Global Information Assurance Certification Paper

SANS GCIA Practical Version 3.0

Kevin Bong
January 31st, 2002

Contents

Assignment 1: State of Intrusion Detection

Intrusion Detection of remote web sites using Sitescope

This document will outline the challenges we faced in monitoring remote web sites and how we use Freshwater Software's "Sitescope" product to overcoming these challenges.

Our company has three different means for delivering web content and services: Local web servers, remote web servers, and custom branded sites through service providers. Local web servers reside in our data center. Web sites are placed on our local web servers if they need to communicate securely with other local systems. Local web server security is provided by firewalls, network and host-based intrusion detection systems, and file integrity checkers. Remote web servers are co-located at an ISP. These are used for sites that need high-bandwidth and high Internet reliability but do not transmit secure information.

Service provider web sites are hosted and managed by a service provider, who usually also hosts the back-end data that drives the site. For remote web servers and service providers, we do not have the ability to install and manage an intrusion detection system. While in most cases the service provider has their own intrusion detection systems monitoring the services, we feel it is insufficient to depend solely on the service provider for security of the sites.

Remote hosting and service provider websites are very common. Some examples are "virtual servers" which most ISP's provide to their customers, in which the ISP manages one server that serves content for many websites. Another example would be a "Yahoo Shop", in which Yahoo's servers and software host your on-line retail shop.

As common as this type of service is, it is difficult to find solutions to ensure the security of this model. A recommended practice for monitoring such a system for intrusion involves installing a network based IDS on the server's network segment, or installing a host based IDS on the server itself. There are many reasons why this option may not be feasible. The ISP may not allow or support network or host based IDS. Many organizations that use remote hosting are small, so network or host based IDS may be too expensive or the company may not have the knowledge or time required to properly administer an IDS. This document will focus on remote hosting where network or host based IDS is not possible.

Sitescope is not well known in the security community because it bills itself as an uptime monitor. I believe it is greatly underselling itself in terms of a security monitor. In many cases, you need to be "creative" to configure it to monitor for security, but even in these cases the configuration is easy and the system is reliable.

Sitescope Features:

One of the great benefits of Sitescope is that it can be used to monitor websites that use the HTTP Protocol as well as secure websites that use HTTPS/Secure Sockets Layer. The Sitescope application runs on Windows NT and 2000, Solaris Unix, and Linux, but it can monitor websites running on any operating system and web server application.

Monitors and Alerts

Sitescope's two main parts are "Monitors" and "Alert". Sitescope has almost 50 different available monitors, as well as the ability for the user to build custom monitors. A monitor is configured to perform a specific network request and look for a specific response. If a sitescope monitor receives a specific response, it then triggers an alert. An alert can communicates the condition of the monitored service or run a script or application.

Uptime/DOS/Response Times using a URL Monitor

A very common use of Sitescope is to monitor whether web services are available. This is done by configuring Sitescope to load a specific URL periodically, and send an alert if the attempt to load the URL fails. From a security perspective, this can be helpful in notifying you if changes have been made to your server or network which make the web services unavailable. As well as sending alerts on failed attempts, Sitescope will log successful and failed attempts, including the time required to complete the request. This can be helpful in tracking web service availability. Sitescope can be configured to send alerts if the response time for URL requests rises above a set threshold. This can be helpful for detecting denial of service attacks.

URL Transaction monitor

An extension of the URL Monitor is the URL Transaction Monitor. This monitor allows you to monitor a series of steps through a website, such as loading the login page, entering a user ID and password, submitting the login form, verifying the appropriate content is on the response page, and logging out. This is a powerful tool that allows you to monitor that transactional web services and their underlying data providers are functioning correctly.

URL Content Monitor

The URL Content Monitor of Sitescope is very helpful from a security perspective. You configure Sitescope to download a web page at regular intervals. The downloaded copy is compared to the previously downloaded version, and if the content has changed an alert is sent. This is helpful in detecting and quickly responding to defacement attacks. The URL Content Monitor allows for matching content using Regular Expressions. This can allow you to detect defacement attacks on dynamic web pages.

There are a couple of limitations of the URL Content Monitor. The first is that each page you wish to monitor configured separately. This makes it difficult to monitor an entire large site. It also can get expensive; Sitescope is licensed based on the number of monitors you use. Another drawback is that when it downloads and checks a web page, it does not download the associated images. An ideal content monitor would allow you to monitor an entire site including images without a lot of hassle.

DNS Monitor

The DNS Queries a Domain Name server to ensure it is up and is returning the appropriate address for a given domain. This ability can help you to detect DNS Cache Poisoning attacks and corrupted DNS records on a compromised DNS server. It also protects against careless DNS administrators making incorrect changes.

Mail Monitor

The mail monitor's purpose is to ensure that a SMTP gateway is up and relaying mail. Mail relaying is desirable to people who wish to send spam or cover their identity, so in many cases you may want to monitor that your system is not relaying mail. You can be "creative" and configure Sitescope to monitor this. First you create a monitor that attempts to relay mail through your server. This monitor should normally "fail" if your server is configured to block mail relay. Then you create an alert that will trigger when the SMTP Monitor is successful. This will then alert you if

your server is ever configured to allow mail relay.

Port Monitor

The Port Monitor's purpose is to ensure that a service is available on a specific port. You can once again be "creative" to use the port monitor to ensure that a service is not available on a port. For example, you may wish to monitor your server to see if anyone enables a service on port 6667 (IRC), 23 (Telnet), or 27374 (SubSeven). Similar to the Mail Monitor configuration, you will create the alert so that it only triggers when the monitor is successful.

Alerts

Sitescope's alerting structure is very flexible. Alerts are triggered for specific monitors when certain conditions are met, such as an error condition twice in a row, a response time falls below a certain threshold, or a certain regular expression is not found in the response page. There are a great many other conditions that can configured to trigger an alert. When an alert is triggered, it can send an email, a page, or an SMNP message, as well as run a custom script or application.

Reporting

Sitescope has a very powerful reporting tool as well. You can select for reports to contain one monitor or groups of monitors. You can select the time span for chich to generate a report. Reports can be configured to contain summaries of uptimes and access times. Reports can also contain graphs ot tables of uptimes, monitor readings, errors, and alerts sent. Reports can be sent by email automatically, and be scheduled to run at regular times. Below is an excerpt from a Sitescope Report.

Table Format
Error List
Warning List

Back to Reports

About Reports

Management Report for Quantech Web 6.0 Login Attempt

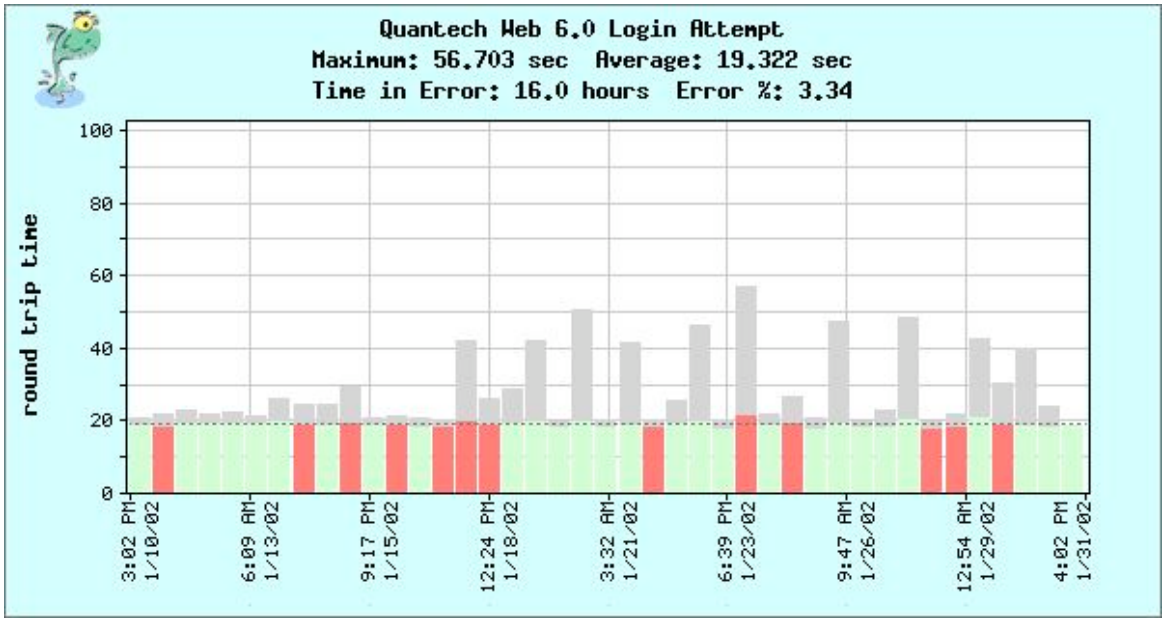
(information from 3:02 PM 1/10/02 to 4:02 PM 1/31/02)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
Quantech Web 6.0 Login Attempt	96.66	3.34	0.00	good

Measurements Summary

Name	Measurement	Max	Avg	Last
Quantech Web 6.0 Login Attempt	round trip time	56.703 sec	19.322 sec	18.469 sec



Time	Round Trip Time
3:02 PM 1/10/02	18.972 sec
3:21 AM 1/11/02	**18.837 sec**
3:40 PM 1/11/02	19.609 sec
3:59 AM 1/12/02	19.815 sec
4:18 PM 1/12/02	19.631 sec
4:37 AM 1/13/02	19.825 sec
4:56 PM 1/13/02	20.046 sec
5:15 AM 1/14/02	**19.004 sec**
5:34 PM 1/14/02	19.022 sec
5:53 AM 1/15/02	**19.621 sec**
6:12 PM 1/15/02	18.978 sec
6:31 AM 1/16/02	**19.143 sec**
6:50 PM 1/16/02	18.403 sec
7:09 AM 1/17/02	**18.846 sec**
7:28 PM 1/17/02	**20.092 sec**
7:47 AM 1/18/02	**19.089 sec**
8:06 PM 1/18/02	19.504 sec
8:25 AM 1/19/02	20.251 sec
8:44 PM 1/19/02	18.372 sec
9:03 AM 1/20/02	20.216 sec
9:22 PM 1/20/02	18.691 sec
9:41 AM 1/21/02	19.280 sec
10:00 PM 1/21/02	**18.496 sec**
10:19 AM 1/22/02	19.622 sec

Time	Round Trip Time
10:38 PM 1/22/02	20.193 sec
10:57 AM 1/23/02	18.018 sec

11:16 PM 1/23/02	**21.824 sec**
11:35 AM 1/24/02	19.123 sec
11:54 PM 1/24/02	**19.878 sec**
12:13 PM 1/25/02	18.254 sec
12:32 AM 1/26/02	19.650 sec
12:51 PM 1/26/02	18.483 sec
1:10 AM 1/27/02	18.826 sec
1:29 PM 1/27/02	20.479 sec
1:48 AM 1/28/02	**18.165 sec**
2:07 PM 1/28/02	**18.674 sec**
2:26 AM 1/29/02	21.121 sec
2:45 PM 1/29/02	**19.024 sec**
3:04 AM 1/30/02	19.255 sec
3:23 PM 1/30/02	18.417 sec
3:42 AM 1/31/02	18.469 sec

Errors from 3:02 PM 1/10/02 to 4:02 PM 1/31/02

Time	Monitor	Status
7:03 AM 1/11/02	Quantech Web 6.0 Login Attempt	Content Matched: HTTP/1.1 200 OK Timed Out Reading on Step 2

There are many other features of Sitescope that make the security administrator's job easier. It allows for aggregation of monitoring tools and centralized alerting and reporting. It has a published API which allows you to build custom monitors for less common or proprietary services. The alerting system allows for escalation paths, so that you can send additional alerts of a different type if initial alerts are not responded to. It allows for scheduled and on-demand reporting, and a log can be kept of all of Sitescope's activity, which makes an excellent audit trail.

When you have your website remotely hosted and managed by an ISP or Application Service Provider, you often have very little control over how the server is configured and are often unable to do any type of Intrusion Detection on the server or the local network. This can make it very difficult to monitor for attacks and other problems. The capabilities of Sitescope listed above make it a very good tool for helping to ensure security of remote websites.

Resources:

Keyes, Jessica ed. "Web Server Monitoring". Handbook OF Internet Management
http://www.freshwater.com/white_paper/chapter.htm

"SiteScope User's Guide". Freshwater Software,
http://www.freshwater.com/SiteScope/UserGuide.htm

"SiteScope Security Essentials". Freshwater Software.
http://www.freshtech.com/white_paper/SiteScopeSecurity.htm

"Sitescope Monitor Types". Freshwater Software.
http://www.freshtech.com/MonitorTypes.htm

Welter, Pete. Why is My Web Site Down.
http://www.freshwater.com/white_paper/article.htm

Assignment 2: Network Detects

Detect 1

```
Jan 8 12:08:12 ns snort: LOCAL - Unexpected TCP connection to a.b.c.10 [Classification: suspicious miscellaneous traffic Priority: 1]: 195.110.131.12:80 -> a.b.c.10:80
Jan 8 12:08:14 Ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2392 -> a.b.c.9:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2393 -> a.b.c.6:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2394 -> a.b.c.4:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2395 -> a.b.c.5:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2398 -> a.b.c.8:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2399 -> a.b.c.15:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2402 -> a.b.c.19:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2405 -> a.b.c.16:80
Jan 8 12:08:14 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2407 -> a.b.c.11:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2409 -> a.b.c.21:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2416 -> a.b.c.3:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2421 -> a.b.c.2:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2423 -> a.b.c.18:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2426 -> a.b.c.17:80
Jan 8 12:08:15 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2427 -> a.b.c.14:80
Jan 8 12:08:16 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2437 -> a.b.c.20:80
Jan 8 12:08:16 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2443 -> a.b.c.12:80
Jan 8 12:08:16 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2401 -> a.b.c.7:80
Jan 8 12:08:18 ns snort: IDS535/web-iis_http-iis5-printer-beavuh [Classification: system integrity attempt Priority: 11]: 195.110.131.12:2458 -> a.b.c.33:80

Internet Protocol
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN:
0x00)
0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 1234
Identification: 0x8d53
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 51
Protocol: TCP (0x06)
Header checksum: 0x0486 (correct)
Source: kboom.chas.mvl.intelos.net (216.12.99.33)
Destination: my.ip.addy.70
Transmission Control Protocol, Src Port: 1740 (1740), Dst Port: 80 (80),
Seq: 4292866325, Ack: 3404677060
Source port: 1740 (1740)
Destination port: 80 (80)
Sequence number: 4292866325
Next sequence number: 4292867507
Acknowledgement number: 3404677060
Header length: 32 bytes
Flags: 0x0018 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
.... ...0 = Fin: Not set
Window size: 32120
Checksum: 0x5949 (correct)
Options: (12 bytes)
NOP
NOP
Time stamp: tsval 418443450, tsecr 4563557
Hypertext Transfer Protocol
GET /NULL.printer HTTP/1.0\r\n
Beavuh:
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\353\003]\353\005\350\370\377\377\377\203\305\025\220\220\220\21
3\3053\311f\271\327\002P\2000\225@\342\372-\225\225d\342\024\255\330\317
\005\225\341\22
Host:
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220\220
\220\220\220\220\
\r\n
```

1. Source of Trace.

Incidents.org intrusion list archive

http://www.incidents.org/archives/intrusions/msg03193.html
http://www.incidents.org/archives/intrusions/msg03192.html

2. Detect was generated by:

The log was generated by the Snort intrusion detection system. The Snort rule for this attack is configured to look for the string "|33 C0 B0 90 03 D8 8B 03 8B 40 60 33 DB B3 24 03 C3|" in traffic destined for port 80.
The packet dump was probably generated by Ethereal or a similar tool.

3. Probability the source address was spoofed:

An attack on the http service (TCP Port 80) requires that a three way handshake be completed. Since these packets have the ack bit set, it appears that the handshake has already been completed. This is not a denial of service attack, so this attack would really have no effect if the source address was spoofed or a three way handshake had not been completed. For these reason, it is unlikely that the source address was spoofed.

4. Description of attack:

This attack is trying to exploit a buffer overflow within the .printer ISAPI filter (C:\WINNT\System32\msw3prt.dll) which provides Windows 2000 with support for the Internet Printing Protocol (IPP). Internet Printing Protocol allows for Web based control of various aspects of networked printers. (Source http://www.eeye.com/html/Research/Advisories/AD20010501.html)

The attacker is attempting to connect to port 80 on a range if IP addresses on the victim's network. The attacker is scanning 6 to 8 machines per second, which means this is almost certianly an automated tool. The source port is incremented each packet, but the order of scanning on the destination addresses seems to be random. This may have been an attempt by the attacker to be covert.

5. Attack mechanism:

The attack works by completing the three-way handshake to a web server (port 80), and then sending an HTTP Get request that could be configured for the Internet Printing Protocol on a Windows 2000 Server. This Get request is followed by HTTP Headers that contain Unicode characters, which are meant to overflow the buffer in the IPP filter application and allow the attacker's code to be run.

6. Correlations:

The Windows 2000 IIS 5.0 remote buffer overflow vulnerability advisory was released in May 2001, and a "proof of concept" exploit is available at http://www.eeye.com/html/research/Advisories/iishack2000.c . Due to the availablity of the exploit, there are many attacks against this vulnerabililty. Similar reports of such scans can be found at http://digitaleyeliner.net/status/snort/sig/sigIDS535.html and http://lists.jammed.com/incidents/2001/07/0072.html.

7. Evidence of active targeting:

This appears to be a scan of a range of IP addresses looking for any machines vulnerable to this exploit.

8. Severity:

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

Note: Since I don't know anything about the victim's network, I will calculate the Severity as though this attack was detected on the network that I administer.

Criticality	4	Some of the machines scanned are critical infrastrucure (DNS, web, and mail servers)
Lethality	4	This attacker would be able to execute code with the privilidges of the IIS application.
System Countermeasures	5	This exploit has been known 7 months before this attack, and all Windows 2000 servers have been appropriately patched

Network Countermeasures	1	The scanned servers not behind the firewall.
(4 + 4) - (5 + 1) = 2		

9. Defensive recommendation:

If the victim's network has any Windows 2000 machines running the IIS webserver, then the machines should be checked to verify that the appropriate patches have been applied to fix this issue, or the IPP filter has been disabled.

10. Multiple choice test question:

The Snort rule to detect this attack is only configured to look at traffic destined for port 80. What is the most likely reason it doesn't also look for web traffic destined for port 443 (SSL)?
A. You cannot run the Internet Printing Protocol over SSL
B. Decrypting the SSL protocol would put too much load on Snort
C. SSL traffic is encrypted, and Snort cannot decrypt it
D. You cannot send HTTP headers to SSL ports

Answer: C. Snort cannot monitor content in traffic that has been encrypted using SSL.

