port traffic, Sun RPC access; Null scan; Happy 99 virus; Broadcast pings to subnet 70; Possible wu-ftpd exploit; and Interesting traffic from the GIAC MY.NET network.

The list of alert files used is documented in the Appendix B, this appendix illustrates the number of each alert type for the give period analyzed. This chart illustrates that the SYN-FIN scans are the primary source of you alerts followed by the two Watchlist entries.

From the Snort scan reports we were able to determine your top 10 source IP's and destination IP's listed in tables 1 and 2 below. I have also included the Whois lookups for these Source IP addresses in Appendix C. All scan log files were used to compile these numbers.

Source IP	Name of Network	Number of Ports Scanned
66.9.27.254	Intellispace Inc.	20649
62.252.21.241	NTL Internet	13057
194.244.78.145	Zanussi Electrolux	11904
63.88.175.201	UUNet Technologies Inc.	11718
62.157.23.237	Deutche Telekom AG	9641
62.96.169.86	De Colt NMG	8939
24.23.151.112	@Home Network	8763
64.50.161.162	CapuNet, LLC	8635
160.78.49.191	Centro di Calcolo di Ateneo	7192
128.211.237.11	Purdue University	7003

Table 1

Top Destination IP's	Number of Accesses
MY.NET.220.2	11908
MY.NET.218.50	2352
MY.NET.206.94	1786
MY.NET.120.36	1586
MY.NET.253.114	1498
MY.NET.215.210	1361

MY.NET.140.57	1216
MY.NET.70.121	1198
MY.NET.204.26	1162
MY.NET.204.218	1116

Table 2

Part 2 – Detailed Analysis of Top Alerts:

Watchlists

There were high instances of Watchlist 000222 IL-ISDNNET-990517. There were the following attempts:

```
10/13-06:22:51.058911 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:51.273017 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:51.778331 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:52.148403 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:53.266932 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:54.572628 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:55.273258 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:55.606272 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:56.356432 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
 10/13-06:22:56.939684 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.41.24:1031 -> MY.NET.214.170:6699
```

From the trace above it looks as if Napster traffic is entering your network. I located the following detail posted from Jordan Ritter, Security Director, Network Operations Napster, Inc.

> To explain briefly, when a user installs Napster on their system and logs in for the first time, they are prompted to automatically configure their file transfer settings. Since file transfers are done client to client, this involves finding an acceptable port on the client from which it can listen for incoming connections, should another client wish to download a file from it. As part of the automatic configuration, the Napster server connects back to the client over a small range of port numbers in an attempt to negotiate an appropriate port. A few of these ports are non-standard, such as '6699'.

Napster traffic is notorious for clogging network bandwidth and allowing access to your systems if a users has installed the server component. You should ensure that no user has the server component installed on his/her PC.

When I performed a reverse lookup on the address 212.179.41.24, I got the following result:

```
24.41.179.212.IN-ADDR.ARPA domain name pointer fr-c41024.bezeqint.net
```

When I performed a whois at the RIPE site, I got the following result:

```
inetnum:      212.179.41.0 - 212.179.41.63
netname:      YTV-VILLEGE
```

```
descr:       YTV-villege-LAN
country:     IL
admin-c:     TP1233-RIPE
tech-c:      NP469-RIPE
status:      ASSIGNED PA
notify:      hostmaster@isdn.net.il
changed:     hostmaster@isdn.net.il 20000109
source:      RIPE


route:       212.179.0.0/17
descr:       ISDN Net Ltd.
origin:      AS8551
notify:      hostmaster@isdn.net.il
mnt-by:      AS8551-MNT
changed:     hostmaster@isdn.net.il 19990610
source:      RIPE
```

There were also numerous attempts from Watchlist 000222 NET-NCFC. The following lists a sample of the attempts. In this particular attempt, the rogue user seems to be sending mail (port 25 is SMTP) to MY.NET.6.7. It is recommended that a filter be created on your mail server, or even better, a rule on your firewall be written which blocks this address from sending/receiving mail from your site.

```
10/04-09:49:15.510938 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:15.562236 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:16.257079 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:16.264965 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:16.290453 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:17.117343 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:17.796997 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:18.504492 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:19.298233 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:19.314770 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:20.745196 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:20.751403 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
 10/04-09:49:20.759437 [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:4082 -> MY.NET.6.7:25
```