Detect 2

```
12/03-11:07:24.340930 209.27.245.128:39999 -> www.xxx.yyy.5:39999
TCP TTL:240 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

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

12/03-11:07:24.342227 209.27.245.128:39999 -> www.xxx.yyy.4:39999
TCP TTL:242 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

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

12/03-11:07:24.343129 209.27.245.128:39999 -> www.xxx.yyy.12:39999
TCP TTL:242 TOS:0x0 ID:1795 IpLen:20 DgmLen:40
******S* Seq: 0x7AE80725 Ack: 0x4E25A69B Win: 0x28 TcpLen: 20

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

1. Source of Trace.

Incidents.org intrusion discussion list archive
http://www.incidents.org/archives/intrusions/msg02733.html

2. Detect was generated by:

The log appears to be Snort output.

3. Probability the source address was spoofed:

The purpose of this scan appears to be to see if a service is available on port 39999. This would indicate that the attacker is looking for hosts that complete the three-way handshake. For this reason, it is unlikely that the source address was spoofed.

4. Description of attack:

The attacker is scanning a range of hosts by sending an initial TCP SYN packet to port 39999 on each host. It is possible that the attacker is looking for servers that have been compromised with the t0rn rootkit. Attackers have been known to run an SSH shell on port 39999 once they have taken over the box with the t0rn rootkit.

5. Attack mechanism:

The attack works by completing sending syn packets very quickly to a large number of hosts. If any host responds with a SYN/ACK packet it would indicate that there is a service running on the specified port. The scanning software will most likely record all hosts that respond to the SYN packet so that they can be attacked later.

There is

6. Correlations:

Stephen Sheperd reported this same attack at
http://www.incidents.org/archives/intrusions/msg02743.html

```
I saw it too.. Looks like the bad guys were busy this weekend. Times are
GMT -7 and synced..


Dec 1 06:46:53 202.181.234.13:109 -> www.xxx.yyy.6:109 SYNFIN ******SF
Dec 1 07:08:33 202.181.234.13:109 -> www.xxx.yyy.7:109 SYNFIN ******SF
Dec 1 07:30:13 202.181.234.13:109 -> www.xxx.yyy.8:109 SYNFIN ******SF
```

7. Evidence of active targeting:

This appears to be a scan of a large range of IP addresses looking for any machines with port 39999 open. It doesn't seem to be targeting any particular network or host.

8. Severity:

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

Note: Since I don't know anything about the victim's network, I will calculate the Severity as though this attack was detected on the network that I administer.

Criticality	4	Some of the machines scanned are critical infrastrucure (DNS, web, and mail servers)
Lethality	3	If a host on the network responded, it would indicate that it may be compromised
System Countermeasures	5	There are no services running on port 39999 on our network. There are no Unix/linux boxes on the network, so there is no chance of the t0rn rootkit having been installed.
Network Countermeasures	1	The scanned servers are outside the firewall
(4 + 3) - (5 + 1) = 1		

9. Defensive recommendation:

Defenses are fine. There are no machines running services on the scanned port. The IDS did not report that any devices responded to the SYN requests.

10. Multiple choice test question:

If a live host receives a SYN packet for port 39999 and the host does NOT have any program listening on port 39999, what will a likely response be?
A. SYN/ACK
B. RESET
C. ICMP Host Unreachable
D. ICMP Protocol unreachable

Answer: B. Most hosts will respond to a SYN on a port that is not listening with a RESET.

Detect 3

```
Scan report generated from Snort portscan log (www.snort.org)
Source: ABayonne-102-1-1-253.abo.wanadoo.fr (217.128.28.253)
Destination port: 21 (ftp) SYN ******S* Count: 2803
Jan 18 22:54:05 GMT 217.128.28.253:2223 -> 142.90.0.19:21 SYN ******S*
Jan 18 22:54:05 GMT 217.128.28.253:2224 -> 142.90.0.31:21 SYN ******S*
Jan 18 22:54:05 GMT 217.128.28.253:2225 -> 142.90.0.70:21 SYN ******S*
Jan 18 22:54:05 GMT 217.128.28.253:2226 -> 142.90.0.75:21 SYN ******S*
Jan 18 22:54:05 GMT 217.128.28.253:2227 -> 142.90.0.127:21 SYN ******S*
etc. (2803 alerts)

220 obfusc.my.org FTP server (Version wu-2.etc.) ready.
USER anonymous
331 Guest login ok, send your complete e-mail address as password.
PASS guest@here.com
230-Greetings !
230-
230 Guest login ok, access restrictions apply.
CWD /_vti_pvt/
550 /_vti_pvt/: No such file or directory.
CWD /upload/
550 /upload/: No such file or directory.
CWD /home/
550 /home/: No such file or directory.
CWD /public/
550 /public/: No such file or directory.
CWD /pub/
250-This is /pub, the public directory.
250-
250-Please read the file README
250- it was last modified (ages ago)
250 CWD co
MKD 010118235653p
550 010118235653p: Permission denied on server. (Upload dirs)
CWD /temp/
550 /temp/: No such file or directory.
CWD /wwwroot/
550 /wwwroot/: No such file or directory.
CWD /cgi-bin/
550 /cgi-bin/: No such file or directory.
CWD /cgibin/
550 /cgibin/: No such file or directory.
CWD /incoming/
550 /incoming/: No such file or directory.
CWD /in/
550 /in/: No such file or directory.
CWD /_vti_cnf/
550 /_vti_cnf/: No such file or directory.
CWD /_vti_txt/
550 /_vti_txt/: No such file or directory.
CWD /_vti_log/
550 /_vti_log/: No such file or directory.
CWD /anonymous/
550 /anonymous/: No such file or directory.
```

```
CWD /outgoing/
550 /outgoing/: No such file or directory.
CWD /tmp/
550 /tmp/: No such file or directory.
CWD /mailroot/
550 /mailroot/: No such file or directory.
CWD /ftproot/
550 /ftproot/: No such file or directory.
CWD /images/
550 /images/: No such file or directory.
CWD /_private/
550 /_private/: No such file or directory.
CWD /usr/
550 /usr/: No such file or directory.
CWD /pub/incoming/
550 /pub/incoming/: No such file or directory.
CWD /public/incoming/
550 /public/incoming/: No such file or directory.
CWD /anonymous/_vti_pvt/
550 /anonymous/_vti_pvt/: No such file or directory.
CWD /anonymous/incoming/
550 /anonymous/incoming/: No such file or directory.
CWD /anonymous/pub/
550 /anonymous/pub/: No such file or directory.
CWD /anonymous/public/
550 /anonymous/public/: No such file or directory.
CWD /usr/incoming/
550 /usr/incoming/: No such file or directory.
CWD / /
550 / /: No such file or directory.
221 You could at least say goodbye.
```

1. Source of Trace.

Incidents.org intrusion list archive
http://www.incidents.org/archives/intrusions/msg03421.html
http://www.incidents.org/archives/intrusions/msg03438.html

2. Detect was generated by:

The first trace was generated by Snort.
The second appears to be the logfile of the FTP server software.

3. Probability the source address was spoofed:

The second trace shows an FTP session. For the two-way communication to take place in the FTP session, the source IP could not have been spoofed.

4. Description of attack:

The attacker is scanning a range of hosts by sending an initial TCP SYN packet to port 21(FTP) on each host. When the attack tool is able to establish a connection to an FTP server, it logs in as "anonymous" and attempts to find folders that it can write files to.

5. Attack mechanism:

The attack works by sending syn packets very quickly to TCP port 21 on a large number of hosts. If any host responds with a SYN/ACK packet it would indicate that there is a service running on the specified port (most likely the FTP service).

If the TCP three-way handshake is completed the server will send a "220 ready" message. The attacker's software then

logs in using USER anonymous and PASSWORD guest@here.com. Once the attacker's software is logged into the FTP server, it attempts to change to directory names that are commonly found on public FTP sites, such as "pub", "temp", and "incoming". If the attack software is successful in entering any of these directories it then issues a MKD (Make Directory) command. This is as much as we can tell from the logfiles shown, but it is likely that if the MKD command is successful, the attack software will log that the victim host contains a public writeable ftp directory. This information can then later be used by the attacker to store or distribute applications and data.

6. Correlations:

Around this time frame, many sites reports scans originating from abo.wanadoo.fr.

The following similar activity was submitted by Ellen Clary at http://www.incidents.org/archives/intrusions/msg03440.html

Yes, it did that to us as well (they're not the only one, but it's often from them). Anyone know what this program is actually trying to upload?

>From our customized Logcheck report:

Jan 20 06:49:20 6D: ftpd[22518]: PASS Hgpuser@home.com
Jan 20 06:49:20 6D: ftpd[22518]: ANONYMOUS FTP LOGIN FROM ANancy-105-1-1-121.abo.wanadoo.fr [80.13.23.121], Hgpuser@home.com
Jan 20 06:49:21 6D: ftpd[22518]: CWD /pub/
Jan 20 06:49:22 6D: ftpd[22518]: MKD 000102155721p
Jan 20 06:49:22 7D: ftpd[22518]: <--- 550 000102155721p: Permission denied.
Jan 20 06:49:22 6D: ftpd[22518]: CWD /public/
Jan 20 06:49:22 7D: ftpd[22518]: <--- 550 /public/: No such file or directory.
Jan 20 06:49:22 6D: ftpd[22518]: CWD /pub/incoming/
Jan 20 06:49:22 7D: ftpd[22518]: <--- 550 /pub/incoming/: No such file or directory.
Jan 20 06:49:22 6D: ftpd[22518]: CWD /incoming/
Jan 20 06:49:22 7D: ftpd[22518]: <--- 550 /incoming/: No such file or directory.
Jan 20 06:49:22 6D: ftpd[22518]: CWD /_vti_pvt/
Jan 20 06:49:22 7D: ftpd[22518]: <--- 550 /_vti_pvt/: No such file or directory.
Jan 20 06:49:23 6D: ftpd[22518]: CWD /
Jan 20 06:49:23 6D: ftpd[22518]: MKD 000102155723p
Jan 20 06:49:23 7D: ftpd[22518]: <--- 550 000102155723p: Permission denied.
Jan 20 06:49:23 6D: ftpd[22518]: CWD /upload/
Jan 20 06:49:23 7D: ftpd[22518]: <--- 550 /upload/: No such file or directory.
Jan 20 06:49:23 6D: ftpd[22518]: CWD /temp/
Jan 20 06:49:23 7D: ftpd[22518]: <--- 550 /temp/: No such file or directory.
Jan 20 06:49:24 6D: ftpd[22518]: CWD /tmp/
Jan 20 06:49:24 7D: ftpd[22518]: <--- 550 /tmp/: No such file or directory.
Jan 20 06:49:24 6D: ftpd[22518]: CWD /mailroot/
Jan 20 06:49:24 7D: ftpd[22518]: <--- 550 /mailroot/: No such file or directory.
Jan 20 06:49:24 6D: ftpd[22518]: CWD /anonymous/
Jan 20 06:49:24 7D: ftpd[22518]: <--- 550 /anonymous/: No such file or directory.
Jan 20 06:49:24 6D: ftpd[22518]: CWD /_vti_log/
Jan 20 06:49:24 7D: ftpd[22518]: <--- 550 /_vti_log/: No such file or directory.

7. Evidence of active targeting:

The attackers seem to be scanning for FTP servers over many networks, so there is not evidence of active targeting.

8. Severity:

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

Criticality	4	Some of the machines scanned are critical infrastrucure (DNS, web, and mail servers)
Lethality	2	A successful attacker would be able to store files on an FTP server, but would not necessarily be able to do anything else to the server or the network.
System Countermeasures	4	The FTP sites shown in the traces did not have write access for the anonymous user.
Network Countermeasures	1	The network was not configured to block this traffic from connecting to the FTP server.
(4 + 2) - (4 + 1) = 1		

9. Defensive recommendation:

The owner of the attacked host should verify that there are no anonymous writeable FTP folders on the FTP servers. If the owner of the attacked host does not have a need to communicate with users of the French ISP wanadoo.fr, she may want to configure her firewall to block traffic from this domain.

10. Multiple choice test question:

Which of the following protocols was used by this attack?
A. TCP
B. UDP
C. TFPT
D. ICMP

Answer: A. FTP uses TCP(Transmission Control Protocol).

Detect 4

```
2001-12-19 19:21:33 MY.NET.1.2 - W3SVC1 AS-NT-WEBQUAN1 MY.NET.1.24 GET
/cfide/administrator/startstop.html 404 604 0 80 - - -
2001-12-19 19:21:33 MY.NET.1.2 - W3SVC1 AS-NT-WEBQUAN1 MY.NET.1.24 GET
/cfide/administrator/startstop.html 404 604 0 443 - - -
```

1. Source of Trace.

IIS Web log at my corporation. I was curious if there were any attacks attempted against my webserver. I wrote a script to group webserver requests by the requested URL and spit out the number of hits for a given URL. I then sorted the list with the least hits at the top. Here is what was generated:

CountOfID	Request
1	/qtweb/help/geninfo.htm
1	/qtweb/help/modlloan.htm
1	/qtweb/help/summary.htm
1	/qtweb/favicon.ico
2	/qtweb/jicustom/Glossary.asp
2	/qtweb/clearobjects.asp
2	/default.asp::$DATA
2	/cfide/administrator/startstop.html
2	/qtweb/help/acctbal.htm
2	/qtweb/help/contents.htm

2	/qtweb/help/transfer.htm

The /qtweb/ folder is the only website that this server contains. The "::$DATA" is an IIS Exploit that I am familiar with. The "/cfide/administrator/startstop.html" was a new signature I had not seen before, and it caught my attention.

2. Detect was generated by:

The detect was generated by Microsoft Internet Information Server 4.0.

3. Probability the source address was spoofed:

The IIS Web server that generated this log is in the DMZ. The address "MY.NET.1.2" is the NAT translated address of all traffic from our private network into the DMZ. The address "MY.NET.1.2" is a RFC 1918 reserved address, meaning it is not routeable on the Internet. If this packet had been inbound into the DMZ from the Internet, it would have it's real source address. It is unlikely the source address was spoofed.

4. Description of attack:

The attacker connects the the webserver and requests the file /cfide/administrator/startstop.html on both the non-secure HTTP Port (port 80), as well as the secure HTTP Port (port 443).

5. Attack mechanism:

The path /cfide/administrator/startstop.html corresponds to the Cold Fusion adminstrator utility for starting and stopping the cold fusion service. This html page contains a java application with a known vulnerability. When Advanced Security is enabled on the webserver, this start/stop utility is not password protected, and an attacker could use it to start or stop the Cold Fusion service on the webserver.

More information can be found at
http://packetstorm.widexs.nl/advisories/allaire/asb99-07.dos_cf_admin

6. Correlations:

The Cold Fusion Start/Stop utility is a well known and document vulnerability, and kind of obscure. It is scanned for by some attack tools, such as whisker, and is also detected in the snort ruleset.

I found a few other traces containing this exploit.

From http://homepage.mac.com/vm_converter/archive/undoukai/log/macosx/apache_access_log.html:

> 10.1.2.143 - - [24/Oct/2000:10:47:46 +0900] "GET /CFIDE/Administrator/startstop.html HTTP/1.0" 404 299

7. Evidence of active targeting:

Since this is a request from an internal network source to our webserver, I would say this is definetely active targeting. What the purpose for the connection attempt was, and whether it was malicious or benign is unknown. Since it is an obscure request, I would imagine that it could have been a sysadmin or some other person running some sort of security scan.

8. Severity:

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

Criticality	4	The machine being scanned is a webserver.
Lethality	2	The attacker could stop or start a web service.
System Countermeasures	5	The vulnerable program is not present on the server.
Network		The traffic was not blocked from reaching the target systems. In fact, due to the NAT

Network Countermeasures	1	done between the internal network and the DMZ, we cannot tell what the real source IP address is.
(4+2) - (5 + 1) = 0		

9. Defensive recommendation:

While there is really no risk from this event, we need to build some system by which we can monitor the source address of outbound traffic from the private network (such as putting Snort on the same network segment as the firewall's internal interface.)

10. Multiple choice test question:

The source address was an RFC 1918 address. Which of the following is not an RFC 1918 reserved address?
A. 10.10.10.1
B. 172.17.10.1
C. 198.97.10.1
D. 192.168.10.1

Answer: C. 192.97 is not one of the RFC 1918 reserved address spaces.

Detect 5

```
Jan 23 15:32:28 hostj named[276]: [ID 295310 daemon.notice] security: notice: denied query from
[212.125.148.97].2042 for "VERSION.BIND" CHAOS
Jan 23 15:32:28 hostj portsentry[318]: [ID 702911 daemon.notice] attackalert: Connect from host:
212.125.148.97/212.125.148.97 to TCP port: 513
Jan 23 15:32:31 hostmi named[411]: [ID 295310 daemon.notice] security: notice: denied query from
[212.125.148.97].2042 for "VERSION.BIND" CHAOS
Jan 23 15:32:31 hostmi portsentry[300]: [ID 702911 daemon.notice] attackalert: Connect from
host: 212.125.148.97/212.125.148.97 to TCP port: 513
```

1. Source of Trace.

Incidents.org intrusion list archive
http://www.incidents.org/archives/intrusions/msg03504.html

2. Detect was generated by:

The detect is in a Unix "Syslog" format. The first and third entries were generated by the named daemon, which provides Domain Name Service. The second and fourth entries were generated by portsentry, which is an intrusion detection system that runs on the host.

3. Probability the source address was spoofed:

It is unlikely the source address was spoofed. The first packet was a query for information, and the attacker would not have received any reply if the source address was spoofed. The second packet was a TCP connect attempt, and the attacker would not have been able to complete the connection if the source address was spoofed.

4. Description of attack:

The attacker is requests "Version BIND" from a server that is running the Domain Name Server service. She then attempts to connect to tcp port 513 on the same machine. A few seconds later, she attempts the same two activities directed at a different host. Based on the information given (and assuming there were no additional logs of attack attempts from this attacker at this site) there are a few things we can assume. The attacker appears to be running some type of automated attack tool. This is assumed because the "Version BIND" query comes at the same exact second as the attempted connection to port 513 on the same host. It also appears that the "Version BIND" query comes from the

same source UDP port (`[212.125.148.97].2042`) on each host, putting more wieght into the automated attack tool theory. We could also assume that this attacker may be scanning from a list of DNS servers, because it appears that on this network it only attacked two hosts, and both were running the named service.

5. Attack mechanism:

The purpose for the "VERSION BIND" request is for the attacker to determine if you are running a version of BIND that has a known buffer overflow vulnerability. If the request returns a response like "4.9.6-REL" or "8.2.1", then the attacker knows you have a system which can be broken into.

The purpose for the connection attempt on port 513 is likely in hopes on connecting to a running rlogin service and gain a remote shell on the victim machine.

These two vulnerabilities have been well known for quite a while, so it is unlikely there are many machines out there that are still vulnerable.

6. Correlations:

Both rlogin scans and BIND Version queries are common.

Here is a report containing a rlogin scan from http://www.incidents.org/archives/intrusions/msg01227.html