When I performed a reverse lookup on the address 212.179.41.24, I got the following result:

3.45.226.159.IN-ADDR.ARPA domain name pointer aphy.iphy.ac.cn

When I performed a whois at the ARIN site, I got the following result:

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

        Netname: NCFC
        Netblock: 159.226.0.0 - 159.226.255.255

        Coordinator:
           Qian, Haulin  (QH3-ARIN)  hlqian@NS.CNC.AC.CN
           +86 1 2569960

        Domain System inverse mapping provided by:

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

        Record last updated on 25-Jul-1994.
        Database last updated on 15-Feb-2001 07:42:15 EDT.
```

Wingate

Wingate is a proxy server that typically utilizes ports 1080 and 8080. On occasion, you will discover users who install and operate a Wingate server in order to avoid detection of Internet usage. The downside to this is that this proxy server has some vulnerability that is listed in CVE-1999-0290, CVE-1999-0291, CVE-1999-0441, and CVE-1999-0494 (See Appendix A).

```
10/02-11:24:01.140538 [**] WinGate 1080 Attempt [**] 204.117.70.5:4694
-> MY.NET.218.166:1080
 10/02-11:32:47.606417 [**] WinGate 1080 Attempt [**] 64.86.5.250:1989
-> MY.NET.201.94:1080
10/02-11:36:54.831911 [**] WinGate 1080 Attempt [**]
195.14.143.248:1167 -> MY.NET.217.38:1080
 10/02-11:42:15.388192 [**] WinGate 1080 Attempt [**]
213.96.27.142:3644 -> MY.NET.203.78:1080
```

I performed some reverse lookups of the addresses and found out the following:

The address 204.117.70.5 returned the following information:

```
5.70.117.204.IN-ADDR.ARPA domain name pointer security.enterthegame.com
```

www.enterthegame.com is a IRC chat site for gamers.

The address 64.86.5.250 returned the following information:

```
250.5.86.64.IN-ADDR.ARPA domain name pointer proxy3.monitor.dal.net
```

www.dal.net is a well-known IRC chat service which claims to be the world's largest.

The address 195.14.143.248 returned the following information:

```
248.143.14.195.IN-ADDR.ARPA domain name pointer ni-8-120.cytanet.com.cy
```

www.cytanet.com.cy is an ISP based out of Cyprus.

The address 213.96.27.142 returned a not known.

Access to the two IRC (Internet Relay Chat) sites listed above, seems to be normal activity that is generated by an IRC server. The IRC server checks for a misconfigured Wingate or SOCKS proxy when attempting to connect. The check is the trigger for this activity. So long as the destination is the GIAC network, you can assume IRC servers. This was discovered by Julie Lefebvre, in a previous trace analyses.

SYN-FIN Scan

A SYN-FIN scan was performed on multiple occasions I have included a sample from October 23 below. The target seems to be a telnet server on the GIAC site. A SYN-FIN scan attempts to bypass firewalls by using a bit combination that is not possible. The FIN flag is used to break a connect, and the SYN to begin one. This could indicate a scan performed by nmap. The source address is that of a well-known cable modem network --previous reports have already seen many scans from this network.

If GIAC doesn't have any telnet servers, this traffic should be blocked at the firewall. If however GIAC is required to offer this service, it is recommended that the service be replaced by SSH to ensure the communications are preformed securely.

```
10/23-16:25:29.782419  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.109.32:23
10/23-16:25:44.629307  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.109.40:23
10/23-16:27:44.901333  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.109.218:23
10/23-16:27:44.901522  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.109.219:23
10/23-16:29:29.714672  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.110.54:23
10/23-16:38:07.298597  [**] SYN-FIN scan! [**] 24.7.227.215:4 ->
MY.NET.111.130:23
```

TCP SMTP Source Port traffic

The following is only a small excerpt of the total number of attempts. However, it does indicate that someone is sending GIAC SMTP traffic. The source of this traffic is from a known cable modem network that has previously shown signs of mischievous behaviour. This is cause for concern since they seem to be pushing this mail to a wide range of GIAC's network addresses. It is probable that the attacker is trying to send e-mail that has a virus or trojan.