```
inetnum 211.232.0.0 - 211.255.255.255
netname KRNIC-KR
descr KRNIC
descr Korea Network Information Center
country KR
[ ISP member ORG information ]
Org Name : NOWLINK CO., LTD
Service Name : NOWLINK
Org Address : 3F YongWon-B/D 146-2 WonHyoRo-3-Ga YongSan-Gu

Jul 31 00:02:00 hostz telnetd[496]: refused connect from 211.233.151.124
Jul 31 00:02:01 hostba portsentry[585]: [ID 702911 daemon.notice] attackalert: Connect from
host: 211.233.151.124/211.233.151.124 to TCP port: 514
Jul 31 00:02:01 hostdr portsentry[353]: [ID 702911 daemon.notice] attackalert: Connect from
host: 211.233.151.124/211.233.151.124 to TCP port: 514
Jul 31 00:02:01 hostl portsentry[11156]: [ID 702911 daemon.notice] attackalert: Connect from
host: 211.233.151.124/211.233.151.124 to TCP port: 513
Jul 31 00:02:08 hostmau portsentry[223]: attackalert: Connect from host:
211.233.151.124/211.233.151.124 to TCP port: 513
Jul 31 00:02:08 hostmau snort: connect to 515 from outside: 211.233.151.124:2169 ->
z.y.w.12:515
Jul 31 00:02:08 hostmau snort: connect to 515 from outside: 211.233.151.124:2169 ->
z.y.w.12:515
Jul 31 00:02:09 hostmau snort: connect to 515 from outside: 211.233.151.124:2169 ->
z.y.w.12:515
Jul 31 00:02:11 hostmau snort: connect to 515 from outside: 211.233.151.124:2169 ->
z.y.w.12:515
Jul 31 00:02:12 hostko /kernel: Connection attempt to TCP z.y.w.21:515 from
211.233.151.124:2178
Jul 31 00:04:51 hosty portsentry[7215]: [ID 702911 daemon.notice] attackalert: Connect from
host: 211.233.151.124/211.233.151.124 to TCP port: 514
```

Here is report containing a version bind query from http://www.sans.org/y2k/022801-1100.htm

```
Server used for this query: [ whois.ripe.net ]
inetnum: 62.100.34.0 - 62.100.47.255
netname: CNCNL01
descr: XO Communications netblocks
country: NL
```

```
Feb 23 16:35:35 hostm named[5978]: security: notice: denied query from
[62.100.36.210].1035 for "version.bind"
Feb 23 16:35:35 hostm named[5978]: security: notice: denied query from
[62.100.36.210].1035 for "version.bind"
Feb 23 16:35:35 hostm snort[16556]: IDS278 - SCAN -named Version probe:
62.100.36.210:1035 -> z.y.w.98:53
Feb 23 16:43:16 hosty named[1329]: security: notice: denied query from
[62.100.36.210].1037 for "version.bind"
Feb 23 16:43:16 hosty named[1329]: security: notice: denied query from
[62.100.36.210].1037 for "version.bind"
Feb 23 16:43:16 hosty snort[80143]: IDS278 - SCAN -named Version probe:
62.100.36.210:1037 -> z.y.w.34:53
```

While "Version BIND" and rlogin scans are common, I could not find any correlations for a scan that includes only these two exploits.

7. Evidence of active targeting:

There is some evidence that there could be active targeting here. The attacker only appears to have attacked two servers on the victim's network, and both were DNS servers. There were also no other reports of similar scans by anyone else to the above list, and I could find no other reports of scans that combine only "Version BIND" and rlogin exploits.

8. Severity:

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

Criticality	5	The machines scanned are critical infrastrucure (DNS servers)
Lethality	4	Rlogin and BIND exploits can allow the attacker a remote shell on the system.
System Countermeasures	5	These vulnerabilities are well known and the servers have been configured so they are not vulnerable. Also, they are running portsentry on the system to block and report invalid connection attempts.
Network Countermeasures	1	The traffic was not blocked from reaching the target systems.
(5 + 4) - (5 + 1) = 3		

9. Defensive recommendation:

Normally I would not take any action on a Version BIND or rlogin scan, but since there may be evidence of active targeting, it would be appropriate to verify that the attacked hosts are configured correctly and not vulnerable to these exploits. You would also want to research the source of the attack and send a notice to that network's administrator alerting them to the attack.

10. Multiple choice test question:

What protocol(s) could that attacker have used to query the DNS Servers?
A. UDP
B. TCP
C. ICMP
D. Either TCP or UDP

Answer: D. DNS can use either TCP or UDP.

Assignment 3

Table of Contents

A. Executive Summary

A quick overview of my analysis process is as follows. I downloaded the data sets, and did some quick analysis of their size and contents, and then determined what tools I would use for my analysis. I wrote PERL scripts to convert the data into a format I could easily import into a Microsoft Access Database. I then used MS Access to combine, sort, and cross-reference the data in various ways to find different types of information. Before I went further analyzing the data, I determined criteria for how to rank the different alerts as high, medium, or low risk. I then used the output from MSAccess, the orginal alert files, and various websites and other resources to determine the cause of the different alerts and the risk involved.

B. Data Sets Used

The following data sets were downloaded for analysis:

Alerts	Scans	Out of Spec
alert.011222	scans.011222	oos_Dec.22.2001
alert.011223	scans.011223	oos_Dec.23.2001
alert.011224	scans.011224	oos_Dec.24.2001
alert.011225	scans.011225	oos_Dec.25.2001
alert.011226	scans.011226	oos_Dec.26.2001

This represents Snort alerts, detected scans, and Out of Spec data for the period around Christmas, 2001. I selected this period because of the likeliness that attackers may increase their activity during the holidays when systemsmay be less closely monitored.

C. Data Import

I was first interested in finding out how many different types of alerts there were in the file. I created a quick PERL script to group the alerts by the first 16 characters of the alert description and count the number of different types of alert.

```
# groupalerts.pl
# parse through Snort alert files, group alerts by the first 16 characters of the
# alert description, allowing us to count the number of different types of alert.

#!perl

@alertfiles = ("alert.011222.gz", "alert.011223.gz",
               "alert.011224.gz", "alert.011225.gz", "alert.011226.gz");

foreach $file (@alertfiles)
{

        open ALERT, $file or die " $! ";

        while ()
        {
                # match the 16 characters after the first 28
                if (m/^.{28}(.{15})/)
                {
                        $alerttypes{$1} ++;
                        $alertsample{$1} = $_;
                }
        }
}
foreach $key (sort keys %alerttypes)
{
```

```
        print $key, "\t" , $alerttypes{$key}, "\t", $alertsample{$key};
}
```

Here is the output from groupalerts.p

```
Attempted Sun R 3 12/26-17:43:16.087898 [**] Attempted Sun RPC high port access [**] 128.183.10.134:53 -> MY.NET.97.237:32771
BACKDOOR NetMet 3651 12/26-18:29:58.557759 [**] BACKDOOR NetMetro Incoming Traffic [**] 208.62.15.41:5031 -> MY.NET.60.8:23
CS WEBSERVER - 14585 12/26-23:52:23.413400 [**] CS WEBSERVER - external web traffic [**] 12.23.184.175:2121 -> MY.NET.100.165:80
DDOS mstream ha 2 12/26-19:40:12.942652 [**] DDOS mstream handler to client [**] MY.NET.97.160:15104 -> 24.78.99.154:3152
DDOS shaft clie 25 12/26-18:53:49.281348 [**] DDOS shaft client to handler [**] 24.120.161.18:3119 -> MY.NET.60.38:20432
DNS zone transf 8 12/26-06:11:51.715979 [**] DNS zone transfer [**] 208.58.66.150:64959 -> MY.NET.1.3:53
EXPLOIT x86 NOO 47 12/26-21:30:49.562235 [**] EXPLOIT x86 NOOP [**] 207.46.177.148:80 -> MY.NET.233.106:1456
EXPLOIT x86 set 11 12/26-21:17:37.325459 [**] EXPLOIT x86 setuid 0 [**] 63.240.202.64:4000 -> MY.NET.97.233:1044
EXPLOIT x86 ste 1 12/26-15:31:35.571771 [**] EXPLOIT x86 stealth noop [**] 207.199.1.201:80 -> MY.NET.111.223:1293
External FTP to 4 12/26-06:57:37.409157 [**] External FTP to HelpDesk MY.NET.83.197 [**] 65.165.14.43:4669 -> MY.NET.83.197:21
External RPC ca 1256 12/23-06:36:18.011432 [**] External RPC call [**] 208.7.170.44:111 -> MY.NET.190.253:111
FTP CWD / - pos 2 12/23-05:21:30.357569 [**] FTP CWD / - possible warez site [**] 212.62.78.56:3234 -> MY.NET.130.123:21
FTP DoS ftpd gl 209 12/26-23:46:46.422499 [**] FTP DoS ftpd globbing [**] 12.40.162.100:51482 -> MY.NET.98.236:21
FTP RETR 1MB po 1 12/25-21:16:37.747535 [**] FTP RETR 1MB possible warez site [**] 80.13.172.141:1338 -> MY.NET.130.123:21
FTP passwd atte 1 12/26-16:01:35.834090 [**] FTP passwd attempt [**] 213.213.40.179:1570 -> MY.NET.253.105:21
High port 65535 32 12/26-23:37:42.959240 [**] High port 65535 udp - possible Red Worm - traffic [**] 66.95.149.154:65535 -> MY.NET.98.158:1123
ICMP Destinatio 7033 12/26-23:52:32.882176 [**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**] 65.207.94.30 -> MY.NET.137.7
ICMP Echo Reque 11358 12/26-23:52:35.293266 [**] ICMP Echo Request BSDtype [**] 141.213.11.120 -> MY.NET.70.148
ICMP Fragment R 1286 12/26-22:19:14.458160 [**] ICMP Fragment Reassembly Time Exceeded [**] MY.NET.70.70 -> 24.131.240.18
ICMP Redirect ( 1 12/22-16:25:47.915963 [**] ICMP Redirect (Undefined Code!) [**] MY.NET.98.201 -> 208.170.46.89
ICMP Source Que 3569 12/26-23:10:26.837333 [**] ICMP Source Quench [**] 203.130.194.2 -> MY.NET.70.70
ICMP redirect ( 15 12/26-16:30:44.339269 [**] ICMP redirect (Host) [**] 195.205.247.238 -> MY.NET.70.70
ICMP traceroute 262 12/26-23:44:15.986478 [**] ICMP traceroute [**] MY.NET.97.10 -> MY.NET.16.14
IDS475/web-iis_ 5 12/23-03:31:53.089398 [**] IDS475/web-iis_web-webdav-propfind [**] 207.202.195.178:48717 -> MY.NET.60.14:80
IDS50/trojan_tr 4 12/26-23:41:26.810782 [**] IDS50/trojan_trojan-active-subseven [**] MY.NET.70.148:1243 -> 204.152.184.75:64454
INFO - Possible 206 12/26-18:21:20.229175 [**] INFO - Possible Squid Scan [**] 193.109.122.5:3957 -> MY.NET.60.39:3128
INFO - Web Cmd 16 12/26-10:51:07.853921 [**] INFO - Web Cmd completed [**] MY.NET.104.133:80 -> 12.78.153.207:1568
INFO - Web Comm 2 12/24-04:12:56.323791 [**] INFO - Web Command Error [**] MY.NET.253.125:80 -> 216.35.116.42:54362
INFO FTP anonym 529 12/26-23:48:51.499146 [**] INFO FTP anonymous FTP [**] 194.215.75.194:25949 -> MY.NET.253.105:21
INFO Inbound GN 503 12/26-23:51:55.730498 [**] INFO Inbound GNUTella Connect accept [**] MY.NET.97.170:6346 -> 64.197.199.186:1199
INFO MSN IM Cha 7580 12/26-23:52:58.348075 [**] INFO MSN IM Chat data [**] MY.NET.97.238:2236 -> 64.4.12.153:1863
INFO Napster Cl 35 12/26-22:53:13.079584 [**] INFO Napster Client Data [**] MY.NET.98.159:2069 -> 172.128.234.61:6699
INFO Outbound G 132 12/26-23:10:12.695054 [**] INFO Outbound GNUTella Connect accept [**] 24.188.141.30:6346 -> MY.NET.97.170:1266
INFO Possible I 170 12/26-23:47:02.456685 [**] INFO Possible IRC Access [**] MY.NET.97.211:1506 -> 207.68.167.253:6667
INFO napster lo 4 12/26-21:20:41.648469 [**] INFO napster login [**] MY.NET.97.186:4531 -> 207.228.250.20:8888
Incomplete Pack 425 12/26-21:11:45.781031 [**] Incomplete Packet Fragments Discarded [**] 217.230.139.154:0 -> MY.NET.178.86:0
MISC Large ICMP 10 12/26-19:26:21.496757 [**] MISC Large ICMP Packet [**] 216.190.0.240 -> MY.NET.5.44
MISC Large UDP 4327 12/26-19:46:53.971732 [**] MISC Large UDP Packet [**] 209.249.123.125:16226 -> MY.NET.70.192:2872
MISC PCAnywhere 3 12/26-21:43:12.105585 [**] MISC PCAnywhere Startup [**] 24.180.10.152:1100 -> MY.NET.87.50:5632
MISC solaris 2. 1 12/26-17:27:58.592437 [**] MISC solaris 2.5 backdoor attempt [**] 131.118.254.132:23580 -> MY.NET.60.8:23
MISC source por 13099 12/26-23:52:40.659153 [**] MISC source port 53 to <1024 [**] 204.111.1.35:53 -> MY.NET.1.5:53
MISC traceroute 25146 12/26-23:53:01.930158 [**] MISC traceroute [**] 131.94.191.102:56209 -> MY.NET.140.9:33460
NMAP TCP ping! 60 12/26-23:40:52.526477 [**] NMAP TCP ping! [**] 64.152.70.68:53 -> MY.NET.1.8:53
Null scan! [**] 180 12/26-23:49:10.610958 [**] Null scan! [**] 63.155.92.94:46763 -> MY.NET.70.70:52765
Port 55850 tcp 93 12/26-23:52:37.272497 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] MY.NET.253.125:80 -> 64.12.96.103:55850
Possible trojan 12 12/26-03:49:20.561731 [**] Possible trojan server activity [**] 203.200.145.222:27374 -> MY.NET.253.125:80
Queso fingerpri 5098 12/26-23:45:06.433383 [**] Queso fingerprint [**] 65.105.159.22:45509 -> MY.NET.6.35:25
RFB - Possible 4 12/25-23:17:13.945655 [**] RFB - Possible WinVNC - 010708-1 [**] MY.NET.70.72:5900 -> 65.1.215.95:1188
SCAN - wayboard 1 12/26-05:20:19.763779 [**] SCAN - wayboard request - allows reading of arbitrary files as http service [**] 216.35.116.77:50366 ->
MY.NET.253.125:80
SCAN FIN [**] 1 14 12/26-06:05:57.056076 [**] SCAN FIN [**] 193.109.122.5:3520 -> MY.NET.98.146:23
SCAN Proxy atte 5706 12/26-23:40:23.782027 [**] SCAN Proxy attempt [**] 204.152.186.58:3219 -> MY.NET.97.102:1080
SCAN Synscan Po 8 12/26-22:27:31.113263 [**] SCAN Synscan Portscan ID 19104 [**] 172.158.124.23:3129 -> MY.NET.178.86:1214
SCAN XMAS [**] 1 12/26-09:05:19.662852 [**] SCAN XMAS [**] 66.65.70.168:0 -> MY.NET.17.64:0
SMB Name Wildca 489 12/26-23:53:05.384573 [**] SMB Name Wildcard [**] MY.NET.223.82:137 -> MY.NET.71.222:137
SMTP chameleon 5 12/26-15:38:16.035713 [**] SMTP chameleon overflow [**] 207.171.188.102:60049 -> MY.NET.6.34:25
SMTP relaying d 436 12/26-21:23:24.867513 [**] SMTP relaying denied [**] MY.NET.6.34:25 -> 209.151.240.80:3440
SNMP public acc 8 12/26-01:06:04.957300 [**] SNMP public access [**] 24.180.202.45:65291 -> MY.NET.190.13:161
SUNRPC highport 12 12/26-06:02:01.822728 [**] SUNRPC highport access! [**] MY.NET.11.4:80 -> MY.NET.16.42:32771
SYN-FIN scan! [ 5026 12/25-22:06:27.536774 [**] SYN-FIN scan! [**] 24.0.28.234:22 -> MY.NET.186.253:22
TCP SRC and DST 330 12/26-23:06:06.956700 [**] TCP SRC and DST outside network [**] 134.192.131.220:1221 -> 169.254.22.87:2840
TELNET access [ 8 12/26-22:36:32.123263 [**] TELNET access [**] MY.NET.60.40:23 -> 151.200.10.147:2242
TELNET login in 178 12/26-23:42:54.978615 [**] TELNET login incorrect [**] MY.NET.60.39:23 -> 32.100.110.147:2037
TFTP - External 2 12/26-17:11:26.769591 [**] TFTP - External UDP connection to internal tftp server [**] 206.65.191.129:63119 -> MY.NET.98.177:69
TFTP - Internal 61 12/26-00:21:23.126112 [**] TFTP - Internal TCP connection to external tftp server [**] MY.NET.98.115:1643 -> 66.69.147.209:69
Tiny Fragments 417 12/26-20:30:39.353725 [**] Tiny Fragments - Possible Hostile Activity [**] 65.2.208.87 -> MY.NET.99.39
Virus - Possibl 15 12/26-23:18:30.827017 [**] Virus - Possible scr Worm [**] MY.NET.6.44:110 -> 65.2.55.4:50277
WEB-CGI archie 2 12/26-18:38:57.222745 [**] WEB-CGI archie access [**] 216.35.116.23:36188 -> MY.NET.253.114:80
WEB-CGI csh acc 2 12/26-22:07:09.595082 [**] WEB-CGI csh access [**] 216.35.116.43:8320 -> MY.NET.253.125:80
WEB-CGI finger 3 12/25-18:02:59.587165 [**] WEB-CGI finger access [**] 216.35.116.41:21594 -> MY.NET.100.165:80
WEB-CGI formmai 14 12/26-21:26:36.799327 [**] WEB-CGI formmail access [**] 158.252.255.163:4187 -> MY.NET.253.115:80
WEB-CGI ksh acc 1 12/26-20:18:13.526558 [**] WEB-CGI ksh access [**] 216.35.116.49:44841 -> MY.NET.60.14:80
WEB-CGI redirec 33 12/26-20:18:04.176337 [**] WEB-CGI redirect access [**] 64.231.12.33:1222 -> MY.NET.253.125:80
WEB-CGI rsh acc 9 12/26-16:46:52.652646 [**] WEB-CGI rsh access [**] 213.122.87.105:1283 -> MY.NET.6.7:80
WEB-CGI survey. 2 12/26-19:50:19.184976 [**] WEB-CGI survey.cgi access [**] 216.35.116.25:34623 -> MY.NET.253.114:80
WEB-CGI tsch ac 2 12/26-16:14:03.900309 [**] WEB-CGI tsch access [**] 216.35.116.56:53883 -> MY.NET.100.165:80
WEB-FRONTPAGE _ 33 12/26-21:29:26.194496 [**] WEB-FRONTPAGE _vti_rpc access [**] 24.180.140.132:1600 -> MY.NET.253.125:80
WEB-FRONTPAGE f 4 12/23-04:00:27.942342 [**] WEB-FRONTPAGE fpcount.exe access [**] 24.124.55.13:1268 -> MY.NET.253.125:80
WEB-FRONTPAGE s 5 12/26-15:58:10.588555 [**] WEB-FRONTPAGE shtml.exe [**] 200.255.45.64:1554 -> MY.NET.6.7:80
WEB-IIS .cnf ac 1 12/24-04:29:27.361300 [**] WEB-IIS .cnf access [**] 216.35.116.71:61970 -> MY.NET.253.125:80
```

```
WEB-IIS File pe 8 12/26-23:52:27.575976 [**] WEB-IIS File permission canonicalization [**] 194.75.172.2:17198 -> MY.NET.253.123:80
WEB-IIS Unautho 25 12/26-18:31:40.570956 [**] WEB-IIS Unauthorized IP Access Attempt [**] MY.NET.130.86:80 -> 207.32.96.53:1650
WEB-IIS _vti_in 39 12/26-21:29:26.127078 [**] WEB-IIS _vti_inf access [**] 24.180.140.132:1599 -> MY.NET.253.125:80
WEB-IIS view so 65 12/26-23:00:42.603163 [**] WEB-IIS view source via translate header [**] 202.110.57.10:28919 -> MY.NET.60.14:80
WEB-MISC /.... 4 12/22-05:20:42.213830 [**] WEB-MISC /.... [**] 64.163.214.35:2810 -> MY.NET.130.123:80
WEB-MISC 403 Fo 387 12/26-23:50:09.623783 [**] WEB-MISC 403 Forbidden [**] MY.NET.253.125:80 -> 210.7.221.22:2132
WEB-MISC Attemp 552 12/26-23:44:46.603879 [**] WEB-MISC Attempt to execute cmd [**] 194.75.172.2:15131 -> MY.NET.253.123:80
WEB-MISC Lotus 5 12/26-22:14:03.215943 [**] WEB-MISC Lotus Domino directory traversal [**] 61.187.56.10:17398 -> MY.NET.100.165:80
WEB-MISC compaq 5 12/25-21:19:16.373027 [**] WEB-MISC compaq nsight directory traversal [**] 64.118.65.6:80 -> MY.NET.98.165:2301
WEB-MISC count. 53 12/26-23:50:00.373960 [**] WEB-MISC count.cgi access [**] 200.68.172.148:1114 -> MY.NET.6.14:80
WEB-MISC guestb 2 12/26-19:00:09.274064 [**] WEB-MISC guestbook.cgi access [**] 200.182.183.106:11959 -> MY.NET.253.125:80
WEB-MISC http d 95 12/26-23:51:14.528114 [**] WEB-MISC http directory traversal [**] 203.197.249.147:33850 -> MY.NET.100.165:80
WEB-MISC prefix 7636 12/26-23:52:58.650548 [**] WEB-MISC prefix-get // [**] 203.199.220.119:1398 -> MY.NET.253.114:80
Watchlist 00022 64128 12/26-23:53:00.136315 [**] Watchlist 000222 NET-NCFC [**] 159.226.117.40:3274 -> MY.NET.253.114:80
X11 outgoing [* 1 12/25-10:04:17.479158 [**] X11 outgoing [**] 63.251.143.213:6003 -> MY.NET.98.190:2028
beetle.ucs [**] 11 12/26-21:54:15.582950 [**] beetle.ucs [**] MY.NET.70.69:21 -> 210.58.102.86:21
connect to 515 161 12/26-22:55:00.998201 [**] connect to 515 from inside [**] MY.NET.1.2:1023 -> MY.NET.50.35:515
spp_http_decode 327 12/26-23:44:42.071721 [**] spp_http_decode: IIS Unicode attack detected [**] 194.75.172.2:17198 -> MY.NET.253.123:80
spp_portscan: E 3293 12/27-00:04:49.772398 [**] spp_portscan: End of portscan from MY.NET.97.35: TOTAL time(15s) hosts(11) TCP(5) UDP(0) [**]
spp_portscan: P 3765 12/27-00:05:15.804780 [**] spp_portscan: PORTSCAN DETECTED from MY.NET.97.35 (THRESHOLD 4 connections exceeded in 24 seconds)
[**]
spp_portscan: p 58332 12/27-00:05:41.782381 [**] spp_portscan: portscan status from MY.NET.87.50: 6 connections across 5 hosts: TCP(0), UDP(6) [**]
x86 NOOP - unic 2 12/26-23:18:09.551887 [**] x86 NOOP - unicode BUFFER OVERFLOW ATTACK [**] 209.247.164.25:80 -> MY.NET.98.125:1171
```

The groupalerts.pl script outputs 101 lines, meaning there were 101 different alert types. The alert files contain about 40 MB of data. This information allows me to decide among some of my options for further analysis:

Analysis Options:

Option 1: SnortSnarf
I ran one of the logfiles through snortsnarf. It seemed that this could be an easy way to do analysis on the data. It took a really long time, and the output didn't allow me to much of the detail I would have liked.

Optioin 2: PERL
I looked at the possibility of writing PERL scritps to analyze the data. This would give me a lot of flexibility in the types of analysis I can do. But for the number of different alert types this would take a whole lot of coding to write scripts to analyze each type.

Option 3: Access Database
I finally decided on importing the alert data into an Access database, where I could use queries to group and manipulate the data.

I created the following perl script to pull the alert message, date, time, source IP, source port, destination IP, and destination port out of each alert in the files and format these fields so that they could be imported into MS Access.

```
#!perl

$outfile = "srcdestout.txt";
$errfile = "srcdesterr.txt";
open OUTFILE, ">$outfile" or die $!;
open ERRS, ">$errfile" or die $!;

# list of alert files to be imported into the database
@alertfiles = ("alert.011222.gz", "alert.011223.gz",
               "alert.011224.gz", "alert.011225.gz", "alert.011226.gz");

foreach $file (@alertfiles)
{

        open ALERT, $file or die " $! ";

        while ()
        {
                # ignore portscan messages
                next if (m/spp_portscan/i) ;
                if (m/\[\*\*\] (.*) \[\*\*\]/)
```

```
                {
                        $msg = $1;
                        if (m/(\w+\.\w+\.\w+\.\w+):?(\d*) -> (\w+\.\w+\.\w+\.\w+):?(\d*)/)
                        {
                                $srci = $1;
                                $srcp = $2;
                                $dsti = $3;
                                $dstp = $4;
                        }
                        else
                        {
                                if (m/from\s*(\w+\.\w+\.\w+\.\w+)/)
                                {
                                        $srci = $1;
                                        $srcp = "";
                                        $dsti = "";
                                        $dstp = "";
                                }
                                else
                                {
                                        $srci = $1;
                                        $srcp = "";
                                        $dsti = "";
                                        $dstp = "";
                                        print "IPNM: " , $_;
                                }
                        }

                        if (m/^12\/(\d\d)-(\d\d:\d\d:\d\d)\.(\d\d\d\d\d\d)/)
                        {
                                $day = $1;
                                $time = $2;
                                $ms = $3;
                                $date = "12/$day/2001";
                        }
                        else
                        {
                                print "DTNM: " , $_;
                                $day = "";
                                $time = "";
                                $ms = "";
                                $date = "";
                        }
                print OUTFILE $date , "\t", $time, "\t", $ms, "\t", $srci,
                        "\t", $srcp, "\t", $dsti, "\t", $dstp, "\t", $msg, "\n";
                }
                else
                {
                        print ERRS "NM: " ,$_;
                }
        }
}

close ERRS;
close OUTFILE;
```

Here an an excerpt from the output of this script:

```
12/22/2001 00:01:08 440925 137.145.206.101 35643 MY.NET.140.9 33485 MISC traceroute
12/22/2001 00:01:10 701989 MY.NET.98.149 1187 64.4.12.180 1863 INFO MSN IM Chat data
12/22/2001 00:01:12 678676 138.26.220.46 39133 MY.NET.140.9 33459 MISC traceroute
12/22/2001 00:01:15 890647 212.66.147.58 53 MY.NET.130.122 53 MISC source port 53 to <1024
12/22/2001 00:01:16 922301 209.179.179.18 53 MY.NET.1.3 53 MISC source port 53 to <1024
12/22/2001 00:01:20 063985 192.80.43.21 MY.NET.140.9 ICMP Destination Unreachable (Communication Administratively Prohibited)
12/22/2001 00:01:22 697210 138.26.220.46 39133 MY.NET.140.9 33461 MISC traceroute
12/22/2001 00:01:25 313775 137.78.21.22 38277 MY.NET.140.9 33475 MISC traceroute
12/22/2001 00:01:28 181787 132.198.101.254 46749 MY.NET.140.9 33465 MISC traceroute
12/22/2001 00:01:34 503143 MY.NET.98.149 1187 64.4.12.180 1863 INFO MSN IM Chat data
```

```
12/22/2001 00:01:37 846929 141.161.61.81 39452 MY.NET.140.9 33451 MISC traceroute
12/22/2001 00:01:38 196021 132.198.101.254 46749 MY.NET.140.9 33467 MISC traceroute
```

This tab-delimited text is then imported into MS Access.

The same process was used for importing the scan alert logfiles.

D. Data Analysis

D.1. Risk Determination Criteria

In Access, we can group the alerts by the alert message and count the number of occurrences.

Alert Message	Number of Occurrences
Attempted Sun RPC high port access	3
BACKDOOR NetMetro File List	3586
BACKDOOR NetMetro Incoming Traffic	65
beetle.ucs	11
connect to 515 from inside	51
connect to 515 from outside	110
CS WEBSERVER - external ftp traffic	91
CS WEBSERVER - external web traffic	14494
DDOS mstream handler to client	2
DDOS shaft client to handler	25
DNS zone transfer	8
EXPLOIT x86 NOOP	47
EXPLOIT x86 setgid 0	6
EXPLOIT x86 setuid 0	5
EXPLOIT x86 stealth noop	1
External FTP to HelpDesk MY.NET.70.49	2
External FTP to HelpDesk MY.NET.70.50	1
External FTP to HelpDesk MY.NET.83.197	1
External RPC call	1256
FTP CWD / - possible warez site	2
FTP DoS ftpd globbing	209
FTP passwd attempt	1
FTP RETR 1MB possible warez site	1
High port 65535 tcp - possible Red Worm - traffic	20
High port 65535 udp - possible Red Worm - traffic	12
ICMP Destination Unreachable (Communication Administratively Prohibited)	3599
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	53
ICMP Destination Unreachable (Host Unreachable)	2707
ICMP Destination Unreachable (Network Unreachable)	4
ICMP Destination Unreachable (Protocol Unreachable)	670
ICMP Echo Request BSDtype	9533
ICMP Echo Request CyberKit 2.2 Windows	95
ICMP Echo Request L3retriever Ping	23
ICMP Echo Request Nmap or HPING2	975
ICMP Echo Request Sun Solaris	475
ICMP Echo Request Windows	257

ICMP Fragment Reassembly Time Exceeded	1286
ICMP redirect (Host)	15
ICMP Redirect (Undefined Code!)	1
ICMP Source Quench	3569
ICMP traceroute	262
IDS475/web-iis_web-webdav-propfind	5
IDS50/trojan_trojan-active-subseven	4
Incomplete Packet Fragments Discarded	425
INFO - Possible Squid Scan	206
INFO - Web Cmd completed	16
INFO - Web Command Error	2
INFO FTP anonymous FTP	529
INFO Inbound GNUTella Connect accept	469
INFO Inbound GNUTella Connect request	34
INFO MSN IM Chat data	7580
INFO Napster Client Data	35
INFO napster login	4
INFO Outbound GNUTella Connect accept	132
INFO Possible IRC Access	170
MISC Large ICMP Packet	10
MISC Large UDP Packet	4327
MISC PCAnywhere Startup	3
MISC solaris 2.5 backdoor attempt	1
MISC source port 53 to <1024	13099
MISC traceroute	25146
NMAP TCP ping!	60
Null scan!	180
Port 55850 tcp - Possible myserver activity - ref. 010313-1	93
Possible trojan server activity	12
Queso fingerprint	5098
RFB - Possible WinVNC - 010708-1	4
SCAN - wayboard request - allows reading of arbitrary files as http service	1
SCAN FIN	14
SCAN Proxy attempt	5706
SCAN Synscan Portscan ID 19104	8
SCAN XMAS	1
SMB Name Wildcard	489
SMTP chameleon overflow	5
SMTP relaying denied	436
SNMP public access	8
spp_http_decode: CGI Null Byte attack detected	4
spp_http_decode: IIS Unicode attack detected	323
SUNRPC highport access!	12
SYN-FIN scan!	5026
TCP SRC and DST outside network	330
TELNET access	8
TELNET login incorrect	178
TFTP - External UDP connection to internal tftp server	2

TFTP - Internal TCP connection to external tftp server	61
Tiny Fragments - Possible Hostile Activity	417
Virus - Possible MyRomeo Worm	3
Virus - Possible scr Worm	12
Watchlist 000220 IL-ISDNNET-990517	62200
Watchlist 000222 NET-NCFC	1928
WEB-CGI archie access	2
WEB-CGI csh access	2
WEB-CGI finger access	3
WEB-CGI formmail access	14
WEB-CGI ksh access	1
WEB-CGI redirect access	33
WEB-CGI rsh access	9
WEB-CGI survey.cgi access	2
WEB-CGI tsch access	2
WEB-FRONTPAGE _vti_rpc access	33
WEB-FRONTPAGE fpcount.exe access	4
WEB-FRONTPAGE shtml.exe	5
WEB-IIS .cnf access	1
WEB-IIS _vti_inf access	39
WEB-IIS File permission canonicalization	8
WEB-IIS Unauthorized IP Access Attempt	25
WEB-IIS view source via translate header	65
WEB-MISC /....	4
WEB-MISC 403 Forbidden	387
WEB-MISC Attempt to execute cmd	552
WEB-MISC compaq nsight directory traversal	5
WEB-MISC count.cgi access	53
WEB-MISC guestbook.cgi access	2
WEB-MISC http directory traversal	95
WEB-MISC Lotus Domino directory traversal	5
WEB-MISC prefix-get //	7636
X11 outgoing	1
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	2

To allow me to choose which alerts I am going to analyze more in-depth, I then defined criteria for determining the severity of the attack.

High Risk	Medium Risk	Low Risk
Evidence of possible successful infection or intrusion Internally originated scans or exploit attempts Evidence of targeting Multiple types of attacks from one host.	Use of non-secure protocols on public network Evidence of mis-configured devices Successful Reconaissance	Normal file sharing traffic IRC Externally originated scans or exploit attempts with no evidence of success or targeting. Network management tools (ping, traceroute, snmp) Likely false alerts (i.e. normal traffic that happens to use an ephemeral port of a hacker tool)

So now we would like to flag all the high risk alerts. First we will look at the alerts themselves for evidence of successful infection or intrustion (The first category of High Risk Alerts from the chart above.)

To determine if the alert is a false positive, I look at alert in the table above and find the snort rule that generated it. Then I find some examples of the alert in the logfile, and see why the alert was generated. This allowed me to exclude "false" alerts quickly.

For example, the two alerts:
Port 55850 tcp - Possible myserver activity - ref. 010313-1
IDS50/trojan_trojan-active-subseven

By looking at the snort rules, we can see that both trigger when there is traffic detected on a certain ephemeral port, port 5580 for myserver and port 1243 for subseven. From that standpoint, both of these alerts would have the same risk.

However, if we look at one of the log entries containing each of these alerts:

```
12/26/2001 23:39:50 962395 64.12.96.166 55850 MY.NET.6.7 80 Port 55850 tcp - Possible myserver
activity - ref. 010313-1
12/26/2001 22:30:31 452106 MY.NET.70.148 1243 204.152.184.75 56442 IDS50/trojan_trojan-active-
subseven
```

We can see that the "Possible myserver activity" connects to port 80, so this is most likely a web request with the ephemeral port 55850 on the client. I would rate this as a "low" risk.
On the other hand, the "trojan-active-subseven" alert communicates between ports 1243 and 56442. Since neither of these are well known services, and one of them is a known port for the trojan subseven, I would rate this a "high" risk.

I do realize that this logic is not foolproof, an attacker could try to mask their activities by using well known service ports as the source ports for attacks. If these logs were from a corporation or government institution, rather than a University, I would likely research these alerts further before categorizing them as a low risk.

This was the type of process I used to parse through the entire list of alerts, rating the risk of each one and adding additional comments where I felt necessary. My results are in the chart below:

D.2 Risk Determination of All Alerts

Alert Message	Number of attacks	Risk	Notes
Watchlist 000220 IL-ISDNNET-990517	62200	Low	KAZAA port 1214, 6346 - GNUTELLA-SVC,
Watchlist 000222 NET-NCFC	1928	Low	Web Traffic
MISC traceroute	25146	Low	Network utility, reconaissance
MISC source port 53 to <1024	13099	Low	DNS Zone Xfer
MISC Large UDP Packet	4327	High	Looks like file transfer on strange UDP Ports
MISC Large ICMP Packet	10	?	MTU Discovery
MISC PCAnywhere Startup	3	Low	A PC Anywhere client was booted, and scanned the network for live PC Anywhere hosts to connect to. Misconfigured PC Anywhere hosts or hosts with easily guessible passwords can be compromised.
MISC solaris 2.5 backdoor attempt	1	Medium	Targeted?
ICMP Echo Request BSDtype	9533	Low	
ICMP Destination Unreachable (Communication Administratively Prohibited)	3599	Medium	Network utility, reconaissance
ICMP Source Quench	3569	Low	
ICMP Destination Unreachable (Host Unreachable)	2707	Medium	Network utility, reconaissance
ICMP Fragment Reassembly Time Exceeded	1286	Medium	
ICMP Echo Request Nmap or HPING2	975	Low	Network utility, reconaissance

ICMP Destination Unreachable (Protocol Unreachable)	670	Medium	
ICMP Echo Request Sun Solaris	475	Low	Network utility, reconaissance
ICMP traceroute	262	Low	Network utility, reconaissance
ICMP Echo Request Windows	257	Low	Network utility, reconaissance
ICMP Echo Request CyberKit 2.2 Windows	95	Low	Tool for network management
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	53	Low	
ICMP Echo Request L3retriever Ping	23	Low	
ICMP redirect (Host)	15	Low	
ICMP Destination Unreachable (Network Unreachable)	4	Low	
ICMP Redirect (Undefined Code!)	1	Medium	Crafted packet?
CS WEBSERVER - external web traffic	14494	Low	
CS WEBSERVER - external ftp traffic	91	Low	
INFO MSN IM Chat data	7580	Low	chat allowed
INFO FTP anonymous FTP	529	Low	ananymous ftp allowed
INFO Inbound GNUTella Connect accept	469	Low	GNUtella allowed
INFO - Possible Squid Scan	206	High	Targeted
INFO Possible IRC Access	170	Medium	
INFO Outbound GNUTella Connect accept	132	Low	File Sharing
INFO Napster Client Data	35	Low	File Sharing
INFO Inbound GNUTella Connect request	34	Low	
INFO - Web Cmd completed	16	High	"Command Completed"
INFO napster login	4	Low	File Sharing
INFO - Web Command Error	2	Low	Invalid file name
WEB-MISC prefix-get //	7636	Low	Attempt to exploit vulnerability in web server software.
WEB-MISC Attempt to execute cmd	552	Low	Attempt to exploit vulnerability in web server software.
WEB-MISC 403 Forbidden	387	Low	Normal web traffic, various source and destination addresses
WEB-MISC http directory traversal	95	Medium	Could be by design or could ba a misconfigure server.
WEB-MISC count.cgi access	53	Low	Attempt to exploit vulnerability in web server software.
WEB-MISC Lotus Domino directory traversal	5	Medium	Obscure attack, targeted?
WEB-MISC compaq nsight directory traversal	5	Medium	Obscure attack, targeted?
WEB-MISC /....	4	Medium	
WEB-MISC guestbook.cgi access	2	Medium	Obscure attack, targeted?
SCAN Proxy attempt	5706	Medium	Large scale proxy scan, targeted?
SCAN FIN	14	Medium	Successful reconaissance
SCAN Synscan Portscan ID 19104	8	Low	
SCAN - wayboard request - allows reading of arbitrary files as http service	1	Low	
SCAN XMAS	1	Medium	Successful reconaissance
Queso fingerprint	5098	Meduim	Successful reconaissance
SYN-FIN scan!	5026	Medium	Successful reconaissance
BACKDOOR NetMetro File List	3586	Low	FTP Traffic on suspicious ephemeral port
BACKDOOR NetMetro Incoming Traffic	65	Low	Telnet traffic on suspicious ephemeral port
External RPC call	1256	Medium	Large scale RPC scan
External FTP to HelpDesk MY.NET.70.49	2	Low	
External FTP to HelpDesk MY.NET.83.197	1	Low	
External FTP to HelpDesk	1	Low	

MY.NET.70.50	1	Low	
SMB Name Wildcard	489	Low	
SMTP relaying denied	436	Low	Someone tried to relay mail through a local server and it was blocked.
SMTP chameleon overflow	5	Low	Exploit attempt with no evidence of success
Incomplete Packet Fragments Discarded	425	Low	
Tiny Fragments - Possible Hostile Activity	417	High	Tiny Fragments mixed in with a null scan to one host
TCP SRC and DST outside network	330	High	Misconfigured hardware or crafted packets, possibly hiding a scan
spp_http_decode: IIS Unicode attack detected	323	low	
spp_http_decode: CGI Null Byte attack detected	4	low	
FTP DoS ftpd globbing	209	low	
FTP CWD / - possible warez site	2	low	
FTP passwd attempt	1	low	
FTP RETR 1MB possible warez site	1	low	
TELNET login incorrect	178	High	> 100 incorrect logins from one host
TELNET access	8	Medium	Telnet is not secure.
Null scan!	180	Medium	Targeted?
connect to 515 from outside	110	Medium	LPD Exploit
connect to 515 from inside	51	Medium	
WEB-IIS view source via translate header	65	Low	Exploit attempt with no evidence of success
WEB-IIS _vti_inf access	39	Low	Exploit attempt with no evidence of success
WEB-IIS Unauthorized IP Access Attempt	25	Low	Blocked access
WEB-IIS File permission canonicalization	8	Low	Exploit attempt with no evidence of success
WEB-IIS .cnf access	1	Low	Exploit attempt with no evidence of success
Port 55850 tcp - Possible myserver activity - ref. 010313-1	93	Low	Web traffic on suspicious ephemeral port
WEB-CGI redirect access	33	Low	Exploit attempt with no evidence of success
WEB-CGI formmail access	14	Low	Exploit attempt with no evidence of success
WEB-CGI rsh access	9	Low	Exploit attempt with no evidence of success
WEB-CGI finger access	3	Low	Exploit attempt with no evidence of success
WEB-CGI csh access	2	Low	Exploit attempt with no evidence of success
WEB-CGI survey.cgi access	2	Low	Exploit attempt with no evidence of success
WEB-CGI archie access	2	Low	Exploit attempt with no evidence of success
WEB-CGI tsch access	2	Low	Exploit attempt with no evidence of success
WEB-CGI ksh access	1	Low	Exploit attempt with no evidence of success
TFTP - Internal TCP connection to external tftp server	61	High	
TFTP - External UDP connection to internal tftp server	2	High	
NMAP TCP ping!	60	Medium	Successful reconaissance
EXPLOIT x86 NOOP	47	Low	Exploit attempt with no evidence of success
EXPLOIT x86 setgid 0	6	Low	Exploit attempt with no evidence of success
EXPLOIT x86 setuid 0	5	Low	Exploit attempt with no evidence of success
EXPLOIT x86 stealth noop	1	Low	Exploit attempt with no evidence of success
WEB-FRONTPAGE _vti_rpc access	33	Low	Exploit attempt with no evidence of success
WEB-FRONTPAGE shtml.exe	5	Low	Exploit attempt with no evidence of success
WEB-FRONTPAGE fpcount.exe access	4	Low	Exploit attempt with no evidence of success
High port 65535 tcp - possible Red Worm - traffic	20	High	
High port 65535 udp - possible Red Worm - traffic	12	High	
DDOS shaft client to handler	25	High	
DDOS mstream handler to client	2	High	
beetle.ucs	11	?	

IDS475/web-iis_web-webdav-propfind	5	Low	Exploit attempt with no evidence of success
IDS50/trojan_trojan-active-subseven	4	High	Two ephemeral ports, one subseven
Virus - Possible scr Worm	12	Medium	Pop traffic, Email containing ".scr" extension
Virus - Possible MyRomeo Worm	3	Medium	Pop traffic, Email containing "I Love You"
Possible trojan server activity	12	High	Mostly web traffic on ephemeral port, except one packet
SUNRPC highport access!	12	Low	Web traffic on suspicious ephemeral port
DNS zone transfer	8	Low	
SNMP public access	8	Low	
RFB - Possible WinVNC - 010708-1	4	Medium	Remote administration tool
Attempted Sun RPC high port access	3	Low	DNS on suspicious ephemeral port
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	2	Low	
X11 outgoing	1	Low	

D.3 Risk Determination of traffic with an internal source

The next criteria for High Risk Alerts is "Internally originated scans or exploit attempts". The following chart shows alerts with an internal source address. I have highlighted traffic that could indicate infected machines on the internal network or people on the internatl network using "hacker" tools to attack external sites.

Message	CountOfID
BACKDOOR NetMetro File List	**3586**
beetle.ucs	7
connect to 515 from inside	51
DDOS mstream handler to client	**2**
High port 65535 tcp - possible Red Worm - traffic	**11**
High port 65535 udp - possible Red Worm - traffic	**3**
ICMP Destination Unreachable (Communication Administratively Prohibited)	117
ICMP Destination Unreachable (Protocol Unreachable)	626
ICMP Echo Request BSDtype	1770
ICMP Echo Request CyberKit 2.2 Windows	95
ICMP Echo Request L3retriever Ping	23
ICMP Echo Request Nmap or HPING2	**974**
ICMP Echo Request Sun Solaris	35
ICMP Echo Request Windows	246
ICMP Fragment Reassembly Time Exceeded	1282
ICMP Redirect (Undefined Code!)	1
ICMP Source Quench	3495
ICMP traceroute	228
IDS50/trojan_trojan-active-subseven	**4**
INFO - Web Cmd completed	16
INFO - Web Command Error	2
INFO Inbound GNUTella Connect accept	469
INFO MSN IM Chat data	4576
INFO Napster Client Data	32
INFO napster login	4
INFO Possible IRC Access	170
Port 55850 tcp - Possible myserver activity - ref. 010313-1	**59**
Possible trojan server activity	**8**
RFB - Possible WinVNC - 010708-1	3
SMB Name Wildcard	256
SMTP relaying denied	**436**
spp_http_decode: IIS Unicode attack detected	**16**
SUNRPC highport access!	7
TELNET access	8
TELNET login incorrect	**178**
TFTP - Internal TCP connection to external tftp server	**61**
Virus - Possible MyRomeo Worm	3
Virus - Possible scr Worm	12

WEB-IIS Unauthorized IP Access Attempt	25
WEB-MISC 403 Forbidden	387

D.4 Most Attacked Host

D.4.1 Most Attacked Hosts by Number of Alerts

The following chart shows the top 25 destination addresses that were most prevalent in the alert file. The number of alerts destined for each host is also shown.

Destination Address	Number of alerts
MY.NET.70.70	62579
MY.NET.140.9	26232
MY.NET.100.165	15316
MY.NET.253.114	9107
MY.NET.70.148	8208
MY.NET.1.3	5236
MY.NET.98.177	4642
MY.NET.153.210	4492
MY.NET.1.5	3770
209.49.12.32	3586
MY.NET.1.4	3477
MY.NET.137.7	3397
24.180.204.24	1757
MY.NET.253.105	840
149.1.1.1	772
62.238.37.227	614
MY.NET.99.39	585
MY.NET.70.11	496
MY.NET.1.2	399
MY.NET.98.187	388
MY.NET.98.202	380
64.4.12.190	332
MY.NET.217.126	319
MY.NET.217.70	287
64.4.12.183	281

D.4.2 Most Attacked Hosts by Types of Alerts

The following chart shows the top 25 destination addresses that had the largest number of different alert messages in the alert file. The number of different types of alerts is also shown.

Destination Address	Number of Alert Types
MY.NET.253.125	20
MY.NET.100.165	18

MY.NET.253.114	13
MY.NET.6.7	13
MY.NET.60.14	11
MY.NET.70.70	11
MY.NET.70.148	10
MY.NET.60.11	10
MY.NET.60.8	9
MY.NET.130.123	8
MY.NET.5.96	8
MY.NET.137.7	6
MY.NET.132.135	6
MY.NET.98.177	6
MY.NET.5.45	6
MY.NET.5.44	6
MY.NET.60.16	6
MY.NET.135.224	5
MY.NET.132.96	5
MY.NET.178.86	5
MY.NET.1.3	5
MY.NET.132.109	5
MY.NET.133.179	5
MY.NET.134.26	5
MY.NET.1.8	5

D.5 Most Active Attacker

D.5.1 Most Active Attacker by number of alerts

The following table shows the source IP which generated the most alert messages. The number of alert messages is also shown.

Source Address	Number of alerts
212.179.35.118	61327
24.0.28.234	5027
206.65.191.129	4908
65.165.14.43	4668
MY.NET.60.11	3645
MY.NET.5.13	3495
128.223.4.21	2914
141.213.11.120	2807
65.207.94.30	2785
61.219.53.135	2361
147.46.59.144	2277
216.106.172.149	2130

MY.NET.60.39	1779
63.146.1.33	1241
MY.NET.87.50	1142
159.226.61.68	888
159.226.116.140	820
160.36.56.17	788
210.183.232.26	624
MY.NET.5.75	604
61.129.52.125	595
138.26.220.46	477
211.137.65.157	477
128.114.129.62	473
152.1.14.3	472

D.5.2 Most Active Attacker by different types of alerts

The following table shows the Source Addresses that generated the larges number of different alert messages. The number of different types of alerts is also shown.

Source Address	Number of Alert Types
64.12.96.170	5
205.188.209.106	4
203.252.62.50	4
24.4.252.28	4
204.152.184.75	4
24.180.238.51	4
MY.NET.98.112	4
MY.NET.98.201	4
MY.NET.98.132	4
MY.NET.98.173	4
MY.NET.6.7	4
MY.NET.253.125	4
MY.NET.98.149	4
MY.NET.98.148	4
MY.NET.97.192	4
MY.NET.60.39	4
MY.NET.97.186	4
159.226.116.140	3
133.5.165.24	3
61.11.16.86	3
194.75.172.2	3
213.33.140.176	3
203.197.119.102	3

128.223.4.21	3
24.180.196.26	3

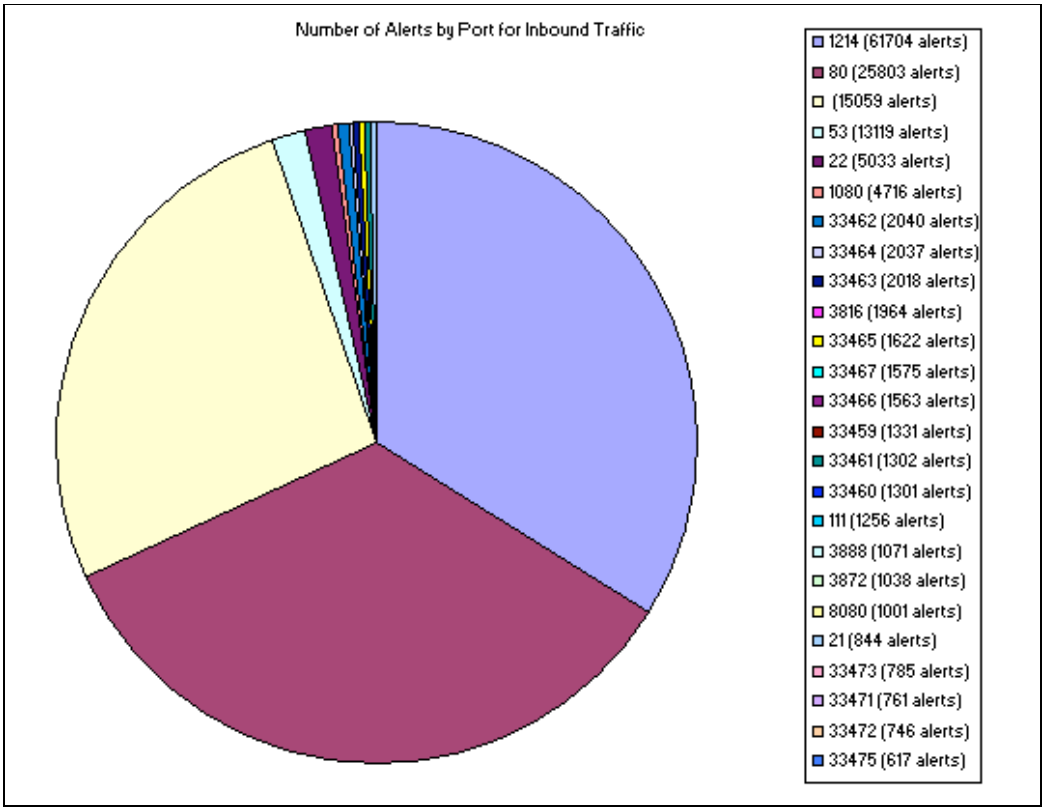
D.6 Most Active Ports

D.6.1 Most active destination ports for incoming traffic

The following table shows the top 25 destination ports for incoming traffic. The number of alerts for that port is also shown.

Most attacked port for inbound traffic	
DestPort	CountOfID
1214	61704
80	25803
	15059
53	13119
22	5033
1080	4716
33462	2040
33464	2037
33463	2018
3816	1964
33465	1622
33467	1575
33466	1563
33459	1331
33461	1302
33460	1301
111	1256
3888	1071
3872	1038
8080	1001
21	844
33473	785
33471	761
33472	746
33475	617

D.6.2 Graph of most active destination ports for incoming traffic



We can see that after alerts with no port, Oubound traffic for port 1214 generated the most alerts. Most alerts with packets destined for port 1214 have the following signature. We can attribute this traffic to KAZAA, a file sharing application.

```
12/23/2001 09:01:02 503226 212.179.45.68 4335 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
12/23/2001 09:01:02 510902 212.179.45.68 4335 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
12/23/2001 09:01:02 518765 212.179.45.68 4335 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
```

Next up was port 80, which is web traffic. These alerts are probably due to worm virus scanning.

```
12/23/2001 08:15:28 707586 141.152.140.115 65363 MY.NET.253.114 80 WEB-MISC prefix-get //
12/23/2001 08:15:28 766606 141.152.140.115 64745 MY.NET.253.114 80 WEB-MISC prefix-get //
12/23/2001 08:15:29 066299 141.152.140.115 64591 MY.NET.253.114 80 WEB-MISC prefix-get //
```

Next was port 53. Most signatures matched the following, and were likely DNS traffic between DNS servers.