```
10/23-17:44:28.010034  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.73:25
10/23-17:44:39.990890  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.82:25
10/23-17:44:42.053323  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.83:25
10/23-17:44:50.240900  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.92:25
```

```
10/23-17:45:07.203530  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.111:25
10/23-17:45:10.081676  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.115:25
10/23-17:45:10.906179  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.119:25
10/23-17:45:10.906228  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.120:25
10/23-17:45:22.074347  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.156:25
10/23-17:45:25.944016  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.163:25
10/23-17:45:25.946556  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.169:25
10/23-17:45:27.022177  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.172:25
10/23-17:45:30.154692  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.178:25
10/23-17:45:30.157557  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.181:25
10/23-17:45:30.158829  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.179:25
10/23-17:45:36.046561  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.204:25
10/23-17:45:38.908188  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.217:25
10/23-17:45:40.982247  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.221:25
10/23-17:45:41.918318  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.225:25
10/23-17:45:43.040778  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.229:25
10/23-17:45:45.903673  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.243:25
10/23-17:45:45.906329  [**] TCP SMTP Source Port traffic [**]
24.7.227.215:25 -> MY.NET.146.239:25
```

If GIAC doesn't already have virus scanning on its desktops, it is advised to install it. It is also recommended that GIAC install anti-virus software on its mail gateway to eliminate viruses when they arrive at the mail server. GIAC should also ensure that it subscribes to monthly signature/software updates to ensure it is constantly protected.

Sun RPC high port access

This access was recorded as the following entry:

```
10/05-23:44:23.183592  [**] SUNRPC highport access! [**]
212.86.129.227:888 -> MY.NET.202.242:32771
```

This system should be checked to determine if RPC's are operational as it could indicate this system has been compromised. There are several known exploits for RPC.

A second system on GIAC's network also is running RPC and has had many attempts to connect. Although this system does not seem to be compromised at this point, it is advisable to restrict the

RPC accesses until it can be determined that the previous system has not been compromised. The following alerts illustrate this activity.

```
10/05-03:27:21.093571  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:28:21.041042  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:34:20.701790  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:35:20.638168  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:38:20.467000  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:39:20.418280  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:41:20.304220  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:42:20.244550  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:49:19.845401  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:51:19.731571  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:53:19.622033  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
10/05-03:58:19.341260  [**] Attempted Sun RPC high port access [**]
205.188.153.116:4000 -> MY.NET.225.210:32771
```

Null Scan

Several null scans were performed on systems. I have included the sampling below. A Null Scan attempts to map a network typology by avoiding detection on your firewall. It accomplishes this task by not having any TCP flags enabled. This function does not work against Microsoft operation systems due the non-conformity to the TCP/IP standard. However, when attempted, it is a good method for identifying the platform for the target system. Basically, if there is no response, you can assume that it is a Microsoft-based system. If a response is received, then you can safely assume the OS is a flavour of unix.

```
10/08-10:28:17.854721  [**] Null scan! [**] 24.200.80.101:0 ->
MY.NET.208.142:1131
10/08-20:37:50.384460  [**] Null scan! [**] 24.65.126.116:1028 ->
MY.NET.207.78:6688
 10/08-11:09:03.084262  [**] Null scan! [**] 24.95.207.144:1140 ->
MY.NET.201.106:6688
10/08-14:08:46.077483  [**] Null scan! [**] 132.178.218.181:2744 ->
MY.NET.204.170:1591
10/08-14:12:45.535560  [**] Null scan! [**] 132.178.218.181:2744 ->
MY.NET.204.170:1591
10/08-14:45:14.077800  [**] Null scan! [**] 130.239.140.108:2268 ->
MY.NET.205.18:6700
```

Happy 99 Virus

The Happy99 is a worm or trojan horse that is spread from one machine to another as an email or

USENET newsgroup message attachment. When Happy99.exe is executed, it displays a dialog box reading "Happy New Year 1999!!" and shows fireworks.

As this trojan was detected on October 5th, GIAC should ensure that none of its systems have been infected with this worm. GIAC should update its mail servers' and desktops' anti-virus software to identify this trojan. You may want to consider installing a mail gate that performs virus scanning on attachments before they enter your network. In that case, if a worm were detected, the attachment could be deleted to avoid infection.

```
10/05-03:59:51.460766  [**] Happy 99 Virus [**] 216.6.117.11:41827 ->
MY.NET.253.41:25
```

Broadcast Ping to subnet 70

This attack takes advantage of a host's IP stack implementation, and how it deals with ICMP packets to the broadcast address. Basically, most hosts will respond to an echo-request to its broadcast address with an echo reply.

For example, a user spoofs his/her source address to be your web server and sends some broadcast pings to a well-populated remote network. His/her ping is amplified by the number of hosts on the remote network. This is evident as:

```
10/23-16:43:15.154914  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:43:28.140539  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:43:41.075297  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:43:47.571573  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:44:20.055593  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:44:58.841750  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:45:50.597185  [**] Broadcast Ping to subnet 70 [**]
213.154.129.28 -> MY.NET.70.255
10/23-16:47:37.113588  [**] Broadcast Ping to subnet 70 [**]
213.154.130.184 -> MY.NET.70.255
10/23-16:51:56.568218  [**] Broadcast Ping to subnet 70 [**]
213.154.130.184 -> MY.NET.70.255
10/23-16:53:01.375687  [**] Broadcast Ping to subnet 70 [**]
213.154.130.184 -> MY.NET.70.255
```

The following is recommended to reduce the broadcast ping from re-occurring in the future.

- Filter all broadcast traffic from coming into GIAC's network. There are no known applications that are both *routed* and use broadcast addresses. If GIAC is utilizing Variable Length Subnet Mask (VLSM) this could be difficult, but most networks are provisioned on an 8 bit boundary, so you can filter 90% of the traffic by filtering to the .255 address.

Possible wu-ftpd exploit - GIAC000623

From the www.cert.org site, I located the following excerpt of information about this vulnerability.

A vulnerability has been identified in wu-ftpd and other ftp daemons based on the wu-ftpd source code. Wu-ftpd is a common package used to provide file transfer protocol (ftp) services. This vulnerability is being discussed as the wu-ftpd "site exec" or "lreply" vulnerability in various public forums. Incidents involving the exploitation of this vulnerability—which enables remote users to gain root privileges—have been reported to the CERT Coordination Center.

*The wu-ftpd "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server (including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root.*

The "site exec" vulnerability appears to have been in the wu-ftpd code since the original wu-ftpd 2.0 came out in 1993. Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.

The vulnerability appears to be exploitable if a local user account can be used for ftp login. Also, if the "site exec" command functionality is enabled, then anonymous ftp login allows sufficient access for an attack.

```
10/01-06:17:23.004770 [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3746 -> MY.NET.205.94:21
 10/01-06:17:25.604955 [**] site exec - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3739 -> MY.NET.97.206:21
10/01-07:38:44.859097 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3815 -> MY.NET.99.130:21
 10/01-07:38:51.118666 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3816 -> MY.NET.130.81:21
 10/01-07:38:55.557580 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3818 -> MY.NET.130.242:21
 10/01-07:38:58.590607 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3818 -> MY.NET.130.242:21
 10/01-07:38:59.756346 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3818 -> MY.NET.130.242:21
 10/01-07:46:18.953717 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3820 -> MY.NET.205.94:21
 10/01-07:46:19.967002 [**] SITE EXEC - Possible wu-ftpd exploit -
GIAC000623 [**] 208.61.44.215:3820 -> MY.NET.205.94:21
```

From the log trace above, we can determine that many attempts of this exploit were performed from 208.61.44.215. A reverse lookup reveals it is generated from `215.44.61.208.IN-ADDR.ARPA domain name pointer adsl-61-44-215.mia.bellsouth.net`.

If GIAC is using this type of ftp server ensure that you have the patch for this exploit installed immediately if it has not already been.

Interesting traffic from the GIAC MY.NET network

Below I have listed a sampling of some traffic that originates on our MY.NET.98.174 going to the target of MY.NET.101.192, I would ensure that this device is properly configured for SNMP. CVE-1999-0294, CVE-1999-0472, CVE-2000-0379, CVE-2000-0515, and CVE-2000-1058 lists some of the vulnerabilities related to this service. (See Appendix A)

```
10/31-11:45:26.179099 [**] SNMP public access [**] MY.NET.98.174:1048 ->
 MY.NET.101.192:161
 10/31-11:45:39.452121 [**] SNMP public access [**] MY.NET.98.174:1052 ->
```