```
12/26/2001 07:31:31 918256 133.163.161.1 53 MY.NET.1.3 53 MISC source port 53 to <1024
12/26/2001 07:31:32 063922 133.163.161.1 53 MY.NET.1.3 53 MISC source port 53 to <1024
```

Next was port 22. Most of this traffic can be attributed to the following SYN-FIN Scan

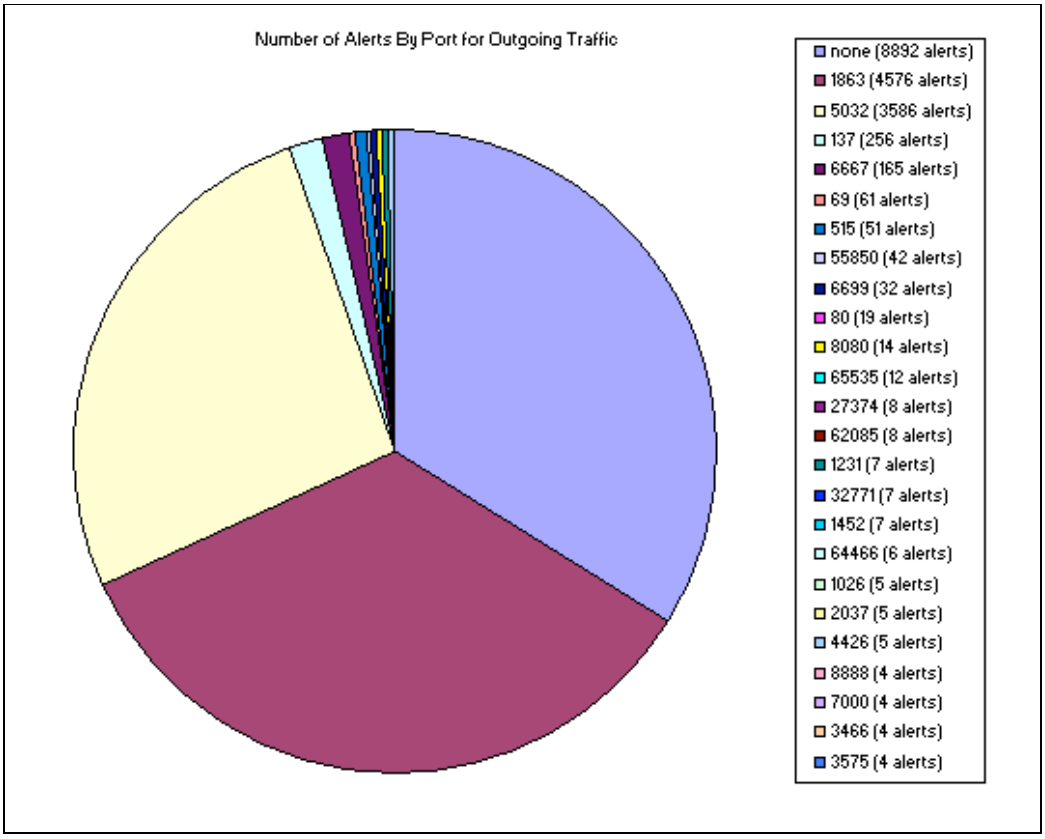
```
12/25/2001 21:50:38 906742 24.0.28.234 22 MY.NET.1.2 22 SYN-FIN scan!
12/25/2001 21:50:38 917032 24.0.28.234 22 MY.NET.1.3 22 SYN-FIN scan!
12/25/2001 21:50:39 022775 24.0.28.234 22 MY.NET.1.8 22 SYN-FIN scan!
12/25/2001 21:50:39 027212 24.0.28.234 22 MY.NET.1.9 22 SYN-FIN scan!
```

D.6.3 Most active destination ports for outbound traffic

The following table shows the top 25 destination ports for outbound alerts. The number of alerts for each destination port is also shown.

Destination Port	Number of Alerts
	8892
1863	4576
5032	3586
137	256
6667	165
69	61
515	51
55850	42
6699	32
80	19
8080	14
65535	12
27374	8
62085	8
1231	7
32771	7
1452	7
64466	6
1026	5
2037	5
4426	5
8888	4
7000	4
3466	4
3575	4

D.6.4 Graph of most active destination ports for outboud traffic



We can see that after alerts with no port, Oubound traffic for port 1863 generated the most alerts. We can see from the following alerts that port 1863 corresponds to MSN Chat data.

```
12/24/2001 03:01:55 704200 MY.NET.98.149 1185 64.4.12.173 1863 INFO MSN IM Chat data
12/24/2001 03:01:56 363309 64.4.12.173 1863 MY.NET.98.149 1185 INFO MSN IM Chat data
```

Next up was port 5032. This corresponds to the alerts for the "NetMetro File List" backdoor.

```
12/25/2001 10:03:49 409781 MY.NET.60.11 20 209.49.12.32 5032 BACKDOOR NetMetro File List
12/25/2001 10:03:49 418539 MY.NET.60.11 20 209.49.12.32 5032 BACKDOOR NetMetro File List
12/25/2001 10:03:49 425169 MY.NET.60.11 20 209.49.12.32 5032 BACKDOOR NetMetro File List
12/25/2001 10:03:49 426399 MY.NET.60.11 20 209.49.12.32 5032 BACKDOOR NetMetro File List
```

Next was port 137. This corresponds to the "SMB Name Wildcard" alert.

```
12/26/2001 22:04:37 656868 130.38.20.34 137 MY.NET.132.116 137 SMB Name Wildcard
```

Next was port 6667, which corresponds to IRC Chat

```
12/22/2001 01:20:04 366216 MY.NET.98.184 1124 64.161.193.221 6667 INFO Possible IRC Access
12/22/2001 01:20:07 520954 MY.NET.98.184 1124 64.161.193.221 6667 INFO Possible IRC Access
```

D.7 Port Scan Analysis

D.7.1 Portscan alerts per source IP

Source IP	Total portscan alerts for this source
MY.NET.87.50	281742

MY.NET.98.203	27085
211.248.231.10	9876
65.165.14.43	9508
210.77.145.30	7952
210.58.102.86	7680
204.152.184.75	5483
24.44.21.206	5412
24.0.28.234	5072
MY.NET.84.185	3712
206.65.191.129	3652
64.51.148.229	2853
MY.NET.60.38	2625
MY.NET.97.186	2330
MY.NET.97.213	2113
MY.NET.98.120	2061
MY.NET.98.138	1992
MY.NET.98.244	1740
MY.NET.98.115	1738
MY.NET.97.237	1693
MY.NET.253.24	1692
192.87.154.59	1668

D.7.2 Number of destinations per source IP

Source IP Address	Number of destination IPs scanned by this source
MY.NET.87.50	36854
210.77.145.30	7952
210.58.102.86	7674
211.248.231.10	7075
65.165.14.43	5740
24.0.28.234	5031
24.44.21.206	3865
64.51.148.229	2473
192.87.154.59	1668
MY.NET.97.186	1207
131.95.97.8	981
MY.NET.98.115	824
MY.NET.98.138	750
MY.NET.98.120	629
MY.NET.97.213	521
MY.NET.100.230	516
209.185.214.9	449

MY.NET.253.24	447
MY.NET.98.133	426
MY.NET.97.242	400
MY.NET.97.236	372

D.7.3 Portscan alerts per destination IP

Destination IP	Total portscan alerts for this destination
24.164.41.210	17610
216.33.98.254	11066
194.251.249.182	7144
MY.NET.70.148	5875
24.157.184.117	4927
24.197.48.74	4428
24.254.241.95	3657
MY.NET.98.177	3453
24.23.140.185	3224
67.165.163.5	2658
24.203.36.254	2640
24.100.50.113	2548
168.73.245.58	2433
24.47.72.191	2350
65.8.111.91	2288
194.251.249.169	2224
194.251.249.189	2223
64.53.16.160	2058
64.223.211.136	2031
80.128.175.234	2002
209.205.178.3	1963
24.180.10.152	1946
63.199.104.237	1869

D.7.4 Number of sources per destination IP

Destination IP	Number of source IP's that scanned this destination
MY.NET.178.86	109
MY.NET.150.133	84
MY.NET.99.39	58
MY.NET.70.70	40
MY.NET.17.64	22
MY.NET.100.236	21
MY.NET.253.114	13
MY.NET.60.8	11

MY.NET.115.115	10
63.240.202.138	10
MY.NET.60.11	9
MY.NET.53.42	9
MY.NET.253.125	9
63.240.202.131	9

D.7.5 Number of portscan alerts with the same source and destination address

Source IP	Destination IP	Number of portscan alerts
MY.NET.87.50	24.164.41.210	17610
MY.NET.98.203	216.33.98.254	11066
MY.NET.98.203	194.251.249.182	7144
204.152.184.75	MY.NET.70.148	5483
MY.NET.87.50	24.157.184.117	4927
MY.NET.98.203	24.197.48.74	4428
MY.NET.87.50	24.254.241.95	3657
206.65.191.129	MY.NET.98.177	3379
MY.NET.87.50	24.23.140.185	3224
MY.NET.87.50	67.165.163.5	2658
MY.NET.87.50	24.203.36.254	2640
MY.NET.87.50	24.100.50.113	2548
MY.NET.60.38	168.73.245.58	2433
MY.NET.87.50	24.47.72.191	2350
MY.NET.87.50	65.8.111.91	2288
MY.NET.98.203	194.251.249.169	2224
MY.NET.98.203	194.251.249.189	2223
MY.NET.87.50	64.53.16.160	2058
MY.NET.87.50	64.223.211.136	2031
MY.NET.87.50	80.128.175.234	2002

D.7.6 Number of unique ports scanned per source IP

Source IP	**Unique Ports Scanned**
MY.NET.87.50	13801
204.152.184.75	3146
MY.NET.60.38	2592
206.65.191.129	1423
203.231.232.213	273
129.128.5.191	258
61.132.222.12	185
MY.NET.84.185	163
MY.NET.100.158	153

62.243.72.50	133
216.106.173.144	126
MY.NET.98.176	112
MY.NET.98.163	105
216.106.173.146	102

D.7.7 Portscan Analysis Summary

From the information above, we can gather some information about the "Top Talkers" and "Top Targets" in terms of portscans.

The host "MY.NET.87.50" was the top talker for the number of alerts genereated by each source, the number of destination IPs scanned by each source, and the number of unique ports scanned by each host. Since this server is on the internal network, this is definetely something that should be looked into further.

As for destination IP's, the most portscan alerts were targeted at 24.164.41.210 and 216.33.98.254, and there were very few "MY.NET" addresses in the list of top destinations. This seems to indicate that overall there is more scanning outbound from this network than scanning of this network by outside addresses.

The address "MY.NET.178.86" was scanned by 109 different hosts, which was the most any host received.

Looking at the table of alerts with the same source and destination IP's we can see that MY.NET.87.50 was targeting 24.164.41.210, while MY.NET.98.203 was targeting its scan toward 216.33.254 and 194.251.249.182.

D.8 Most active pairs by multiple attack means

One thing I am interested in is how many source/destination host pairs generated mutiple types of alerts. This could be evidence of active targeting, one machine attempting multiple attacks against a different machine.

23 pairs of source/destination IP addresses for which there were 3 or more different alerts generated. Of these, the most was for unique alerts. The following chart shows each pair of source and destination addresses, as well as the different alert messages that were generated for that pair.

Number of alerts	Source	Destination	Alert Message
4	204.152.184.75	MY.NET.70.148	High port 65535 tcp - possible Red Worm - traffic
4	204.152.184.75	MY.NET.70.148	INFO - Possible Squid Scan
4	204.152.184.75	MY.NET.70.148	Port 55850 tcp - Possible myserver activity - ref. 010313-1
4	204.152.184.75	MY.NET.70.148	SCAN Proxy attempt
3	MY.NET.70.148	204.152.184.75	High port 65535 tcp - possible Red Worm - traffic
3	MY.NET.70.148	204.152.184.75	IDS50/trojan_trojan-active-subseven
3	MY.NET.70.148	204.152.184.75	Port 55850 tcp - Possible myserver activity - ref. 010313-1
3	MY.NET.16.42	MY.NET.11.4	High port 65535 tcp - possible Red Worm - traffic
3	MY.NET.16.42	MY.NET.11.4	Port 55850 tcp - Possible myserver activity - ref. 010313-1
3	MY.NET.16.42	MY.NET.11.4	spp_http_decode: IIS Unicode attack detected
3	MY.NET.11.4	MY.NET.16.42	High port 65535 tcp - possible Red Worm - traffic
3	MY.NET.11.4	MY.NET.16.42	Port 55850 tcp - Possible myserver activity - ref. 010313-1
3	MY.NET.11.4	MY.NET.16.42	SUNRPC highport access!
3	67.160.72.60	MY.NET.253.125	WEB-FRONTPAGE _vti_rpc access
3	67.160.72.60	MY.NET.253.125	WEB-IIS _vti_inf access

3	67.160.72.60	MY.NET.253.125	WEB-IIS view source via translate header
3	64.12.96.170	MY.NET.253.125	spp_http_decode: CGI Null Byte attack detected
3	64.12.96.170	MY.NET.253.125	spp_http_decode: IIS Unicode attack detected
3	64.12.96.170	MY.NET.253.125	WEB-CGI redirect access
3	24.180.238.51	MY.NET.253.125	WEB-FRONTPAGE _vti_rpc access
3	24.180.238.51	MY.NET.253.125	WEB-IIS view source via translate header
3	24.180.238.51	MY.NET.253.125	WEB-MISC guestbook.cgi access
3	24.180.196.26	MY.NET.5.96	WEB-FRONTPAGE _vti_rpc access
3	24.180.196.26	MY.NET.5.96	WEB-IIS _vti_inf access
3	24.180.196.26	MY.NET.5.96	WEB-IIS view source via translate header
3	213.33.140.176	MY.NET.100.165	CS WEBSERVER - external web traffic
3	213.33.140.176	MY.NET.100.165	WEB-FRONTPAGE _vti_rpc access
3	213.33.140.176	MY.NET.100.165	WEB-IIS _vti_inf access
3	212.199.203.9	MY.NET.5.45	spp_http_decode: IIS Unicode attack detected
3	212.199.203.9	MY.NET.5.45	WEB-IIS File permission canonicalization
3	212.199.203.9	MY.NET.5.45	WEB-MISC Attempt to execute cmd
3	211.99.180.131	MY.NET.100.165	CS WEBSERVER - external web traffic
3	211.99.180.131	MY.NET.100.165	spp_http_decode: IIS Unicode attack detected
3	211.99.180.131	MY.NET.100.165	WEB-MISC Attempt to execute cmd
3	206.65.191.129	MY.NET.98.187	Null scan!
3	206.65.191.129	MY.NET.98.187	Queso fingerprint
3	206.65.191.129	MY.NET.98.187	TFTP - External UDP connection to internal tftp server
3	206.65.191.129	MY.NET.98.177	Null scan!
3	206.65.191.129	MY.NET.98.177	Queso fingerprint
3	206.65.191.129	MY.NET.98.177	TFTP - External UDP connection to internal tftp server
3	205.188.209.106	MY.NET.60.14	spp_http_decode: CGI Null Byte attack detected
3	205.188.209.106	MY.NET.60.14	spp_http_decode: IIS Unicode attack detected
3	205.188.209.106	MY.NET.60.14	WEB-CGI redirect access
3	203.252.62.50	MY.NET.100.165	CS WEBSERVER - external web traffic
3	203.252.62.50	MY.NET.100.165	WEB-FRONTPAGE _vti_rpc access
3	203.252.62.50	MY.NET.100.165	WEB-IIS _vti_inf access
3	203.229.99.150	MY.NET.100.165	CS WEBSERVER - external web traffic
3	203.229.99.150	MY.NET.100.165	spp_http_decode: IIS Unicode attack detected
3	203.229.99.150	MY.NET.100.165	WEB-MISC Attempt to execute cmd
3	194.75.172.2	MY.NET.253.123	spp_http_decode: IIS Unicode attack detected
3	194.75.172.2	MY.NET.253.123	WEB-IIS File permission canonicalization
3	194.75.172.2	MY.NET.253.123	WEB-MISC Attempt to execute cmd
3	194.102.221.215	MY.NET.100.165	CS WEBSERVER - external web traffic
3	194.102.221.215	MY.NET.100.165	WEB-FRONTPAGE _vti_rpc access
3	194.102.221.215	MY.NET.100.165	WEB-IIS _vti_inf access
3	193.109.122.5	MY.NET.98.189	INFO - Possible Squid Scan
3	193.109.122.5	MY.NET.98.189	SCAN FIN

3	193.109.122.5	MY.NET.98.189	SCAN Proxy attempt
3	193.109.122.5	MY.NET.98.146	INFO - Possible Squid Scan
3	193.109.122.5	MY.NET.98.146	SCAN FIN
3	193.109.122.5	MY.NET.98.146	SCAN Proxy attempt
3	193.109.122.5	MY.NET.60.8	INFO - Possible Squid Scan
3	193.109.122.5	MY.NET.60.8	SCAN FIN
3	193.109.122.5	MY.NET.60.8	SCAN Proxy attempt
3	193.109.122.5	MY.NET.60.39	INFO - Possible Squid Scan
3	193.109.122.5	MY.NET.60.39	SCAN FIN
3	193.109.122.5	MY.NET.60.39	SCAN Proxy attempt
3	161.142.100.80	MY.NET.100.165	CS WEBSERVER - external web traffic
3	161.142.100.80	MY.NET.100.165	WEB-MISC http directory traversal
3	161.142.100.80	MY.NET.100.165	WEB-MISC Lotus Domino directory traversal
3	147.46.59.144	MY.NET.70.148	ICMP Echo Request BSDtype
3	147.46.59.144	MY.NET.70.148	INFO FTP anonymous FTP
3	147.46.59.144	MY.NET.70.148	MISC traceroute
3	133.5.165.24	MY.NET.6.7	WEB-FRONTPAGE _vti_rpc access
3	133.5.165.24	MY.NET.6.7	WEB-IIS _vti_inf access
3	133.5.165.24	MY.NET.6.7	WEB-IIS view source via translate header
3	128.223.4.21	MY.NET.70.148	ICMP Echo Request BSDtype
3	128.223.4.21	MY.NET.70.148	INFO FTP anonymous FTP
3	128.223.4.21	MY.NET.70.148	MISC traceroute

At the very top of the chart we see multiple types of suspicious traffic between 204.152.184.75 and MY.NET.70.80. The different alerts contain possible trojans, scans, and possible virus activity.

D.9 Scanning that lead to later attacks

The next thing I was interested in finding out was if any machines did a port scan of a host, and then later returned to attack that host in another way. This type of activity would indicate that reconaissance from the portscan was successful, and that attacker found something interesting.

To find this out, I first grouped all alerts by SourceIP, Destination IP, and Message. I then grouped all portscan alerts by Source IP and Destination IP. I then compared these two lists to see all the alerts that occurred between a host and destination that pair that had also generated a portscan alert. This query cturned up 10800 matches, meaning there were 10800 instances where a pair of machines had generated both a portscan alert and a different snort alert.

To narrow the analysis of this information down, I then grouped by message only, and counted up the number of times that message appeared in conjuntion with a portscan alert. The following table shows the results:

Number of portscan alerts	Alert Message
2	beetle.ucs
105	connect to 515 from outside
2	CS WEBSERVER - external web traffic
1	External FTP to HelpDesk MY.NET.70.49
1	External FTP to HelpDesk MY.NET.70.50
1	External FTP to HelpDesk MY.NET.83.197
854	External RPC call
3	High port 65535 tcp - possible Red Worm - traffic

1	High port 65535 udp - possible Red Worm - traffic
1	ICMP Echo Request Nmap or HPING2
11	ICMP Fragment Reassembly Time Exceeded
2	Incomplete Packet Fragments Discarded
5	INFO - Possible Squid Scan
16	INFO FTP anonymous FTP
52	INFO Inbound GNUTella Connect accept
1	MISC Large UDP Packet
1	MISC PCAnywhere Startup
52	Null scan!
3	Port 55850 tcp - Possible myserver activity - ref. 010313-1
34	Queso fingerprint
6	SCAN FIN
4566	SCAN Proxy attempt
1	SCAN XMAS
2	SMTP relaying denied
18	spp_http_decode: IIS Unicode attack detected
5002	SYN-FIN scan!
43	TCP SRC and DST outside network
1	TELNET login incorrect
2	TFTP - External UDP connection to internal tftp server
3	Tiny Fragments - Possible Hostile Activity
1	WEB-IIS File permission canonicalization
18	WEB-MISC Attempt to execute cmd

As we can see, there could be a lot of instances where a portscan was done from one host to another, and then later a different alert was generated by snort. This could indicate that the attacker may have found something out on her initial port scan.

D.10 Analysis of Out-of-spec data

There were 8390 Out of Spec Packets for the 5 days that were analyzed.

7391 of those packets were part of a Syn-Fin Scan on December 25th with the following signature:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:50:50.128940 24.0.28.234:22 -> MY.NET.1.190:22
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x11924268 Ack: 0xC4F2C7C Win: 0x404
00 00 00 00 00 00 ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:50:50.148647 24.0.28.234:22 -> MY.NET.1.191:22
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x11924268 Ack: 0xC4F2C7C Win: 0x404
00 00 00 00 00 00 ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:50:50.168567 24.0.28.234:22 -> MY.NET.1.192:22
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x11924268 Ack: 0xC4F2C7C Win: 0x404
00 00 00 00 00 00 ......
```

Packet detail:
Syn and Fin flags set
Same source and destination port
TTL low (25)
ID of 39426

This SYN-FIN Scan was also reported in the Snort alert file:

```
12/25/2001 21:50:38 906742 24.0.28.234 22 MY.NET.1.2 22 SYN-FIN scan!
```

The other 999 Out of spec packets were of various kinds.

Here is an interesting one for which we received one to three packets each day:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-01:48:26.418312 65.129.38.2:18245 -> MY.NET.253.114:21536
TCP TTL:118 TOS:0x0 ID:402 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-09:40:28.549128 65.129.33.89:18245 -> MY.NET.253.114:21536
TCP TTL:118 TOS:0x0 ID:57555 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-11:58:34.413866 65.129.21.105:18245 -> MY.NET.253.114:21536
TCP TTL:118 TOS:0x0 ID:4822 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-23:27:57.456183 65.129.48.98:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:1795 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/23-11:09:15.974118 65.129.32.4:18245 -> MY.NET.253.114:21536
TCP TTL:117 TOS:0x0 ID:449 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/23-11:51:29.193186 65.129.41.99:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:47984 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/24-22:29:31.510742 65.129.46.147:18245 -> MY.NET.253.125:21536
TCP TTL:120 TOS:0x0 ID:10241 DF
**SFRP*U Seq: 0x2F7E6367 Ack: 0x6568726D Win: 0x7072
31 2F 70 72 65 73 5F 73 69 74 65 2F 70 72 65 73 1/pres_site/pres
63 2E 68 74 6D 6C c.html

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-01:57:49.449545 65.129.57.114:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:14863 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

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

```
12/24-10:38:20.607721 65.129.57.235:20559 -> MY.NET.11.4:21332
TCP TTL:120 TOS:0x0 ID:887 DF
2*SF*P*U Seq: 0x202F7370 Ack: 0x6970652F Win: 0x6720
63 65 70 74 3A 20 cept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/24-13:38:41.570586 65.129.38.118:18245 -> MY.NET.11.4:21536
TCP TTL:117 TOS:0x0 ID:127 DF
2*SFR**U Seq: 0x2F737069 Ack: 0x70652F70 Win: 0x3F41
3D 7B 32 33 41 41 33 35 36 36 ={23AA3566

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/24-15:04:40.755071 65.129.29.16:18245 -> MY.NET.253.114:21536
TCP TTL:117 TOS:0x0 ID:40451 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/24-16:40:40.549022 65.129.31.168:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:40960 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/24-18:18:03.315858 65.129.21.34:18245 -> MY.NET.253.114:21536
TCP TTL:120 TOS:0x0 ID:421 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-11:29:11.306840 65.129.24.90:20559 -> MY.NET.11.4:21332
TCP TTL:120 TOS:0x0 ID:113 DF
2*SF*P*U Seq: 0x202F7370 Ack: 0x6970652F Win: 0x6720
63 65 70 74 3A 20 cept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-11:29:18.123489 65.129.24.90:18245 -> MY.NET.11.4:21536
TCP TTL:120 TOS:0x0 ID:157 DF
2*SFR**U Seq: 0x2F737069 Ack: 0x70652F70 Win: 0x3F41
3D 7B 32 33 41 41 33 35 36 36 ={23AA3566

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-12:45:48.334746 65.129.16.140:18245 -> MY.NET.253.114:21536
TCP TTL:119 TOS:0x0 ID:14349 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-19:03:02.069272 65.129.44.128:18245 -> MY.NET.253.114:21536
TCP TTL:119 TOS:0x0 ID:1658 DF
2*SF***U Seq: 0x2F686F6D Ack: 0x6573756E Win: 0x7373
65 73 75 6E 2E 63 73 73 20 48 54 54 50 2F 31 2E esun.css HTTP/1.
31 0D 0A 41 63 63 65 70 74 3A 1..Accept:
```

Packet detail:
All packets originate at 65.129.X.X, which is Quest networks.
All packets have source port of 18245 and destination of 21536
All packets have SYN and FIN and URG flags set, some also have Reset and Push set.
All packets seem to contain HTTP headers.

The following packet was analyzed in David Hed's GCIA Practical

(http://www.giac.org/practical/David_Hed_GCIA.zip) and shows a similar signature (source port 18245, destination port 21536, data appears to be HTTP headers.)

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
04/27-16:46:09.062984 212.123.172.102:18245 -> MY.NET.179.77:21536
TCP TTL:111 TOS:0x0 ID:2137 DF
2*SFR*AU Seq: 0x2F746573 Ack: 0x742F6272 Win: 0x7365
54 50 2F 31 2E 31 0D 0A 41 63 TP/1.1..Ac
```

A simiar signature was reported by Bob Fawcett at http://www.sans.org/y2k/120200.htm

```
Nov 29 03:49:09 212.2.215.113:18245 -> my.net.26.7:21536 NOACK **U*PRSF
```

After some research, I found this: http://cert.uni-stuttgart.de/archive/incidents/2000/12/msg00135.html

> We've posted some information about 18245/21536 recently, but you probably missed it. TCP packets comming from 18245 to 21536 are not scans, but corrupted packets. They are TCP packets WITHOUT TCP header, there is IP header and TCP data immediatly after it.
> String "GET " in TCP data placed in the place of TCP header means connection from port 18245 to 21536.
> Polish Telecom (tpnet.pl) has corrupted access-server which produce such packets.

So that while these packets are not originating from tpnet.pl, there is some explaination. Apparently these appear to be TCP packets with the TCP header missing. Since the first part of a HTTP request is the string "GET", this string fills in where the TCP header would normally be and sets the ports to 18245 and 21536. Since all this traffic is coming from the same network, it is very likely that Quest has a router or similar device that is corrupting packets.

A great number of the packets were similar to the following:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:07:42.434716 213.84.157.192:45210 -> MY.NET.100.236:1214
TCP TTL:51 TOS:0x0 ID:5836 DF
21S***** Seq: 0xF8D5BADE Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 14527506 0 EOL EOL EOL EOL


=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:07:51.739694 213.84.157.192:45210 -> MY.NET.100.236:1214
TCP TTL:51 TOS:0x0 ID:5838 DF
21S***** Seq: 0xF8D5BADE Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 14528406 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-21:44:15.494109 213.84.157.192:45448 -> MY.NET.100.236:1214
TCP TTL:51 TOS:0x0 ID:43987 DF
21S***** Seq: 0x82B5AD7F Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 14747308 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-22:21:33.723260 213.84.157.192:45672 -> MY.NET.100.236:1214
TCP TTL:51 TOS:0x0 ID:18211 DF
21S***** Seq: 0x100A2A38 Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 14970438 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/25-22:21:38.079425 213.84.157.192:45672 -> MY.NET.100.236:1214
TCP TTL:51 TOS:0x0 ID:18212 DF
```

```
21S***** Seq: 0x100A2A38 Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 14971038 0 EOL EOL EOL EOL
```

Packet detail:
SYN Flag set
Both reserved bits are set
TCP Options: Maximum Segment Size set (1460 normal for Ethernet)
TCP Options: A Timestamp and selective acknowledgement are set as well
The destination port here is 1214 Which is KAZAA, a file sharing application.

John Jenkinson analyzed very similar out of spec packets in his GCIA practical at http://www.giac.org/practical/John_Jenkinson_GCIA.doc.

Another common type of Out of Spec data concerned fragmentation problems, such as these:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-12:55:56.078126 64.172.24.155 -> MY.NET.70.70
TCP TTL:108 TOS:0x0 ID:22235 DF MF
Frag Offset: 0x0 Frag Size: 0x22
70 DB C9 3A CB 40 7A 48 D2 FC 2F 75 42 FD 57 A3 p..:.@zH../uB.W.
6C 6E 05 47 4F A0 E1 B4 48 78 5C F5 FF 8B F9 76 ln.GO...Hx\....v
20 05 .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-12:55:56.309531 64.172.24.155 -> MY.NET.70.70
TCP TTL:108 TOS:0x0 ID:22237 DF MF
Frag Offset: 0x0 Frag Size: 0x22
74 23 C3 CA 86 A1 45 C4 17 F7 04 05 71 0F 23 49 t#....E.....q.#I
83 B6 6D 9D 1C 14 66 F0 21 40 C7 FD DF 49 EE 0A ..m...f.!@...I..
01 B8 ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
12/22-12:56:05.276093 64.172.24.155 -> MY.NET.70.70
TCP TTL:108 TOS:0x0 ID:22326 DF MF
Frag Offset: 0x0 Frag Size: 0x22
D1 65 6F BE A6 8D 1C D1 8C 3C 83 7B EF 2F C1 46 .eo......<.{./.F
AF 30 98 A2 2A 5A 1F EF 3E FF 6A 1F AB C4 E1 32 .0..*Z..>.j....2
D1 D5 ..
```

Packet Detail:
Don't Fragment and More Fragment flags both set.
Tiny fragment size of 22 bytes.

Corresponding alerts also show up in the snort alert file:

12/22/2001 13:00:21 765570 MY.NET.70.70 64.172.24.155 ICMP Fragment Reassembly Time Exceeded

D.11 Analysis of time of alerts

I was interested in finding out if there were any patterns or anomolies in the time of attacks. To find this out, I grouped all the alerts into thirty minute segments of time. The following chart shows the number of alerts for each thirty minute period:

Thirty minutes beginning	Number of alerts
12/22/01 12:00 AM	466

12/22/01 12:30 AM	496
12/22/01 1:00 AM	728
12/22/01 1:30 AM	21
12/22/01 2:00 AM	478
12/22/01 2:30 AM	978
12/22/01 3:00 AM	35
12/22/01 3:30 AM	387
12/22/01 4:00 AM	712
12/22/01 4:30 AM	1283
12/22/01 5:00 AM	1017
12/22/01 5:30 AM	11
12/22/01 6:00 AM	30
12/22/01 6:30 AM	510
12/22/01 7:00 AM	1169
12/22/01 7:30 AM	1145
12/22/01 8:00 AM	895
12/22/01 8:30 AM	532
12/22/01 9:00 AM	996
12/22/01 9:30 AM	1328
12/22/01 10:00 AM	741
12/22/01 10:30 AM	1001
12/22/01 11:00 AM	1476
12/22/01 11:30 AM	1064
12/22/01 12:00 PM	479
12/22/01 12:30 PM	569
12/22/01 1:00 PM	580
12/22/01 1:30 PM	21
12/22/01 2:00 PM	31
12/22/01 2:30 PM	755
12/22/01 3:00 PM	546
12/22/01 3:30 PM	1198
12/22/01 4:00 PM	512
12/22/01 4:30 PM	655
12/22/01 5:00 PM	679
12/22/01 5:30 PM	5660
12/22/01 6:00 PM	713
12/22/01 6:30 PM	397
12/22/01 7:00 PM	401
12/22/01 7:30 PM	365
12/22/01 8:00 PM	290
12/22/01 8:30 PM	381
12/22/01 9:00 PM	412

12/22/01 9:30 PM	329
12/22/01 10:00 PM	839
12/22/01 10:30 PM	11
12/22/01 11:00 PM	626
12/22/01 11:30 PM	25
12/23/01 12:00 AM	41
12/23/01 12:30 AM	48
12/23/01 1:00 AM	482
12/23/01 1:30 AM	15
12/23/01 2:00 AM	752
12/23/01 2:30 AM	17
12/23/01 3:00 AM	608
12/23/01 3:30 AM	1077
12/23/01 4:00 AM	744
12/23/01 4:30 AM	732
12/23/01 5:00 AM	269
12/23/01 5:30 AM	13
12/23/01 6:00 AM	339
12/23/01 6:30 AM	2062
12/23/01 7:00 AM	7
12/23/01 7:30 AM	15
12/23/01 8:00 AM	53
12/23/01 8:30 AM	14
12/23/01 9:00 AM	404
12/24/01 12:00 AM	30
12/24/01 12:30 AM	29
12/24/01 1:00 AM	18
12/24/01 1:30 AM	1043
12/24/01 2:00 AM	19
12/24/01 2:30 AM	29
12/24/01 3:00 AM	545
12/24/01 3:30 AM	34
12/24/01 4:00 AM	992
12/24/01 4:30 AM	957
12/24/01 5:00 AM	1037
12/24/01 5:30 AM	942
12/25/01 12:00 AM	872
12/25/01 12:30 AM	791
12/25/01 1:00 AM	222
12/25/01 1:30 AM	702
12/25/01 2:00 AM	321
12/25/01 2:30 AM	5

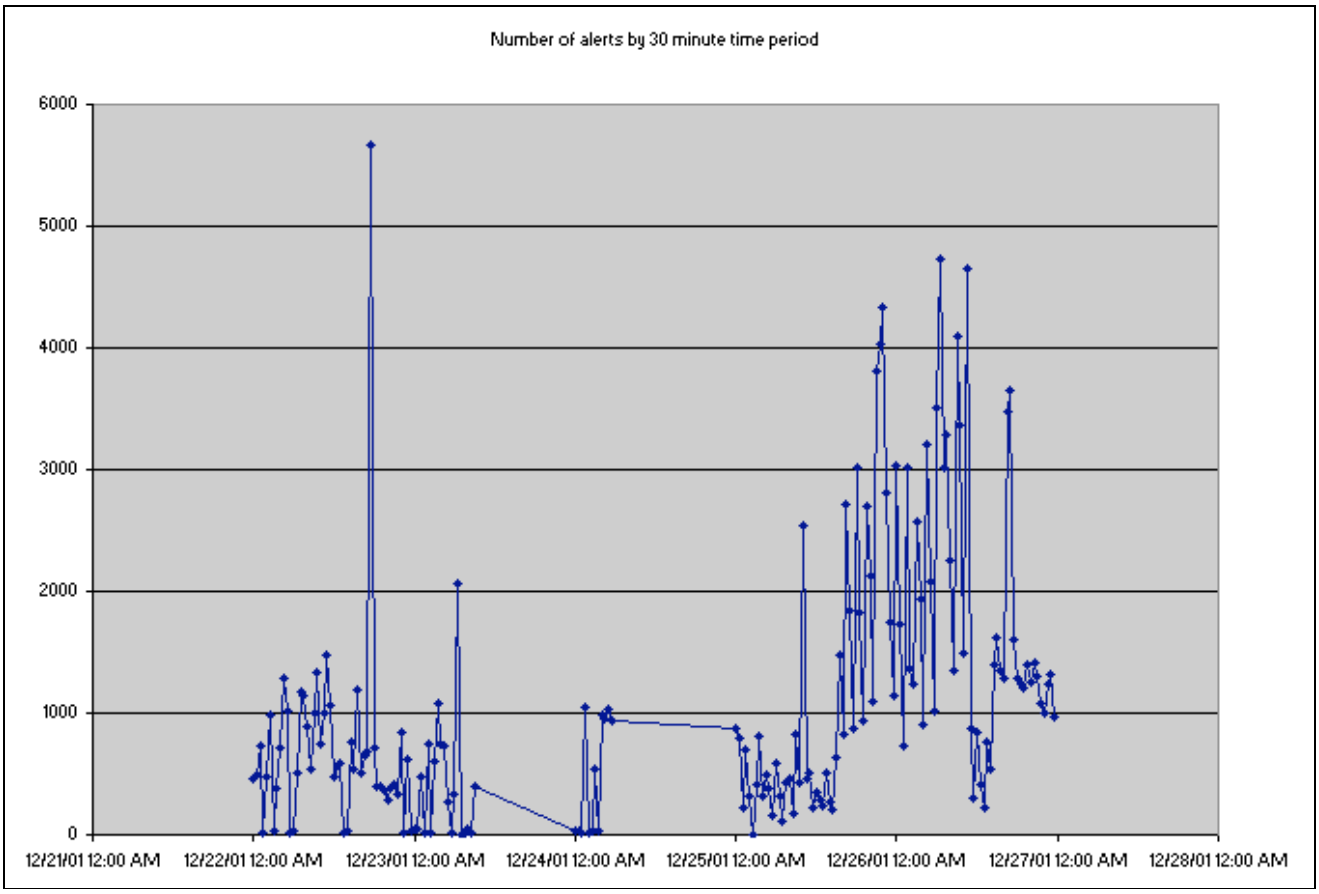
12/25/01 3:00 AM	409
12/25/01 3:30 AM	805
12/25/01 4:00 AM	321
12/25/01 4:30 AM	499
12/25/01 5:00 AM	386
12/25/01 5:30 AM	152
12/25/01 6:00 AM	594
12/25/01 6:30 AM	311
12/25/01 7:00 AM	116
12/25/01 7:30 AM	432
12/25/01 8:00 AM	461
12/25/01 8:30 AM	167
12/25/01 9:00 AM	827
12/25/01 9:30 AM	433
12/25/01 10:00 AM	2536
12/25/01 10:30 AM	468
12/25/01 11:00 AM	508
12/25/01 11:30 AM	221
12/25/01 12:00 PM	356
12/25/01 12:30 PM	291
12/25/01 1:00 PM	244
12/25/01 1:30 PM	503
12/25/01 2:00 PM	263
12/25/01 2:30 PM	209
12/25/01 3:00 PM	633
12/25/01 3:30 PM	1483
12/25/01 4:00 PM	833
12/25/01 4:30 PM	2718
12/25/01 5:00 PM	1838
12/25/01 5:30 PM	878
12/25/01 6:00 PM	3013
12/25/01 6:30 PM	1827
12/25/01 7:00 PM	929
12/25/01 7:30 PM	2703
12/25/01 8:00 PM	2133
12/25/01 8:30 PM	1091
12/25/01 9:00 PM	3813
12/25/01 9:30 PM	4027
12/25/01 10:00 PM	4330
12/25/01 10:30 PM	2812
12/25/01 11:00 PM	1744
12/25/01 11:30 PM	1143

12/26/01 12:00 AM	3035
12/26/01 12:30 AM	1732
12/26/01 1:00 AM	732
12/26/01 1:30 AM	3021
12/26/01 2:00 AM	1372
12/26/01 2:30 AM	1236
12/26/01 3:00 AM	2567
12/26/01 3:30 AM	1935
12/26/01 4:00 AM	904
12/26/01 4:30 AM	3214
12/26/01 5:00 AM	2076
12/26/01 5:30 AM	1021
12/26/01 6:00 AM	3509
12/26/01 6:30 AM	4736
12/26/01 7:00 AM	3012
12/26/01 7:30 AM	3285
12/26/01 8:00 AM	2251
12/26/01 8:30 AM	1353
12/26/01 9:00 AM	4099
12/26/01 9:30 AM	3363
12/26/01 10:00 AM	1492
12/26/01 10:30 AM	4652
12/26/01 11:00 AM	878
12/26/01 11:30 AM	303
12/26/01 12:00 PM	839
12/26/01 12:30 PM	415
12/26/01 1:00 PM	218
12/26/01 1:30 PM	761
12/26/01 2:00 PM	533
12/26/01 2:30 PM	1393
12/26/01 3:00 PM	1616
12/26/01 3:30 PM	1342
12/26/01 4:00 PM	1286
12/26/01 4:30 PM	3474
12/26/01 5:00 PM	3644
12/26/01 5:30 PM	1611
12/26/01 6:00 PM	1280
12/26/01 6:30 PM	1231
12/26/01 7:00 PM	1211
12/26/01 7:30 PM	1400
12/26/01 8:00 PM	1261
12/26/01 8:30 PM	1415

12/26/01 9:00 PM	1297
12/26/01 9:30 PM	1084
12/26/01 10:00 PM	1005
12/26/01 10:30 PM	1238
12/26/01 11:00 PM	1320
12/26/01 11:30 PM	975

To get a better understanding of the data we can graph it:

D.11.1 Time of Day Graph



The first thing that stands out from the graph is the highest peak which corresponds to 12/22/01 5:30 PM.

If we go back to the data for that time, we see that this peak was due to traffic with the following signature:

```
12/22/2001 17:37:54 523485 61.219.53.135 1654 MY.NET.153.210 3816 MISC Large UDP Packet
12/22/2001 17:37:54 589514 61.219.53.135 1654 MY.NET.153.210 3816 MISC Large UDP Packet
12/22/2001 17:37:54 821987 61.219.53.135 0 MY.NET.153.210 0 Incomplete Packet Fragments Discarded
12/22/2001 17:37:54 930172 61.219.53.135 1654 MY.NET.153.210 3816 MISC Large UDP Packet
12/22/2001 17:37:55 094367 61.219.53.135 1654 MY.NET.153.210 3816 MISC Large UDP Packet
```

From the traffic signature, it could be assumed that someone was doing a large file transfer using non-standard ephemeral UDP ports. This should definetely be looked into further, so we will flag it as one of our "Top Ten".

There are other high data points at 12/26/01 6:30 AM and 12/26/01 10:30 AM. Here are the most prevalent alert signatures for those times:

```
12/26/2001 06:47:23 432047 65.165.14.43 4854 MY.NET.1.44 1080 SCAN Proxy attempt
12/26/2001 06:47:23 555561 65.165.14.43 4869 MY.NET.1.49 1080 SCAN Proxy attempt
12/26/2001 06:47:23 559150 65.165.14.43 4872 MY.NET.1.50 1080 SCAN Proxy attempt
12/26/2001 06:47:23 574804 65.165.14.43 4875 MY.NET.1.51 1080 SCAN Proxy attempt
12/26/2001 06:47:23 617264 65.165.14.43 4884 MY.NET.1.54 1080 SCAN Proxy attempt
12/26/2001 06:47:23 631029 65.165.14.43 4887 MY.NET.1.55 1080 SCAN Proxy attempt
```

This is a large scale incoming scan of our network.

```
12/26/2001 10:37:58 505809 212.179.35.118 60339 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
12/26/2001 10:37:58 895805 212.179.35.118 60339 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
12/26/2001 10:37:59 173951 212.179.35.118 60339 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
12/26/2001 10:37:59 511277 212.179.35.118 60339 MY.NET.70.70 1214 Watchlist 000220 IL-ISDNNET-990517
```

This traffic is flagged as "Watchlist", which means it comes from a network which is known for lax security. Port 1214 is used by the file sharing program "KAZAA".

The next most interesting thing on the chart is actually what is not on the chart- There are NO data points between 12/23/01 9:00 am and 12/24/01 12:30 am and again between 12/24/01 5:30 am and 12/25/01 12:00 am. If we go back to the data, we find that there is in fact no data recorded for these time periods.

A few possible causes for this missing data are:

The IDS system was down during this time period.
The network was down during this period (either due to scheduled maintenance or due to problems) and there was no traffic. This could be possible, because netork maintenance is often done over the holidays, especially at a University.
An attacker was able to delete data from the IDS or block the IDS from receiving it to hide their activities.

Clearly the reason for this data gap would require further research.

E. Top 10 "Talkers" List

From all the analysis above, we can see that we could list the Top Ten of any of the different groupings of data I created. I decided it would be more valuable to chose 10 of the high risk situations and give a bit more detail on those.

E.1 Internal host MY.NET.87.50

There were a number of alerts for "MISC Large UDP Packet" destined for the host MY.NET.87.50, with various sources and various ports. This could indicate there is some backdoor running on the host MY.NET.87.50

```
12/26/2001 19:33:00 426270 24.158.75.105 27005 MY.NET.87.50 999 MISC Large UDP Packet
```

From the tables above, we also saw that the host MY.NET.87.50 was among the Most Active Attackers (see D.5.1), generating 1142 alerts. It was also the most active portscanner, generating the most portscan alerts (see D.7.2) scanning the most destination addresses (see D.7.5) and scanning the most unique ports (see D.7.6). Someone with access to this box has been doing a lot of scanning.

E.2. IDS50/trojan_trojan-active-subseven

These packets match the signature of subseven traffic. Both are ephemeral ports, and one is commonly used by subseven (1243). It looks as though the internal host MY.NET.70.148 may be compromised. We also saw that this was the most attacked host with 8208 alert messages destined for it. See D.4.1.

```
12/23/2001 04:07:47 856530 MY.NET.70.148 1243 204.152.184.75 51827 IDS50/trojan_trojan-active-subseven
```

More information on the subseven trojan can be found in the Sans Institute Intrusion Detection Faq:

SubSeven V1.1 at http://www.sans.org/newlook/resources/IDFAQ/subseven.htm

E.3 Possible trojan server activity

These packets match the signature of subseven traffic. Both are ephemeral ports, and one is commonly used by subseven (27374). It looks as though the internal host MY.NET.190.34 may be compromised.

12/22/2001 21:34:42 347884 204.251.203.223 3699 MY.NET.190.34 27374 Possible trojan server activity

E.4 DDOS mstream handler to client, DDOS shaft client to handler

These packets appear to match the signature of a known distributed denial or service program. Both ports are ephemeral, and one is commonly used by this DDOS client.

12/26/2001 19:36:00 454198 MY.NET.97.160 15104 24.78.99.154 3152 DDOS mstream handler to client

More information on thid DDOS attack can be found at http://security.royans.net/info/posts/bugtraq_ddos3.shtml

E.5 MISC Large UDP Packets for MY.NET.153.210

Again we see Large UDP packets with non-standard ports. These stuck out because they showed up as a high traffic peak on 12/22/01 between 5:30 PM and 6:00 PM (see D.11.1).

12/22/2001 17:32:20 369527 61.219.53.135 1654 MY.NET.153.210 3816 MISC Large UDP Packet

E.6 Possible myserver activity for MY.NET.70.148

Here again, TCP traffic on non-standard ports, one of which is a known hacker tool. The fact that this internal host has generated other alerts that may indicate compromise makes this host very suspect. (see E.2)

12/23/2001 04:51:13 281283 204.152.184.75 55850 MY.NET.70.148 2706 Port 55850 tcp - Possible myserver activity - ref. 010313-1
12/23/2001 04:51:13 281361 MY.NET.70.148 2706 204.152.184.75 55850 Port 55850 tcp - Possible myserver activity - ref. 010313-1

Myserver is a little known Distributed Denial of Service agent that binds to port 55850. More information can be found at http://archives.neohapsis.com/archives/incidents/2000-10/0136.html

E.7 Targeting of MY.NET.253.125

The host MY.NET.253.125 was the most targeted machine, with 20 different types of attacks (see D.4.2). Most of these were web attacks:

12/22/01 12:35:12 AM 24.180.140.132 4565 MY.NET.253.125 80 WEB-IIS _vti_inf access
12/22/01 12:35:12 AM 24.180.140.132 4566 MY.NET.253.125 80 WEB-FRONTPAGE _vti_rpc access
12/22/01 4:13:22 AM 24.180.238.51 3511 MY.NET.253.125 80 WEB-MISC guestbook.cgi access
12/22/01 10:52:31 AM 193.231.20.2 48281 MY.NET.253.125 80 Queso fingerprint
12/22/01 1:00:16 PM 24.8.58.167 MY.NET.253.125 Tiny Fragments - Possible Hostile Activity
12/22/01 1:00:17 PM 24.8.58.167 6 MY.NET.253.125 20327 Null scan!
12/22/01 1:00:17 PM 24.8.58.167 MY.NET.253.125 Tiny Fragments - Possible Hostile Activity
12/22/01 5:58:58 PM 66.61.182.252 3303 MY.NET.253.125 80 WEB-IIS _vti_inf access
12/22/01 5:58:58 PM 66.61.182.252 3305 MY.NET.253.125 80 WEB-IIS _vti_inf access
12/23/01 3:46:48 AM 165.121.126.67 4483 MY.NET.253.125 80 WEB-CGI formmail access
12/23/01 3:57:07 AM 24.124.55.13 1240 MY.NET.253.125 80 WEB-FRONTPAGE fpcount.exe access

E.8 Communication between internal hosts MY.NET.16.42 and MY.NET 11.14

We saw in D.8 that the hosts MY.NET.16.42 and MY.NET.11.14 generated various types of alerts between them, which

could indicate that one or both are compromised with a virus or trojan.

MY.NET.16.42	MY.NET.11.4	High port 65535 tcp - possible Red Worm - traffic
MY.NET.16.42	MY.NET.11.4	Port 55850 tcp - Possible myserver activity - ref. 010313-1
MY.NET.16.42	MY.NET.11.4	spp_http_decode: IIS Unicode attack detected
MY.NET.11.4	MY.NET.16.42	High port 65535 tcp - possible Red Worm - traffic
MY.NET.11.4	MY.NET.16.42	Port 55850 tcp - Possible myserver activity - ref. 010313-1
MY.NET.11.4	MY.NET.16.42	SUNRPC highport access!

E.9 External RPC Call following portscan

In section D.9, we saw that there were 854 external RPC call attempts in conjunction with other portscans. This could indicate that there was successful reconaissance during the scan, and now the attacker is targeting machines with potentially vulnerable services running.

E.10 Attacks from 64.12.96.170

In section D.5.2, we saw that the external host 64.12.96.170 was the origin for the most differnet types of alert messages. This could indicate an attacker trying multiple means for breaking into the network

F. 5 External addresses with registration information

F.1 204.251.203.223

This address appeared to be a host system connecting to a subseven backdoor on our network. (see E.3)

Output from ARIN Whois for 204.251.203.223:
EZ WEBTECH (NETBLK-SPRINT-CCFBCB-4) SPRINT-CCFBCB-4
204.251.203.0 - 204.251.203.255

DNS reverse lookup produced no results.
EZ WEBTECH appears to be a Milwaukee Wisconsin based ISP (http://www.ezwebtech.com/access/local_access.htm)

F.2 24.78.99.154

This address appears to be a DDOS Client (see E.4)

Output from ARIN Whois for 24.78.99.154:
Shaw Fiberlink (aka Shaw@HOME) (NETBLK-FIBERLINK-CABLE-2BLK)
Suite 800, 630 3rd Avenue SW
Calgary, Alberta T2P 4L4
CA

Netname: FIBERLINK-CABLE-2BLK
Netblock: 24.76.0.0 - 24.79.255.255
Maintainer: FBCA

Coordinator:
Shaw High-Speed Internet (ZS178-ARIN) ipadmin@sjrb.ca
(403)750-7428

A DNS reverse lookup of this address yeilds h24-78-99-154.vs.shawcable.net. This is likly a home cable-modem user.

F.3 64.12.96.170

This was the most active external attacker by different types of attacks. (see E.10)
Output from ARIN WHois for 64.12.96.170:
America Online, Inc. (NETBLK-AOL-MTC)
10600 Infantry Ridge Road
Manassas, VA 20109
US

Netname: AOL-MTC
Netblock: 64.12.0.0 - 64.12.255.255

Coordinator:
America Online, Inc. (AOL-NOC-ARIN) domains@AOL.NET
703-265-4670

Domain System inverse mapping provided by:

DNS-01.NS.AOL.COM 152.163.159.232
DNS-02.NS.AOL.COM 205.188.157.232

Record last updated on 16-Dec-1999.
Database last updated on 29-Jan-2002 19:56:39 EDT.

DNS Revers lookup of this address yields cache-mtc-ah05.proxy.aol.com

F.4 209.49.12.32

This was the most attacked external host. (see D.4.1)

Output from ARIN Whois for 209.49.12.32:
Business Internet, Inc. (NET-ICIX-MD-BLK14)
3625 Queen Palm Drive
Tampa, FL 33619
US

Netname: ICIX-MD-BLK14
Netblock: 209.48.0.0 - 209.49.255.255
Maintainer: IMBI

Coordinator:
Business Internet, Inc. (ZI44-ARIN) ipreq@icix.net
240-616-2000

Domain System inverse mapping provided by:

NS.DIGEX.NET 64.245.20.14
NS2.DIGEX.NET 64.245.43.14

Record last updated on 02-Jan-2001.
Database last updated on 29-Jan-2002 19:56:39 EDT.

DNS Reverse lookup returned no results.

F.5 212.179.35.118

This was the most active external attacker by number of alerts generated. (see D.5.1)

Output from RIPE Whois for 212.179.35.118:

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 212.179.0.0 - 212.179.255.255
netname: IL-ISDNNET-990517
descr: PROVIDER
country: IL
admin-c: NP469-RIPE
tech-c: TP1233-RIPE
tech-c: ZV140-RIPE
tech-c: ES4966-RIPE
status: ALLOCATED PA
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 19990517
changed: hostmaster@ripe.net 20000406
changed: hostmaster@ripe.net 20010402
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

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE

person: Tomer Peer
address: Bezeq International
address: 40 Hashakham St.
address: Petakh Tiqwah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: TP1233-RIPE
changed: registrar@ns.il 19991113
source: RIPE

person: Zehavit Vigder
address: bezeq-international
address: 40 hashacham
address: petach tikva 49170 Israel
```

phone: +972 52 770145
fax-no: +972 9 8940763
e-mail: hostmaster@bezeqint.net
nic-hdl: ZV140-RIPE
changed: zehavitv@bezeqint.net 20000528
source: RIPE

person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

DNS Reverse lookup returned no results.

G. Any insights into internal machines such as compromise or possible dangerous or anomalous activity.

There were many instances where insights into compromises and other suspicious activity was detailed in the analysis above. See expecially sections E.1 through E.10.

H. Correlations

Correlations to other students practicals and other outside resources were made throughout the analysis.

I. Defensive recommendations

Each of the high risk alerts above should be researched further. Special attention should be paid to the internal hosts specified in sectiosn E.1 through E.10.

Any of the external addresses that were specified above as wither the source or destination for dangerous activity should be researched, and the network owner should be contacted so that they can attempt to keep attackers and compromised hosts off of their networks.

I would also recommend that the University implement a firewall to attempt to block some of the suspicious traffic. Universities usually would like to be an open environment where students and professors have the freedom to use the Internet without restriction. Machines in Universities often have full-time high-speed Internet access and may not have the level of security applied to the host that is necessary when connected to the Internet. This is especially true for dormitory machines.

J. References

Allaire Security Bulletin. "Solution Available for Denial-of-Service Attack Using CF Admin. Start/Stop Utility". Allaire Corp. May 19, 1999
http://packetstorm.widexs.nl/advisories/allaire/asb99-07.dos_cf_admin

ARIN.net Whois Database Search. American Registry of Internet Numbers.
http://www.arin.net/whois/index.html

David Hed GCIA Practical

http://www.giac.org/practical/David_Hed_GCIA.zip

Dietrich, Sven . An analysis of the ``Shaft'' distributed denial of service tool. Administrators & Security Archive.
http://security.royans.net/info/posts/bugtraq_ddos3.shtml

"iishack 2000" Source Code. eEye Digital Security.
http://www.eeye.com/html/research/Advisories/iishack2000.c

Janoszka, Grzegorz. "Re: scan on TCP/21536". RUS-CERT-Archiv
http://cert.uni-stuttgart.de/archive/incidents/2000/12/msg00135.html

RIPE.net Whois Database Search. Réseaux IP Européens.
http://www.ripe.net/ripencc/pub-services/db/whois/whois.html

SubSeven V1.1. Sans Institute Intrusion Detection Faq
http://www.sans.org/newlook/resources/IDFAQ/subseven.htm

Windows 2000 IIS 5.0 Remote buffer overflow vulnerability. eEye Digital Security.
http://www.eeye.com/html/Research/Advisories/AD20010501.html

Worman, Mike. Neohapsis Archives.
http://archives.neohapsis.com/archives/incidents/2000-10/0136.html.