```
MY.NET.101.192:161
10/31-11:45:39.885360 [**] SNMP public access [**] MY.NET.98.174:1055 ->
MY.NET.101.192:161
10/31-11:45:42.990721 [**] SNMP public access [**] MY.NET.98.174:1059 ->
MY.NET.101.192:161
10/31-11:45:45.392388 [**] SNMP public access [**] MY.NET.98.174:1061 ->
MY.NET.101.192:161
10/31-11:50:00.057694 [**] SNMP public access [**] MY.NET.98.174:1072 ->
MY.NET.101.192:161
10/31-11:51:09.041930 [**] SNMP public access [**] MY.NET.98.174:1073 ->
MY.NET.101.192:161
10/31-11:51:09.042066 [**] SNMP public access [**] MY.NET.98.174:1074 ->
MY.NET.101.192:161
10/31-11:56:38.788533 [**] SNMP public access [**] MY.NET.98.174:1088 ->
MY.NET.101.192:161
10/31-11:56:42.583242 [**] SNMP public access [**] MY.NET.98.174:1094 ->
MY.NET.101.192:161
```

I have included the following detail of what SNMP is and what can be done to reduce the risk. This information was gathered at www.sans.org/topten.htm

The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public", with a few "clever" network equipment vendors changing the string to "private". Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks.

Advice on correcting the problem:
A. If you do not absolutely require SNMP, disable it.
B. If you are using SNMP, use the same policy for community names as used for passwords.
C. Validate and check community names using snmpwalk.
D. Where possible make MIBs read only.

The second suspicious traffic I found on GIAC's network included SMB Name Wildcard. This was indicated by the following alerts:

```
10/31-12:36:15.698573 [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
 MY.NET.101.192:137
 10/31-12:36:15.745980 [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
 MY.NET.101.192:137
```

I have included the following explanation from www.sans.org/topten.htm to give you a better idea of the issues of this exploit.

These services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to any hostile party connected to the network. Many computer owners and administrators use these services to make their file systems readable and writeable in an effort to improve the convenience of data access. Administrators of a government computer site used for software development for mission planning made their files world readable so people at a different government facility could get easy access. Within two days, other people had discovered the open file shares and stolen the mission planning software.

When file sharing is enabled on Windows machines they become vulnerable to both information theft and certain types of quick-moving viruses. A recently released virus called the 911 Worm uses file shares on Windows 95 and 98 systems to propagate and causes the victim's computer to dial 911 on its modem. Macintosh computers are also vulnerable to file sharing exploits.

The same NetBIOS mechanisms that permit Windows File Sharing may also be used to enumerate sensitive system information from NT systems. User and Group information (usernames, last logon dates, password policy, RAS information), system information, and certain Registry keys may be accessed via a "null session" connection to the NetBIOS

Session Service. This information is typically used to mount a password guessing or brute force password attack against the NT target.

The third activity I located on your network includes port scans. They were detected from MY.NET.224.150, MY.NET.221.82, and MY.NET.5.25, the totals were 2981, 2668, and 2300 respectively. These systems should be tracked down and GIAC should determine the purpose of these scans. It could be GIAC's networking staff performing tests, or a rogue user who is attempting to gain access to a system he/she may not have.

Summary of Recommendations

For the next budget year, funding should be set aside to deal with the issue of lost and damaged log files. I recommend GIAC implement a UPS on the systems collecting the data, and use a RAID to reduce the possibility of data loss. Your ability to correctly identify suspicious activity will depend on the data you have available to you.

Ensure all systems especially those listed in the top 10 destinations are securely configured with the latest patches, minimal services operating, auditing turn on, and utilize strong password methodology.

Have firewalls and network based intrusion detection sensors on all gateways to your networks. You should also install host based on system(s) contained on your DMZ (Demilitarized Zone), if you have one.

Other issues:

- Ensure no systems are configured with Napster server or WinGate proxy server.
- Ensure all devices are correctly configured if using SNMP. If this is not required, it should not be configured.
- Determine the internal systems that are scanning your network. They include MY.NET.224.150, MY.NET.221.82, and MY.NET.5.25
- Continue to monitor the traffic from the Watchlists to ensure they you log the compromises. If the number of attacks increase you may want to contact the FBI for assistance in dealing with this situation.
- Do not allow anonymous logins to any system.
- Ensure you not only enable audit logging but also you put a process in place to check these logs on scheduled bases. Remember you can automate this process.
- Replace telnet with SSH for remote administration.
- Ensure you install anti-virus software on your servers and desktops. It would also be well advised to keep the signature bases up-to-date.

Assignment 3: Analysis Process

For the analysis, I primarily used publicly available scripts to generate html-based reports then imported this data to Microsoft Excel and/or Access for correlation purposes.

From www.snort.org, I used the following:

I. SnortSnarf-102700-1
II. snort_sort.pl
III. snort_stat.pl

From other sites, I used the following:
I. ethereal 0.8.12

Unfortunately, I was not able to get snort_stat.pl functioning correctly on my linux box in time for this report's deadline. After many hours of wrestling with the code, I opted for Excel.

My process involved reducing the amount of collected data to a group of categories. Step 1 required me to take a scan file (SnortSx.txt) and strip off the header information included in the file. I then imported this information into a spreadsheet. For each file that was entered, I added another column. I also separated the data between source IP and destination IP into two different spreadsheets. From here, I could use functions such as count and PivotTable Report to analyze the number of instances and so forth.

For the firewall-1 log files, I used the following command to export the log files to a colon-delimited file: fw logexport –l <logfilename> -o <outputfile>

Importing the outputfile into Excel allowed me analyze the data. For problem type IP's, I would store this activity in an Access database for historical tracking.

With one of my sensors, producing tcpdump files, I would run Snort 1.6.3 against this file using the full rules base. From this, I would conduct any further analysis or create an entry in the Access database if this was something I wanted to track. I configured Snort on Mandrake 7.1 to create my alert files.

The firewall logs from the NetworkICE firewall were created in a .enc format. I downloaded a copy of ethereal and used this to analyze the packets. This product makes viewing the details of packets very easy and I like the fact that it supports tcpdump files.

For the analyses I perform on my site I know the target systems on my network. Working with the "Analyze This" scenario was much more difficult with no network architecture. With no indication of the type of target system and function of the system, it is difficult to zoom in on any specifics of a target system.

Appendix A: CVE References

CVE-1999-0128
Oversized ICMP ping packets can result in a denial of service, aka Ping o' Death.

CVE-1999-0290
The WinGate telnet proxy allows remote attackers to cause a denial of service via a large number of connections to localhost.

CVE-1999-0291
The WinGate proxy is installed without a password, which allows remote attackers to redirect connections without authentication.

CVE-1999-0294
All records in a WINS database can be deleted through SNMP for a denial of service.

CVE-1999-0441
Remote attackers can perform a denial of service in WinGate machines using a buffer overflow in the Winsock Redirector Service.

CVE-1999-0472
The SNMP default community name "public" is not properly removed in NetApps C630 Netcache, even if the administrator tries to disable it.

CVE-1999-0494
Denial of service in WinGate proxy through a buffer overflow in POP3.

CVE-2000-0379
The Netopia R9100 router does not prevent authenticated users from modifying SNMP tables, even if the administrator has configured it to do so.

CVE-2000-0515
The snmpd.conf configuration file for the SNMP daemon (snmpd) in HP-UX 11.0 is world writable, which allows local users to modify SNMP configuration or gain privileges.

CVE-2000-0813
Check Point VPN-1/FireWall-1 4.1 and earlier allows remote attackers to redirect FTP connections to other servers ("FTP Bounce") via invalid FTP commands that are processed improperly by FireWall-1, aka "FTP Connection Enforcement Bypass."

CVE-2000-1058
Buffer overflow in OverView5 CGI program in HP OpenView Network Node Manager (NNM) 6.1 and earlier allows remote attackers to cause a denial of service, and possibly execute arbitrary commands, in the SNMP service (snmp.exe), aka the "Java SNMP MIB Browser Object ID parsing problem."

Appendix B: Alert totals for log files analyzed (Assignment #2)

		Attempted Sun RPC high port access	Back Orifice	Broadcast Ping to subnet 70	External RPC call	Happy 99 Virus	NMAP TCP Ping!	Null Scan!	Probable NMAP fingerprint attempt	Queso Fingerprint	site exec - Possible wu-ftpd exploit - GIAC000623	SITE EXEC - Possible wu-ftpd exploit- GIAC000623	SMB Name Wildcard	SNMP public address	SUNRPC highport access!	SYN-FIN scan!	TCP SMTP Source port traffic	Tiny Fragments - Possible Hostile Activity	Watchlist 000222 IL-ISDNNET-990517	Watchlist 000222 NET-NCFC	WinGate 1080 Attempt
SnortA2	4-Oct	183		46			1	1		7	1		2			5652			117	6044	238
SnortA3	16-Oct	46		59			2	2		1	2				7	1			668	27	64
SnortA4	2-Oct	113	24					6		1						6636			164	61	54
SnortA5	2-Oct	16	336	76	1		1	6		4					3	3860			950	15	33
SnortA6	1-Nov	11	61	37	1		3	17	1	1					2				1011	2	25
SnortA7	13-Oct	5		35				3											1353	13	49
SnortA8	1-Oct	8	69					2		3	2	7	7	40		3545			7	30	66
SnortA9	30-Sep	2						6								10598		1	51	34	45
SnortA10	10-Oct		17	1	4		1	3					10	66		2338			1190	4	38
SnortA11	15-Oct			1			1	3											51	69	37
SnortA12	28-Sep							3							3			1	3	84	100
SnortA13	27-Sep							10		16									5	44	160
SnortA14	9-Oct							6											1	32	38
SnortA15	26-Sep	29					4	8		16								1	299	30	124
SnortA19	9-Oct							6											1	32	38
SnortA20	12-Oct	137		1				4											589	7	52
SnortA21	26-Oct	48	23	78				3							2	2582			221	7	37
SnortA22	8-Oct	28		1			2	6	1	5			4					2	3945	15	53
SnortA23	11-Oct		66	62	3			7		1									86	13	37
SnortA24	27-Oct		155	21			2	2	2										18	581	31
SnortA25	7-Oct		2	18				5			1					1105			42	4	24
SnortA26	6-Oct			33			1	5	1	1									963	10	31
SnortA27	25-Oct	128		6			1	4											94	4	31
SnortA28	5-Oct	32		2		1		2							1				1305	26	1917
SnortA29	24-Oct	178		19				9		1			3		1	1			129	25	44
SnortA30	31-Oct	4	70	99	4	5		5				9	52						669	25	24
SnortA31	20-Oct	99	134	44			2	4	1	2			2	3					381	170	34
SnortA32	7-Nov	154	1	53			4	6	1							1085			800	12	26
SnortA33	21-Oct	9	26	39				3		16											33
SnortA34	30-Oct	4		78			4	13		26									63	14	44
SnortA35	23-Oct	63		74	1		5	4	1							3623	1096		1	17	59
SnortA36	28-Oct		95	50	1			2		11			5	31		1			11	5	45
SnortA37	3-Nov	66	8	108			1	7	2				15			3292			48	3	19
SnortA38	22-Oct		174	177				4	1	1						7			3	6	75
SnortA39	29-Oct	49	291	168			4	6		1									8	5	37

Appendix C: Top Source IP's Whois'

1.

```
Intellispace Inc. (NETBLK-ISPACE-NET-2)
        1156 Avenue of the Americas
        New York, NY 10036
        US

        Netname: ISPACE-NET-2
        Netblock: 66.9.0.0 - 66.9.223.255
        Maintainer: ITLS

        Coordinator:
           Admin, IP  (IA43-ARIN)  ipadmin@intellispace.net
           212-536-7968 (FAX) 212-536-7979

        Domain System inverse mapping provided by:

        NS1.INTELLISPACE.NET         160.79.6.130
        NS2.INTELLISPACE.NET         160.79.5.130

        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

        Record last updated on 22-Jan-2001.
        Database last updated on 17-Feb-2001 18:26:34 EDT.
```

2.

```
inetnum:     62.252.0.0 - 62.252.31.255
netname:     NTL
descr:       NTL Internet
descr:       Guildford site
country:     GB
admin-c:     NNMC1-RIPE
tech-c:      COH1-RIPE
status:      ASSIGNED PA
changed:     hostmaster@ntli.net 20001219
source:      RIPE
```

3.

```
inetnum:     194.244.78.0 - 194.244.78.255
netname:     ZANUSSI
descr:       Electrolux Zanussi
descr:       Pordenone
country:     IT
admin-c:     FN148-RIPE
tech-c:      FN148-RIPE
tech-c:      KH565-RIPE
changed:     helpdesk@unisource.it 19970805
changed:     ripe-dbm@ripe.net 19990706
source:      RIPE
```

4.

```
UUNET Technologies, Inc. (NETBLK-UUNET63) UUNET63   63.64.0.0 - 63.127.255.255
MultiLateral Solutio (NETBLK-UU-63-88-175-192) UU-63-88-175-192 63.88.175.192 -
63.88.175.223
```

5.

```
inetnum:     62.157.0.0 - 62.157.86.159
```

```
netname:     DTAG-RAR
descr:       Deutsche Telekom AG
country:     DE
admin-c:     RH2086-RIPE
tech-c:      PH2352-RIPE
tech-c:      KK1550-RIPE
status:      ASSIGNED PA
remarks:     ***************************************************************
remarks:     * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS,      *
remarks:     * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC.        *
remarks:     ***************************************************************
notify:      auftrag@nic.telekom.de
notify:      dbd@nic.dtag.de
mnt-by:      DTAG-NIC
changed:     auftrag@nic.telekom.de 20000913
source:      RIPE
```

6.

```
inetnum:     62.96.128.0 - 62.96.175.255
netname:     DE-COLT-NMG
descr:       neue mediengesellschaft ulm mbh
descr:       Konrad-Celtis-Str.77
descr:       81369 Muenchen
country:     DE
admin-c:     AR134-RIPE
tech-c:      JG1261-RIPE
status:      ASSIGNED PA
notify:      support@addcom.de
notify:      hostmaster@de.colt.net
mnt-by:      DE-COLT-MNT
changed:     bernward@de.colt.net 19990623
changed:     fl1ger@de.colt.net 20000601
source:      RIPE
```

7.

```
@Home Network (NETBLK-ATHOME)   ATHOME               24.0.0.0 - 24.23.255.255
@Home Network (NETBLK-VA-COMCAST-5) VA-COMCAST-5   24.23.144.0 - 24.23.159.255
```

8.

```
CapuNet, LLC (NETBLK-CAPUNET-BLK-CIDR1)
        6000 Executive Blvd. Suite 600
        Rockville, MD 20852
        US

        Netname: CAPUNET-BLK-CIDR1
        Netblock: 64.50.128.0 - 64.50.223.255
        Maintainer: CAPU

        Coordinator:
           Dvorak, John  (JD707-ARIN)  noc@capu.net
           301-881-4900

        Domain System inverse mapping provided by:

        NS.CAPU.NET                 64.50.128.2
        NS2.CAPU.NET                64.50.128.6
        NS3.CAPU.NET                64.50.128.10

        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

        Record last updated on 20-Jun-2000.
        Database last updated on 17-Feb-2001 18:26:34 EDT.
```

9.

```
Centro di Calcolo di Ateneo (NET-PARMANET1)
        Centro di Calcolo di Ateneo
        Universita` di Parma
        Viale Delle Scienze
        43100 PARMA - ITALIA

        Netname: PARMANET
        Netblock: 160.78.0.0 - 160.78.255.255

        Coordinator:
           Fausto, Lina  (LF112-ARIN)  FAUSTO@IPRUNIV
           +39 521 580392

        Domain System inverse mapping provided by:

        SERVER.FIS.UNIPR.IT          192.135.11.20
        CAIO.CCE.UNIPR.IT            160.78.48.10

        Record last updated on 08-Apr-1998.
        Database last updated on 17-Feb-2001 18:26:34 EDT.
```

10.

```
Purdue University (NET-PURDUE-CS-CYP)
        Department of Computer Sciences
        Computer Science Building
        West Lafayette, IN 47907

        Netname: PURDUE-CS-CYP
        Netblock: 128.211.0.0 - 128.211.255.255

        Coordinator:
           Trinkle, Daniel  (DT50-ARIN)  trinkle@CS.PURDUE.EDU
           765-494-7844 (FAX) 765-494-0739

        Domain System inverse mapping provided by:

        PENDRAGON.CS.PURDUE.EDU      128.10.2.5
        MOE.RICE.EDU                 128.42.5.4
        NS.PURDUE.EDU                128.210.11.5
        HARBOR.ECN.PURDUE.EDU        128.46.154.76

        Record last updated on 15-Jul-1994.
        Database last updated on 17-Feb-2001 18:26:34 EDT.
```

Last Updated: July 25th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced