Intrusion Detection in Depth - Track 3
GCIA Practical Assignment by Ruth Kizlyk
Version 2.0

ASSIGNMENT 1
DESCRIBE THE STATE OF INTRUSION DETECTION

DON'T FORGET TO DESIGN IT, TUNE IT AND MAINTAIN IT

Background

Picture the boardroom, full of tension. Consultants on one side of the table, reassuring the client they will have the Intrusion Detection in place when the new infrastructure is deployed. The client is apprehensive after project delays and budget-overruns. They've never allowed Internet access on the network and their board members are nervous. The new infrastructure promises a much more secure environment with a firewall, an anti-virus gateway, intrusion detection and a switched network. The contract included implementation of an intrusion detection system with real time alerts, 24 hours a day. Just before implementation, several issues surface and it's discovered that it is not just a matter of building the box and putting it on the network.

Intrusion detection is often a component of a larger project but it is essential it is given the attention it requires. Effective intrusion detection can be accomplished it you take the time to *design it*, *tune it* and *maintain it*. Management must budget for each of these elements and understand the impact of each stage.

Design It

The next few paragraphs describe the many design issues that require careful consideration. It is important to understand the difference of host-based or network-based sensors and their placement on your network. Management needs to understand what real-time alerts are so their expectations can be managed. The intrusion detection solution may need to be designed for a switched network. There are many different configurations for alerts. The options should be discussed and their impact understood. Finally, it is prudent to understand how the sensors communicate in the design stage as this has impact on your secure environment.

Design It - Sensors

There are two types of intrusion detection sensors, host-based sensors and network-based sensors. A host-based ID sensor reports on activity or changes on a specific box. This information is based on traffic, logs or events specific to that box. Sensors report on local alerts as well as changes to important files and local access attempts. Software for these sensors should be installed on all critical boxes. Management must determine which boxes require this type of monitoring.

A network-based sensor gathers information from network traffic. Network-based sensors may detect malicious packets, which matched a firewall rule and were accepted. Network traffic may include traffic between any number of boxes depending on the placement of the network-based sensor and if the environment is switched or not. Often a network-based sensor is placed at the single-point of entry to an environment. A sensor placed on the outside of a firewall will see all traffic including packets that are dropped by the firewall. A sensor placed on the inside will see less traffic and only the traffic that passed through the firewall. Some argue that placement outside the Firewall provide an important measurement of looming traffic including possible intrusion attempts. This can also be used as a measurement of the firewall's effectiveness. Others argue placement inside the Firewall reduces alerts thereby increases relevance and response to those alerts. Management needs to consider these factors and the resources required to follow up on alerts before placing the network sensor.

One basic security principle is defense in depth. Intrusion detection is most effective using a combination of host-based and network-based sensors.

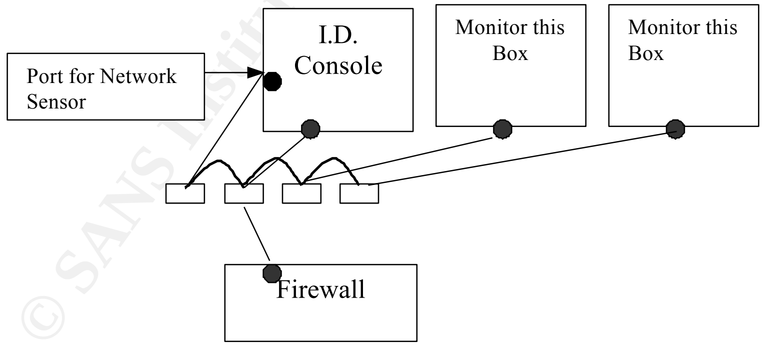
Design It - Real Time Alerts

Real time alerts is more of a marketing term, which misleads management. It is very difficult to achieve real time responses even when the budget provides for resources. A response is always after the event. Some options like paging alerts or automated responses decrease the response time but are not always desirable. A computer incident response procedure will decrease the response time. Management is often mislead by the term and need to understand the reality that responses are after the events.

Design It - Switched Environment

Switched environments provide a unique challenge for implementing ID systems. The switch forwards frames based on the destination MAC address of each frame. You may want the network-based ID sensor is listen to all traffic on a particular network segment. Port spanning is a popular option to solve this problem. It allows monitoring of all traffic within a VLAN. (Port spanning is not limited to monitoring traffic in the same VLAN. You can span ports that are in different VLANs). The ports of all boxes to be monitored are spanned on the switch. Port spanning adds additional costs, may not be supported by all switches and put additional load on the switch but it does allow ID to function in a switched environment.

PORT SPANNING



Design It - Sensors Securely Reporting

Both network-based and host-based sensors can report to a console providing consolidated reporting. Sensors communicate on specific ports and report events, logging information and other status information. For example, Real Secure IIS listens on port 901 (common location for realsecure) for communication from the console. Corporate policy or infrastructure may restrict ports at the firewall or between VLANs. Management should be aware of the communication requirement between sensors and console. Often this traffic could be encrypted to prevent intruder reconnaissance or tampering of logs.

Tune It

If you've designed it properly and implemented according to design why do you have to tune it? Well, that is simple. You need time to experience it and that can only be done after it is up and running for a while. The tuning period is time spent reacting to alerts. Learning which signatures to alert on. It is the time to discover the relationship of alerts to other logs. It is the time a security officer needs to become familiar with their infrastructure so that the security officer, in conjunction with the intrusion detection product can best protect their unique environment.

Tune It - Log or Alert on Detects

Ideally, only the most relevant alerts should be paged out for the best response. Using the recommended default settings on an ID product can produced extensive alerts and may not be suited for your environment. The security officer must assess the severity of each alert, weed out the false positives and be aware of false negatives. This commitment determines which detects to log and which to alert on.

The number of alerts will be overwhelming. This number is often bolstered by false positives. These are events that are detected but shouldn't be detected because only some of the criteria match the ruleset or signature. False positives can be reduced by further defining the ruleset or eliminating the match on that particular signature. False negative events are not detected but should be. False negatives can be reduced by layered defenses.

Each alert is analyzed for relevance to the operating systems and infrastructure. The alert will be handled based on the criticality of the alert. Most products offer paging or emailing of alerts in addition to logging. Some ID systems can also be set up to react to an alert. Reacting to alerts can be dangerous as it may backfire or you may drop a connection based on a false positive. Reactionary techniques include slowing down a port scan, dropping a connection or blocking all traffic with the ‘suspicious’ IP. The more sever techniques include dropping connection to the Internet, sending false responses to lure an attacker and reset kills.

The goal is to find a balance between alerting enough and not too much. If there are too many alerts if is hard for the security officer to continue to be attentive. On the other hand there could be missed alerts if alerts with high false positives are eliminated. If you are emailing or paging out alerts, the number of alerts should be reduced to a manageable amount for email. This allows alerts to be email to a security team rather than log review. This is referred to as a push technology instead of a pull technology where logs are queried when time allowed.

Tune It - Is this Normal

An important element of a successful intrusion detection system is an alert security officer. This fine tuning period is when the security officer learns what is normal for network-based alerts. They learn the normal logon patterns of staff and regular events on particular boxes using host-based sensors. They learn the fluctuations in alerts as events like Code-Red and Nimda infiltrate the Internet.

While investigating alerts, an astute security officer will look for corroborating evidence in web server, system event, firewall, router or switch logs. It is always easier to determine alert criticality with more information. Information from other logs will help create a clearer picture of the event or events.

Maintain It

In some respects the real work doesn't begin until after the *design it* and *tune it* phase. What good is your alerting and logging if you don't have the manpower or the skills for follow up and your signatures are outdated?

Maintain It - Alert Follow-up

After the 'tune it' period the Security Officer will know how to react to many alerts. However, there will still be new alerts and regular alerts that require investigation. This can include tracking events through multiple logs. There is often action required and documentation of actions taken. The security officer may be dealing with a compromised machine or eradication or may even end up convening the Computer Incident Response Team. Ensure that alert follow-up is a daily activity. Decide who will follow up on alerts and how quick the response will be.

Maintain It - Signature Updates

Intrusion detection products are based on rule-sets or signature databases. Updates should be applied as soon as an update is available so that the ID system can alert on the latest vulnerabilities. Some products will update automatically but corporate policy or network infrastructure may restrict automation of updates. Whether updates are done manually or automatically, the security officer must ensure that updates are always current. It should also be noted that as each new update is applied, a new influx of alerts could follow. All need to be assessed for criticality and relevance.

Maintain It - Security Officers Update

It is also important for security officers to keep up to date with new vulnerabilities and to spend the time assessing and determining criticality of new alerts. Time is well spent keeping up to date with changes to hosts, networks, employee usage or other details which keep you most familiar with your infrastructure. This builds the in-house skill required of an alert security officer.

Summary:

As Pete Lindstrom, senior security analyst at Hurwitz Group pointed out, "IDS is like a Christmas puppy." People just don't realize it is a lot of work to care for that puppy. (www.hurwitz.com). Successful implementation of an IDS requires a commitment of time. Management does not always budget and plan for each of the *design it, tune it and maintain it* stages of an ID system. This investment of time results in an effective ID system, which is a critical component of any network defense.

References:

Zirkle, Laurie and Sans Institute Resources "Intrusion Detection FAQ. What is host-based intrusion detection?" 2000. http://www.sans.org/newlook/resources/IDFAQ/host_based.htm (2Jan2002)

Thurman, Mathias "Zen and the Art of Intrusion Detection." 12Mar2001. http://www.computerworld.com/cwi/story/0,1199,NAV65-663_STO58458_NLTS,00.html, (24Nov2001)

Internet Security Systems "Real Secure Server Sensor" August 2001. http://documents.iss.net/literature/RealSecure/rs601_ss_faq.pdf (20Nov2001)

Brady, Phil and Money, Michael and Worstell, Karen "Should Communication between the Sensor and the Monitor be Encrypted?" SANS 2000. http://www.sans.org/newlook/resources/IDFAQ/communication.htm (3Jan2002)

Bace, Rebecca. "An Introduction to Intrusion Detection and Assessment". http://www.secinf.net/info/ids/intrusion/ (29Dec2001)

Watson, Peter "Best Approach to Computer Security is a Layered Approach" SANS 2000 http://www.sans.org/newlook/resources/IDFAQ/layered_defense.htm (2Jan2002)

Northcutt, Stephen. and Novak, Judy. Network Intrusion Detection An Analyst's Handbook Second Edition Indianapolis: New Riders, September 2000. 157-159, 368-373

Tipton, Harold and Krause, Micki. Information Security Management 4th Edition Washington: Auerbach, 2000.

Northcutt, Stephen. Track 3 - Network Based Intrusion Detection Tutorial 1, SANS 2000, 2001 1-6

McClure, Stuart and Scambray, Joel and Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions Berkeley: Osborne/McGraw-Hill, 1999. 28, 124, 308,315, 348-249

ASSIGNMENT 2

NETWORK DETECTS - TRACE #1

HTTP_Campas' Source Address: **212.154.190.160** Source Port: 1739 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:52:28 Protocol: TCP (6) Priority: high Actions mask: 0x244 Event Specific Information: URL: /cg%69-b%69%6E/ca%6D%70a%73 OBJECT: /cgi-bin/campas 2 similar attempts on same day, same SRC IP	**HTTP_Cold_Fusion'** Source Address: **212.154.190.160** Source Port: 1654 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:51:53 Protocol: TCP (6) Priority: high Actions mask: 0x244 Event Specific Information: URL: /cf%64%6Fc%73/%65%78%70%65val/%65%78 %70 %72calc.cf%6D OBJECT: /cfdocs/expeval/exprcalc.cfm 4 similar attempts on same day, same SRC IP
HTTP_DotDot' Source Address: 212.154.190.160 Source Port: 1731 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:52:23 (FIREWALL SHOWS as 12:47:24) Protocol: TCP (6) Priority: high Actions mask: 0x244 Event Specific Information: URL: /../../../../../../../.././/%65%74c/%70a%73%73w%64 OBJECT: /etc/passwd QUERY: Event Specific Information: URL: ../../../../../../%73ca%6E64%69%73%6B.l%6Fg OBJECT: /scandisk.log (LOTS) QUERY: Event Specific Information: URL: ....../au%74%6F%65 %78%65c.ba%74 OBJECT: /autoexec.bat: 25 similar attempts on same day, same SRC IP	**HTTP_IIS_Showcode'** Source Address: 212.154.190.160 Source Port: 1438 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:49:59 Protocol: TCP (6) Priority: medium Actions mask: 0x244 Event Specific Information: URL: /%6D%73a%64c/Sa%6D%70l%65%73/S%65l%65c%74%6F%72/%73%68%6Fwc%6F%64%65.a%73%70 OBJECT: /msadc/Samples/Selector/showcode.asp 4 similar attempts on same day, same SRC IP.
HTTP_IIS_Obtain_Code. Source Address: 212.154.190.160 Source Port: 1603 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:51:33 Protocol: TCP (6) Priority: medium Actions mask: 0x244 Event Specific Information: URL: /gl%6Fbal.a%73a%3F+.%68%74%72 OBJECT: /global.asa?+.htr 10 similar attempts on same day, same SRC IP	**HTTP_Unix_Passwords'** Source Address: 212.154.190.160 Source Port: 3779 Source MAC Address: 00:02:4B:B9:08:D0 Destination Address: **OurWeb server** Destination Port: HTTP (80) Destination MAC Address: 00:50:8B:5E:E1:07 Time: Monday, November 05, 2001 12:17:07 Protocol: TCP (6) Priority: high Actions mask: 0x244 Event Specific Information: URL: /%74a%72a%6E%74%65lla/cg%69-b%69%6E/%74%74aw%65b%74%6F%70.cg%69/?ac%74%69%6F%6E=%73%74a%72%74&%70g= OBJECT: /tarantella/cgi-bin/ttawebtop.cgi/ QUERY: action=start&pg=../../../../../../../../../../../../../../../etc/passwd 23 similar attempts on same day, same SRC IP

1. SOURCE OF TRACE

The source of this trace is from our company network.

2. DETECT WAS GENERATED BY:

RealSecure intrusion detection (version 5.0) detected each of these 6 events as either unauthorized access or suspicious activity. The following fields were used in the alerts:

Type	Name of signature that event matched
Source Address	IP address of system attempting connection
Source Port	Specific port used to originate TCP/IP or UDP connection
Source MAC Address	Unique hardware address of system attempting connection

Destination Address	IP address of target system
Destination Port	Specific TCP/IP or UDP port on target system while connection was attempted
Destination MAC Address	Unique hardware address of target system
Time	Day, Date and Time of connection attempt
Protocol	The communications 'language' (i.e. TCP, UDP, etc) of connection attempt
Priority	Real Secure's priority based on High, Med or Low
Actions mask	The field that selectively includes or excludes certain values from the Real Secure database of signatures.
Event Specific Information	URL, Object or Query matching a signature in the Real Secure database.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED:

All attacks were 'GET' requests or 'Unauthorized Access' requests. The intruder is attempting to gather information and gain access from 212.154.190.160. When reconnaissance is attempted, it is most likely that spoofing is not involved.

4. DESCRIPTION OF ATTACK:

The attack occurred on 5Nov2001 between 12:10:13 and 13:18:26. Most likely an attack tool was used to run scripts on the many common vulnerabilities. There were a total of 728 IIS Log entries from 19:15:37 to 20:24:03 on 5Nov2001 from IP 212.154.160. Times are recorded in GMT (Greenwich Mean Time) which is 7 hours ahead of our local time. Therefore the IIS events correspond to the Firewall activity between 12:10:13 and 13:18:26. The following table provides Internet Security Systems' Real Secure description of the attacks as found on the Real Secure console. Similar descriptions can also be found within the Signature Reference Guide found at http://documents.iss.net/literature/RealSecure/RS_Signatures_6.0.pdf.

HTTP_Campas
TYPE: Unauthorized access attempt
DESC: This is an attack against web servers making use of the campas cgi-bin script. If attack successful, allows execution of command. Web servers typically use Common Gateway Interface (CGI) programs. There is a wide category of CGI vulnerabilities. CGI programs facilitate functions such as web page data collection and verification. The risk with CGI programs is that it can provide unauthorized access to the web server operating system resulting in defaced web pages, loss of data and compromised machines.
AFFECTED: Old NCSA web servers
REMOVE VULNERABILITY: Upgrade HTTP Server to latest version and also remove cgi-bin script. All sample programs should be removed and programmers should be aware of this risk to decrease risk. Whisker (a scanning tool) can be used to understand risks of vulnerable CGI scripts on your web server. http://www.wiretrip.net/rfp/

CVE-1999-0146
CVE-1999-0067, CVE-1999-0346, CVE-2000-0207, CAN-1999-0509,
CVE-1999-0021, CVE-1999-0039, CVE-1999-0058, CVE-2000-0012, CVE-2000-0039,
CVE-2000-0208, CAN-1999-0455, CAN-1999-0477

HTTP_Cold_Fusion
TYPE: Unauthorized access attempt
DESC: This is an attack against web servers making use of sample scripts. A sample script with Cold fusion (up to version 4.0) could allow attacker to view or delete files. The example application allows outside access to upload, read or execute files by spoofing the HTTP Host variable in the Web Publish example script and the Email example script. Most web servers are delivered with sample programs and scripts. The severity of this vulnerability is rated as high.
AFFECTED: Macromedia, Cold Fusion 4.5
REMOVE VULNERABILITY: Upgrade HTTP Server to latest version and remove the Web Publish and eMail sample scripts. All sample programs should be removed and programmers should be aware of this risk. Whisker (a scanning tool) can be used to understand risks of vulnerable CGI scripts on your web server. http://www.wiretrip.net/rfp/

CAN-2001-0535

HTTP_DotDot
TYPE: Unauthorized access attempt.
DESC: This is an attack against web servers via a dot dot attack. The attack can use the eXtropia bbs_forum.cgi script. This signature recognized an attack to attempt to obtain information above the server root directory. Web servers vulnerable to this attack will allow remote users to list the contents of any directory on the system during the attack. Another directory traversal vulnerability in Search.cgi in LB5000 LB5000II 1029 and earlier allows remote attackers to overwrite files and gain privileges via .. (dot dot) sequences in a member name cookie.
AFFECTED: IIS Servers are affected
REMOVE VULNERABILITY: Upgrade IIS server to latest version. Ensure all CGI programs are legitimate and that programmers are aware of this risk. Whisker (a scanning tool) can be used to understand risks of vulnerable CGI scripts on your web server. http://www.wiretrip.net/rfp/

CVE-2001-0123 CAN-2001-0842

HTTP_IIS_Obtain_Code
TYPE: Unauthorized access attempt.
DESC: Attack against IIS servers using .htr scripts to either slow the server's response or obtain source code of certain types of files under very restricted conditions. Source Code fragment can be obtained using +.htr The signature detects HTTP GET requests that include the string "t.htr". No False Positives or False Negatives. LOW RISK

Microsoft patch MS00-31"eliminates two security vulnerabilities that are unrelated except by virtue of the fact that both exist in the ISAPI extension that provides web-based password administration via .HTR scripts.

- The "Undelimited .HTR Request" vulnerability is a denial of service vulnerability. If a malicious user provided a password change request that was missing an expected delimiter, the algorithm would conduct an unbounded search. This would prevent it from servicing additional .HTR requests, and could also slow the overall response of the server.
- The ".HTR File Fragment Reading" vulnerability could allow fragments of certain types of files to be read by providing a malformed request that would cause the .HTR processing to be applied to them. However, the vulnerability could only be exploited under extremely restrictive conditions, and the most valuable data in the files would be the least likely to actually appear in the fragments sent to the user.

Neither of these vulnerabilities would allow data to be added, deleted or changed on the server, nor would they allow any administrative control on the server to be usurped. Although .HTR files are used to allow web-based password administration, neither of these vulnerabilities involves any weakness in password handling. Also, if security best practices have been followed, and unneeded script mappings have been removed, many customers will have removed the .HTR script mapping and thus be unaffected by either vulnerability. "
AFFECTED: IIS 4 and 5 unpatched
REMOVE VULNERABILITY: If .HTR functionality is not required then disable the >HTR script mapping. Ensure all scripts are legitimate and that programmers are aware of these vulnerabilities.

MS Bul MS00-031, MS01-004

HTTP_IIS_Showcode
TYPE: Suspicious activity
DESC: An attack against a web server using the showcode.asp sample files. These can be remotely exploited to read files.
AFFECTED: Web server with sample showcode files.
REMOVE VULNERABILITY: Upgrade HTTP Server to latest version and remove showcode sample scripts. All sample programs should be removed.

CAN-1999-0736

HTTP_Unix_Passwords
TYPE: Unauthorized access attempt
DESC: An attack to gain root access using a buffer overflow in the HPUX passwd command. This allows local users to gain root privileges via a command line option. An attempt to access /etc/passwd/file. The severity is rated at high.
AFFECTED: Unix.
REMOVE VULNERABILITY: Windows O/S not affected.

CVE-1999-0962

5. ATTACK MECHANISM:

HTTP_Campas: This is an attack against web servers making use of the campas cgi-bin script.

HTTP_Cold_Fusion: This is an attack against webservers making use of sample scripts.

HTTP_DotDot: This is an attack against webservers via a dot dot attack.

HTTP_IIS_Obtain_Code: Attack against IIS servers using .htr scripts to either slow the server's response or obtain source code of certain types of files under very restricted conditions.

HTTP_IIS_Showcode: An attack against a webserver using the showcode.asp sample files.

HTTP_Unix_Passwords: An attack to gain root access using a buffer overflow in the HPUX passwd command.

These were all part of an automated attack with over 700 entries in just over an hour. These are *stimuli*, which target access attempts and reconnaissance on our web server. The web server is the most visible and publicly exposed box and this was a definite attempt to gain information or access by multiple web server vulnerabilities.

6. CORRELATIONS:

The web server log corroborated the events detected and logged by the intrusion detection product. The following extract from the web server show traffic from the same source IP from 19:15:37 until 20:24:03. All commands were 'GETS' and all were one of the following codes: 200 = Successful - OK, 206 = Successful - Partial Content, 304 = Redirection - Not Modified, 400 = Client Error - Bad Request, 403 = Client Error - Forbidden, 404 = Client Error - Not found, 500 = Server Error - Internal Server Error

Greenwich Mean Time	CMD	CODE	String, Query or URL
19:15:37	GET	200	/default.asp - 200 1871 18 0 HTTP/1.0 - - -
19:15:37	GET	404	/winnt/system32/cmd.exe /c+%64%69%72 404 604 171 0 HTTP/1.0 - - -
19:15:39	GET	404	/Demon/LookFor/Exploit.dm - 404 604 107 0 HTTP/1.0 - - -
19:15:39	GET	404	/windows/system32/cmd.exe /c+%64%69%72 404 604 175 0 HTTP/1.0 - - -
19:15:41	GET	404	/win2000/system32/cmd.exe /c+%64%69%72 404 604 169 0 HTTP/1.0 - - -
19:15:41	GET	404	/winnt/system32/cmd.exe /c+%64%69%72 404 604 167 0 HTTP/1.0 - - -
19:15:42	GET	404	/winnt/system32/cmd.exe /c+%64%69%72 404 604 153 0 HTTP/1.0 - - -
19:15:43	GET	404	/windows/system32/cmd.exe /c+%64%69%72 404 604 171 0 HTTP/1.0 - - -
19:15:44	GET	404	/win2000/system32/cmd.exe /c+%64%69%72 404 604 165 0 HTTP/1.0 - - -
19:15:44	GET	404	/windows/system32/cmd.exe /c+%64%69%72 404 604 157 0 HTTP/1.0 - - -
19:15:45	GET	200	/default.asp - 200 2221 308 0 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) - -
19:15:45	GET	404	/win2000/system32/cmd.exe /c+%64%69%72 404 604 151 0 HTTP/1.0 - - -
19:15:46	GET	404	/winnt/system32/cmd.exe /c+%64%69%72 404 604 161 0 HTTP/1.0 - - -
19:15:47	GET	200	/topbnr.htm - 200 9010 318 0 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) ASPSESSIONIDQQGQGGZE=JKDLFMJBNMJBGOGMKAKOM
19:15:47	GET	404	/windows/system32/cmd.exe /c+%64%69%72 404 604 165 30 HTTP/1.0 - - -
19:15:47	GET	404	/winnt/system32/cmd.exe /c+%64%69%72 404 604 164 0 HTTP/1.0 - - -
19:15:49	GET	200	/index2.htm - 200 1222 318 0 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) ASPSESSIONIDQQGQGGZE=JKDLFMJBNMJBGOGMKAKOM
19:15:49	GET	404	/windows/system32/cmd.exe /c+%64%69%72 404 604 168 0 HTTP/1.0 - - -
19:15:50	GET	404	/win2000/system32/cmd.exe /c+%64%69%72 404 604 159 10 HTTP/1.0 - - -
19:15:51	GET	200	/nav.htm - 200 4762 325 0 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) ASPSESSIONIDQQGQGGZE=JKDLFMJBNMJBGOGMKAKOMOJE
19:15:51	GET	404	/win2000/system32/cmd.exe /c+%64%69%72 404 604 162 0 HTTP/1.0 - - -
			Log truncated …..

Other correlations: These attacks on web servers are documented through several different Common Vulnerabilities and Exposures (CVE) entries. CVE-1999-0146, CVE-1999-0067, CVE-1999-0346, CVE-2000-0207, CAN-1999-0509, CVE-1999-0021, CVE-1999-0039, CVE-1999-0058, CVE-2000-0012, CVE-2000-0039, CVE-2000-0208, CAN-1999-0455, CAN-1999-04, CAN-2001-0535, CVE-2001-0123 CAN-2001-0842, MS Bul MS00-031, MS01-004, CAN-1999-0736, CVE-1999-0962

Information on offending IP address: It was interesting to discover, by use of Sam Spade, that the source IP address range is assigned to the Country of Kazakhstan. Ripe "who is" look up http://www.ripe.net/rpsl provides the following information. Geek tools offered the same information.

```
    netname:       KZ-KAZAKTELECOM-990707
    descr:         PROVIDER
    country:       KZ
    admin-c:       KNIC1-RIPE
    tech-c:        KNIC1-RIPE
    status:        ALLOCATED PA
    mnt-by:        RIPE-NCC-HM-MNT
    changed:       hostmaster@ripe.net 19990707
    source:        RIPE
    route:         212.154.128.0/17
    descr:         Kazakhtelecom Data Network Administration
    origin:        AS9198
    mnt-by:        KNIC-MNT
    changed:       nic@online.kz 19990319
    source:        RIPE
    role:          Kazakhtelecom Network Information Center
    address:       Kazakhtelecom Data Network Administration
    address:       129 Panfilov
    address:       Almaty 480091
    address:       Kazakhstan
    phone:         +7 327-258-8254
    phone:         +7 327-263-8796
    fax-no:        +7 327-258-1425
    e-mail:        nic@online.kz
    trouble:       Questions and bug reports ... mailto: nic@online.kz
    admin-c:       LS6502-RIPE
    tech-c:        NG2502-RIPE
    tech-c:        MG3326-RIPE
    nic-hdl:       KNIC1-RIPE
    remarks:       Please call us 09:00 - 12:00 UTC only
    notify:        hm-dbm-msgs@ripe.net
    changed:       lserebryanik@online.kz 20010716
    source:        RIPE
```

7. EVIDENCE OF ACTIVE TARGETING:

All traffic originated from one IP. The probe was directed to OURWEBSERVER. However we were likely just one of many servers continually being probed. There has not been any other activity from this IP since 5Nov2001. Some of the probes were for Unix machines, (i.e. HTTP_Unix_Passwords), indicating that the script was run at random on our site. There are many web server hacking tools available at hacker sites, which could have generated this signature.

8. SEVERITY:

(Critical	**+ Lethal)**	**-**	**(System**	**+ Network Countermeasure)**	**=**	**Severity**

This is a critical box	Root access attempts are severe		The box is hardened with latest patches and service packs. Not all attacks are relevant to this box.	Box is behind FW, monitored by Real Secure and located in DMZ		
5	**3**	**-**	**4**	**5**	=	**-1**

9. DEFENSIVE RECOMMENDATION:

The web server at this site patched and service packed up to date. All sample files were removed. The IIS Log was reviewed and it appears that none of the intrusion attempts were successful. A product like AppScan or Whisker (UNIX) should be run to verify the legitimate CGI scripts. Products like Microsoft URLScan (an application layer filter), can block malicious traffic which is accepted through port 80 (HTTP) on the firewall. This would prevent the script from running on the web server. Additionally, egress filtering on the web server could prevent undesirable outbound traffic.

ATTACK	**COMMENT**
HTTP_Campas	Web server up to date
HTTP_Cold_Fusion	Not running Cold Fusion
HTTP_DotDot	IIS server up-to-date
HTTP_IIS_Obtain_Code	MS00-031 and MS01-004 applied
HTTP_IIS_Showcode	Code previously removed
HTTP_Unix_Passwords	Not affected

These SANS Top 20 Vulnerability site provides the following defense recommendations to protect against vulnerable CGI programs:

1. Remove all sample CGI programs from your production web server.
2. Audit the remaining CGI scripts and remove unsafe CGI scripts from all web servers.
3. Ensure all CGI programmers adhere to a strict policy of input buffer length checking in CGI programs.
4. Apply patches for known vulnerabilities that cannot be removed.
5. Make sure that your CGI bin directory does not include any compilers or interpreters.
6. Remove the "view-source" script from the cgi-bin directory.
7. Do not run your web servers with administrator or root privileges. Most web servers can be configured to run with a less privileged account such as "nobody."
8. Do not configure CGI support on Web Servers that do not need it.

10. MULTIPLE CHOICE TEST QUESTION:

Most of the following are valid IIS Log server Status Codes. Which one is not a valid Status Code?

a. 200 = Successful - OK and 206 = Successful - Partial Content
b. 304 = Redirection - Not Modified

c. 400 = Client Error - Bad Request, 403 = Client Error - Forbidden
d. 404 = Client Error - Not found
e. 500 = Server Error - Internal Server Error
f. 600 = Intrusion Denied

ANSWER: f is not a valid code. See http://www/w3/org/Protocols/HTTP/htresp.html for a list of all HTTP Status Codes.

NETWORK DETECTS - TRACE #2

```
'Email_Listserv_Overflow' event detected by the RealSecure network sensor
Details:
        Source Address: 206.112.74.59
        Source Port: 5088
        Source MAC Address: 00:02:4B:B9:08:D0
        Destination Address: OurMailServer
        Destination Port: E-mail (25)
        Destination MAC Address: 00:50:8B:5E:E1:07
        Time: Thursday, November 29, 2001 23:11:49
        Protocol: TCP (6)
        Priority: high
        Actions mask: 0x244
        Event Specific Information:
              Buffer Length: 460
```

1. SOURCE OF TRACE

The source of this trace is from our company network. It matched a firewall rule and was forwarded to Real Secure intrusion detection system. The ID system is monitoring traffic in a promiscuous mode (passive).

2. DETECT WAS GENERATED BY:

This traffic was logged and an alert generated because it matched a Real Secure ID signature from Real Secure (version 5.0). It was detected as it entered the network destined for the Mail Server. The signature, "eMail list server overflow" recognizes a buffer overflow.

Type and sensor	Name of signature that matched event and the network or host-based sensor that detected
Source Address	IP address of system attempting connection
Source Port	Specific port used to originate TCP/IP or UDP connection
Source MAC Address	Unique hardware address of system attempting connection
Destination Address	IP address of target system
Destination Port	Specific TCP/IP or UDP port on target system while connection was attempted
Destination MAC Address	Unique hardware address of target system
Time	Day, Date and Time of connection attempt
Protocol	The communications 'language' (i.e. TCP, UDP, etc) of connection attempt
Priority	Real Secure's priority based on High, Med or Low
Actions mask	The field that selectively includes or excludes certain values from the Real Secure database of signatures.
Event Specific Information	URL, Object or Query matching a signature in the Real Secure database.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED:

Upon investigating this alert, it was found there was lots of other SMTP activity from the same source IP. Though there was substantial traffic, it did not appear to be a DoS attack. If it were a buffer overflow, then the traffic would be directed to a legitimate IP, as often root access is the goal of the attacker. In this case it would most likely not be from a spoofed address.

4. DESCRIPTION OF ATTACK:

By sending a specific command to the Listserv software, an internal buffer in the program can be overflowed and commands can be executed on the machine on which Listserv is running. The following table provides Internet Security Systems' Real Secure description of the attack as found on the Real Secure console. Similar descriptions can also be found within the Signature Reference Guide found at http://documents.iss.net/literature/RealSecure/RS_Signatures_6.0.pdf.

Email_Listserv_Overflow
TYPE: Unauthorized Access Attempt
DESCRIPTION: A buffer overflow was attempted against the Listserv mailing list. With successful buffer overflow, command line access can be obtained.
AFFECTED: Really old versions of Listserv. UNIX only.
REMOVE VULNERABILITY: Upgrade your version of Listserv

Linux Security lists this vulnerability as COVERT-2000-07. A component on the list server web contains an unchecked buffer allowing the attacker to send a long query, overwrite the stack and replace data allowing execution of code. http://www.linuxsecurity.com/advisories/other_advisory-565.html

5. ATTACK MECHANISM:

This alert appeared to be a *stimulus* targeting our mail server. Further investigation revealed 34 accepted events on the firewall from 28Nov2001 21:48:13 to 30Nov2001 at 1:10:11. As this only produced one alert, it is most likely that the list server was malfunctioning. The FW log included our staff's email address. The staff member indicated they belonged to that list server but had not noticed any unusual traffic.

```
29Nov2001   23:11:49 accept   smtp   206.112.74.59   OurMailServer 5088
agent mail server orig_from <bounce-ms2k-securitydesign-8623605@list.cramsession.com> orig_to
<ourstaff@ourmail.ca>

29Nov2001   23:11:55  accept   smtp   206.112.74.59   OurMailServer 5088
agent mail dequeuer orig_from <bounce-ms2k-securitydesign-8623605@list.cramsession.com> orig_to <ourstaff@ourmail.ca>
from <bounce-ms2k-securitydesign-8623605@list.cramsession.com> to <ourstaff@ourmail.ca> reason Content Security Server
has approved the requested resource: CVP Server: file scanned & declared safe

28Nov2001   21:48:13  accept   smtp   206.112.74.59   OurMailServer 13458
 agent mail server orig_from <bounce-ms2k-pro-8623604@list.cramsession.com> orig_to <ourstaff@ourmail.ca>  116997

28Nov2001   21:48:18  accept   smtp   206.112.74.59   OurMailServer 13458
agent mail dequeuer orig_from <bounce-ms2k-pro-8623604@list.cramsession.com> orig_to <ourstaff@ourmail.ca>
from <bounce-ms2k-pro-8623604@list.cramsession.com> to <ourstaff@ourmail.ca> reason Content Security Server has
approved the requested resource: CVP Server: file scanned & declared safe
```

6. CORRELATIONS:

The intrusion detection logs correlate to the FW Logs as shown above. The linux security advisory at http://www.linuxsecurity.com/advisories/other_advisory-565.html correlates to the alert.

7. EVIDENCE OF ACTIVE TARGETING:

There is no evidence of targeting of this vulnerability to our mail server. Our staff subscribes to this list server. Real Secure indicates that there are no false positives. That this is always indicative of malicious intent. Perhaps it was an attempted compromise of the listserver at 206.112.74.59 resulting bounced messages to our staff as a result of the mail list. Alternatively, this could be a listserver malfunction at 206.112.74.59 resulting in an alert at our end (though Real Secure indicates there are no false positives).

8. SEVERITY:

(Critical	+ Lethal)	-	(System	+ Network Countermeasure)	=	Severity
Mail server is a critical box	Possible execution of unauthorized code		Root access attempts but doesn't affect windows O/S The box is hardened with latest patches and service packs.	Box is behind FW, monitored by Real Secure and located in DMZ		
5	4	-	4	5	=	0

9. DEFENSIVE RECOMMENDATION:

We are not running any version of listserv or UNIX for that matter. The analyst advised the staff member to watch for any unusual traffic from that source.

General defenses include applying applicable patches and the latest service packs. Windows NT/2000 disk drives should be NTFS formatted with suitable access control lists. The mail server should not have an open relay.

10. MULTIPLE CHOICE TEST QUESTION:

How do listservers deal with incorrect email addresses?

a. When an email address is incorrect in some way (the system's name is wrong, the domain doesn't exist, whatever), the mail system will bounce the message back to the sender
b. The message will include the reason for the bounce.
c. Listservers determine how many times an email must bounce before it is removed from the list.
d. All of the above.

ANSWER: d

NETWORK DETECTS - TRACE #3

```
21-May-01   2:42:21    accept    http    198.107.213.105    OUR.WEB.SRV
21-May-01   2:57:27    accept    http    12.27.166.105      OUR.WEB.SRV
21-May-01   3:02:07    accept    http    206.229.153.105    OUR.WEB.SRV
21-May-01   3:03:17    accept    http    4.20.90.105        OUR.WEB.SRV
21-May-01   3:26:39    accept    http    216.52.169.65      OUR.WEB.SRV
21-May-01   4:30:41    accept    http    207.86.73.105      OUR.WEB.SRV
21-May-01   4:45:51    accept    http    206.98.113.105     OUR.WEB.SRV
21-May-01   5:55:08    accept    http    4.20.90.105        OUR.WEB.SRV
21-May-01   6:34:59    accept    http    198.107.213.105    OUR.WEB.SRV
21-May-01   6:41:00    accept    http    12.27.166.105      OUR.WEB.SRV
21-May-01   6:42:09    accept    http    207.86.73.105      OUR.WEB.SRV
21-May-01   6:55:05    accept    http    206.64.105.105     OUR.WEB.SRV
21-May-01   7:48:26    accept    http    216.52.169.65      OUR.WEB.SRV
21-May-01   8:08:30    accept    http    12.27.166.105      OUR.WEB.SRV
21-May-01   8:22:30    accept    http    206.98.113.105     OUR.WEB.SRV
21-May-01   8:48:22    accept    http    206.229.153.105    OUR.WEB.SRV
21-May-01   8:48:24    accept    http    206.64.105.105     OUR.WEB.SRV
21-May-01   10:03:24   accept    http    206.98.113.105     OUR.WEB.SRV
21-May-01   10:18:17   accept    http    4.20.90.105        OUR.WEB.SRV
21-May-01   11:10:29   dropped   ICMP    206.64.105.105     OUR.WEB.SRV
21-May-01   11:12:45   dropped   ICMP    12.27.166.105      OUR.WEB.SRV
21-May-01   13:17:25   dropped   ICMP    206.229.153.105    OUR.WEB.SRV
21-May-01   13:36:29   dropped   ICMP    4.20.90.105        OUR.WEB.SRV
21-May-01   13:39:46   dropped   ICMP    12.27.166.105      OUR.WEB.SRV
21-May-01   14:33:29   dropped   ICMP    216.52.169.65      OUR.WEB.SRV
21-May-01   14:42:22   dropped   ICMP    4.20.90.105        OUR.WEB.SRV
21-May-01   15:17:04   dropped   ICMP    198.107.213.105    OUR.WEB.SRV
21-May-01   15:30:20   dropped   ICMP    207.86.73.105      OUR.WEB.SRV
21-May-01   15:48:22   dropped   ICMP    206.98.113.105     OUR.WEB.SRV
21-May-01   16:27:26   dropped   ICMP    206.98.113.105     OUR.WEB.SRV
21-May-01   16:55:33   dropped   ICMP    206.64.105.105     OUR.WEB.SRV
21-May-01   17:28:09   dropped   ICMP    4.20.90.105        OUR.WEB.SRV
21-May-01   17:42:12   dropped   ICMP    206.229.153.105    OUR.WEB.SRV
21-May-01   17:44:19   dropped   ICMP    12.27.166.105      OUR.WEB.SRV
21-May-01   18:18:43   dropped   ICMP    206.64.105.105     OUR.WEB.SRV
21-May-01   18:20:57   dropped   ICMP    12.27.166.105      OUR.WEB.SRV
21-May-01   18:45:41   dropped   ICMP    207.86.73.105      OUR.WEB.SRV
21-May-01   19:06:14   dropped   ICMP    198.107.213.105    OUR.WEB.SRV
21-May-01   19:52:38   dropped   ICMP    206.64.105.105     OUR.WEB.SRV
21-May-01   20:28:20   dropped   ICMP    4.20.90.105        OUR.WEB.SRV
21-May-01   21:14:45   dropped   ICMP    206.98.113.105     OUR.WEB.SRV
21-May-01   22:31:30   dropped   ICMP    216.52.169.65      OUR.WEB.SRV
```

1. SOURCE OF TRACE

This company's firewall logged this traffic.   The increase in dropped ICMP packets caught the analyst's eye.

2. DETECT WAS GENERATED BY:

A repeated pattern of dropped ICMP traffic from several IPs caught the analyst's eye. This warranted further investigation. The trace above includes Date, Time, Action, Protocol, Source IP and Destination IP.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED:

At this point we weren't sure what the traffic indicated. The number of different source IPS and the number of events at first, lead us to believe in probability of a distributed denial of service attack. IPs initiating the ICMPs were all directing the packet to our web server and typically in a denial of service attack the attacker hides behind a spoofed IP. On the other hand if this was a slow information gathering attempt by several different IPs over several days, the IPs would not likely be spoofed.

4. DESCRIPTION OF ATTACK:

There were 17 attempts from various IPS during the period of 6:45 to 7:04 on 21May2001. The firewall policy drops and logs all ICMP packets inbound. All accepted http packets are logged.
On this particular day, the security analyst detected a pattern of dropped ICMP request events. The investigation lead to the discovery of daily attempts to send ICMP messages to our web server from several different ISP. This appeared to be persistent ICMP traffic from several hosts specifically targeted for our web server. This activity had not caused any alerts by the ID system and the volume of activity had not caused any bandwidth issues. If this was a denial of service attempt it was not successful.

ICMP can be maliciously used for reconnaissance or covert channels as well as denial of service. This was not a case of reconnaissance, as mapping was not used. All traffic was directed only to the web server and not sent to a broadcast address or multiple hosts on the same subnet. This wasn’t a Smurf attack or Loki as we were seeing echo requests not unsolicited replies.

A Ping Flood consists of sending a continuous series of ICMP Echo Request (Ping) packets to which the target replies. The requests and replies can slow the network or effectively disable it. This could not be categorized as a Ping Flood attack.

A Tribe Flood Network attack commands multiple hosts to attempt an ICMP echo request flood against a target. The volume of hosts and volume of replies were not sufficient to degrade or cause a denial of service of our web server. A TFN attack more closely matched this detect but it still wasn't the case.

As it turned out, this was unauthorized reconnaissance by a company called Internap. They were using ICMP requests and regular HTTP browsing to monitor and map our web server for their purposes.

5. ATTACK MECHANISM:

Internap claims this was not an attack. "The performance monitor simply sends a few ICMP Echo Request to your site, which is no way compromises security or constitutes an attack, even though occasionally an overzealous firewall might report it as such."

This unauthorized reconnaissance of monitoring and mapping was attempted through use of ICMP requests from multiple hosts. These all appeared to be *stimulus* events targeted at our web server.

6. CORRELATIONS:

The Web server's IIS Logs were verified and found many instances of this string. http://www.Internap.com/measurements/readme.html When a search was done in the IIS Log for this message the following IPs appeared. When the firewall log was cross-referenced for these IPS, the evidence between the 2 sources was supported.

IP	Name	SAM Spade
206.229.153.105	Address doesn't resolve	Sprint (NETBLK-SPRINTLINK-BLKQ) SPRINTLINK-BLKQ 206.228.0.0 - 206.231.255.255 InterNAP Network Services (NETBLK-SPRINT-347408-36289) SPRINT-347408-36289 206.229.153.0 - 206.229.153.255
206.64.105.105	Address doesn't resolve	UUNET Technologies, Inc. (NETBLK-NETBLK-UUNETCBLK64-67) NETBLK-UUNETCBLK64-67 206.64.0.0 - 206.67.255.255 InterNAP Network Services (NETBLK-UU-206-64-105-D1) UU-206-64-105-D1 206.64.105.0 - 206.64.105.255
12.27.166.105	Address doesn't resolve	AT&T ITS (NET-ATT) ATT 12.0.0.0 - 12.255.255.255 InterNAP Network Services (NETBLK-INTERNAP-166) INTERNAP-166 12.27.166.0 - 12.27.166.255
207.86.73.105	Address doesn't resolve	Business Internet, Inc. (NET-ICIX-MD-BLK12) 3625 Queen Palm Drive Tampa, FL 33619 US Netname: ICIX-MD-BLK12 Netblock: 207.86.0.0 -207.87.255.255
198.107.213.105	Address doesn't resolve	Verio, Inc. (NET-VRIO-198-106) 8005 South Chester Street, Englewood, CO 80112 US Netname: VRIO-198-106 Netblock:198.106.0.01 98.107.255.255
206.98.113.105	Address doesn't resolve	Cable & Wireless USA (NETTBLK-CW-06BLK) CW-06BLK 206.96.0.0 - 206.103.255.255 INTERNAP NETWORK (NETBLK-CW-206-98-113) CW-206-98-113 206.98.113.0 - 206.98.113.255
4.20.90.105	Address doesn't resolve	GENUITY (NET-GNTY-4-0) GNTY-4-0 4.0.0.0 - 4.255.255.255 Internap Network Services (NETBLK-INTERNAP-90-02) INTERNAP-90-02 4.20.90.0 - 4.20.90.255
216.52.169.65	Performance.hou.pnet.net	InterNAP Network Services (NETBLK-PNAP-8-98) PNAP-8-98 216.52.0.0 - 216.52.255.255 InterNAP Network Services, PNAP-HOU (NETBLK-PNAP-HOU-INAP-BB-1) PNAP-HOU-INAP-BB-1 216.52.168.0 - 216.52.169.255

Internap is a company, which monitors websites to improve access and performance from their customers to various websites, as well as to the rest of the Internet. The performance monitor sends an ICMP Echo Request to the target site. The impact on server load and traffic is intended to be minimal. They advise that if this causes some disruption your website will be excluded from further performance monitoring.

7. EVIDENCE OF ACTIVE TARGETING:

Internap, through various hosts was persistently targeting our web server for several days. They probably already had some reconnaissance information from the successful http traffic to our web server.

8. SEVERITY:

(Critical	**+ Lethal)**	**-**	**(System**	**+ Network Countermeasure)**	**=**	**Severity**
Critical web server	Unauthorized reconnaissance rates high		The box is hardened with latest patches and service packs.	Box is behind FW, monitored by Real Secure and located in DMZ. The FW drops incoming requests.		
5	4	-	5	5	=	-1

9. DEFENSIVE RECOMMENDATION:

Generally, the perimeter router or firewall should not allow ICMP echo requests and replies on your internal network. This prevents some ICMP activity like ICMP flood, SMURF and LOKI attacks from the outside.

To prevent further unauthorized reconnaissance and use ICMP requests, we contacted Internap Research and requested the activity be stopped. The firewall was monitored and no further activity occurred from any of the IPs used in the original detect. The company used many different IPS so blocking the IPS at the firewall may not prevent future traffic from yet another IP of Internap.

10. MULTIPLE CHOICE TEST QUESTION:

What does ICMP Type 8 indicate?

a. Echo Reply
b. Source Quench
c. Router Selection
d. Echo
e. Traceroute

ANSWER: d.

NETWORK DETECTS - TRACE #4

```
11/15-14:39:10.354669 0:2:4B:B9:8:D0 -> 0:50:8B:5E:E1:7 type:0x800 len:0x5C
209.115.205.80:137 -> OUR.WEB.SERVER:137 UDP TTL:123 TOS:0x0 ID:58371 IpLen:20 DgmLen:78
Len: 58
80 E2 00 10 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/15-14:39:10.855090 0:2:4B:B9:8:D0 -> 0:50:8B:5E:E1:7 type:0x800 len:0x5C
209.115.205.80:137 -> OUR.WEB.SERVER:137 UDP TTL:123 TOS:0x0 ID:59651 IpLen:20 DgmLen:78
Len: 58
80 E4 00 10 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
11/15-14:39:12.390183 0:2:4B:B9:8:D0 -> 0:50:8B:5E:E1:7 type:0x800 len:0x5C
209.115.205.80:137 -> OUR.WEB.SERVER:137 UDP TTL:123 TOS:0x0 ID:62467 IpLen:20 DgmLen:78
Len: 58
80 E6 00 10 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01                                            ..
```

1. SOURCE OF TRACE

Snort was running just outside our firewall to test the value of running Snort in conjunction with our ID product. The analyst detected the "AAA" signature while reviewing the logs.

2. DETECT WAS GENERATED BY:

The following snort options were used: -d dump the application layer, -e display the second layer header information, -v be verbose, -i2 listen on interface 2 and -l to log to directory.

```
The following fields are used in this trace:

DATE-time  Source MAC -> Destination MAC  type:   len:
Source IP and Port: -> Destination IP and Port:   Protocol:     Time to Live:    Type of
Service:    IPID:   Header Length:    Datagram Length:
TCP Header Length:
Application Layer Data                           Partial interpretation of data
```

Snort sorts output by Source IP and labels sessions with Source and Destination Port. The file UDP_137.137 caught the analyst's eye. The packet with "CKA AAA" string was recognized from the SANS ID course.

The rule that would trigger this alert, is "alert UDP any any ->$HOME_NET 137 (msg:'SMB Name Wildcard"; content: "CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/0000/";). It alerts on any traffic destined for host destination on port 137 (netbios-ns) with that string.

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED:

UDP scanning occurred on port 137 (netbios-ns). In a reconnaissance attack, spoofing is most likely not used. A reality check on the source IP can be performed by looking at the arriving TTL. The initial TTL can be guessed as either a UDP TTL of 255 from a Solaris 2.x or a UDP TTL of 128 from a VMX/UCS machine. Subtracting the TTL value from the trace (123) from each of the guessed values

of 255 or 128 provides a likely hop count for the packet to travel from source IP to our network. Each router decrements the value by one so this packet could have either traveled for 132 or 5 hops.
The following tracert repeats after reaching Interbaun on the 5th hop. The offending IP resolves to Interbaun with different IP. The tracert bounces back between the cb-199-185-131-248.interbaun.net and the ns21.interbaun.net systems for the remainder of the tracert. If the hop count is set to 100, it bounces back and forth for the 100 hops. This could be a misconfigured router or perhaps some bazaar plan to deflect pings.

This information unfortunately doesn't add validity to the opinion that the IP is not spoofed.

```
D:\>tracert 209.115.205.80

Tracing route to 080.209-115-205-0.interbaun.com [209.115.205.80]
over a maximum of 30 hops:

  1    10 ms     *       10 ms  209.115.152.26
  2    10 ms    10 ms    10 ms  v911.edtnabxmdr00.bb.telus.com [209.115.152.14]
  3    10 ms    10 ms    10 ms  c8-0-0.edtnabkddr01.bb.telus.com [205.233.111.134]
  4    10 ms    10 ms 10 ms  EDTNXJ-COMP02.ab.tac.net [209.115.219.133]
  5    10 ms    10 ms    10 ms  cb-199-185-131-248.interbaun.net [199.185.131.248]
  6    10 ms    20 ms    10 ms  ns21.interbaun.net [199.185.130.182]
  7    10 ms    10 ms    20 ms  cb-199-185-131-248.interbaun.net [199.185.131.248]
  8    10 ms    20 ms    10 ms  ns21.interbaun.net [199.185.130.182]   truncated …..
 truncated …..
 29    10 ms    20 ms    10 ms  cb-199-185-131-248.interbaun.net [199.185.131.248]
 30    10 ms    10 ms    20 ms  ns21.interbaun.net [199.185.130.182]
Trace complete.
```

4. DESCRIPTION OF ATTACK:

There were 16 of the same attempts all from 209.115.205.80 (interbaun.com) to OUR.WEB.SERVER. The events occurred between 14:39:10 .354669 and 14:39:19.768791. Traffic from port 137 (netbios-ns) to port 137 (netbios-ns) can be indicative of a nbtstat request.

There are many vulnerabilities of Netbios traffic, ports 137 - 139. It could be a worm looking for unprotected shares, it could be a port 137 (netbios-ns) scan or it could be an attacker searching for shared resources. CVE-1999-0288 describes a denial of service in WINS with malformed data to port 137 (netbios-ns).

SANS taught that Snort packet capture would recognize a nbtstat request when the packet contains the string of CKAAAA followed by the binary value of 0000. Snort reads the application layer and recognizes this string as a search for resources in the NetBIOS table. The firewall reported one accepted http event and three dropped events from this source IP during the period of 14:48:35 to 14:48:48.

5. ATTACK MECHANISM:

It appeared to be *stimulus* targeting of our web server for reconnaissance on port 137 (netbios-ns).

According the string " CKAAA…" this was a nbtstat request. Nbtstat requests normally occur in a windows environment within the network. A windows host that runs NetBIOS will automatically answer a nbtstat request.

However, nbstat or finger (for UNIX) can be used for intelligence gathering. Mitnick used finger to determine trust relationships. You can discover who is logged on to the system, when they logged on, when they last logged on, where they are logging on from and how long they have been idle. Nbtstat reveals the NetBIOS name of the machine, the workgroups, the logon name and other information like a master browser cookies. This use from outside the network appears to be a deliberate attempt to gain information from the NetBIOS table.

6. CORRELATIONS:

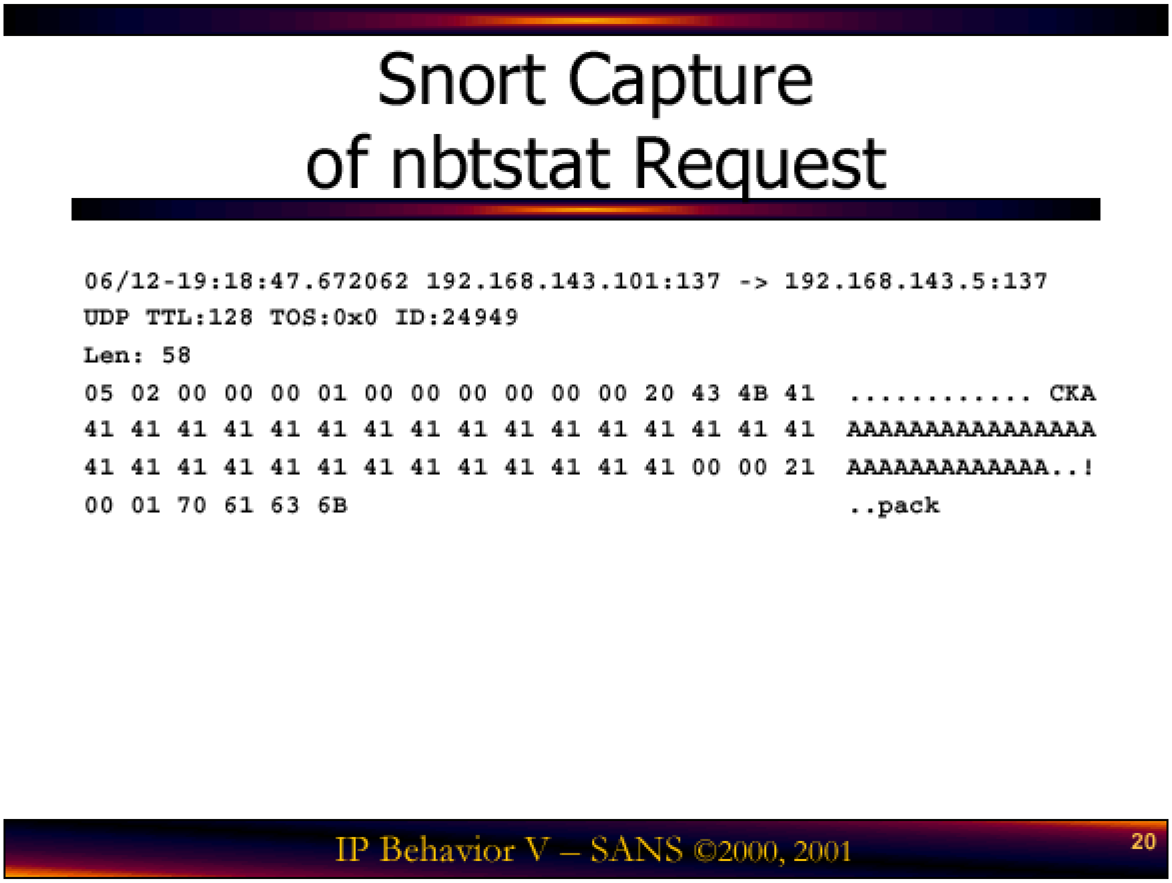
The firewall log verified that the activity was dropped and supported the Snort trace. The

Offending IP Address resolved to Interbaun.

```
nslookup 209.115.205.80
Server:  lithium.ab.tac.net
Address:  209.115.152.130

Name:    080.209-115-205-0.interbaun.com
Address:  209.115.205.80
```

RIPE, GEEK or other WHOIS tools did not provide further information.



Snort Capture
of nbtstat Request

```
06/12-19:18:47.672062 192.168.143.101:137 -> 192.168.143.5:137
UDP TTL:128 TOS:0x0 ID:24949
Len: 58
05 02 00 00 00 01 00 00 00 00 00 00 20 43 4B 41  ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAAA..!
00 01 70 61 63 6B                                ..pack
```

IP Behavior V – SANS ©2000, 2001

20

This sample from IP Behavior V - Microsoft Networking, page 20 correlates to Detect 4.

7. EVIDENCE OF ACTIVE TARGETING:

The event appeared specific to this host with repeated targeted attempts.

8. SEVERITY:

(Critical	**+ Lethal)**	**-**	**(System**	**+ Network Countermeasure)**	**=**	**Severity**
Web server is critical box	Attempts to gain information or access through shares		The box is hardened with latest patches and service packs.	Box is behind FW, monitored by Real Secure and located in DMZ. Netbios traffic is not allowed from outside the network		
5	**4**	**-**	**4**	**5**	**=**	**0**

9. DEFENSIVE RECOMMENDATION:

Inbound traffic to UDP port 137 (netbios-ns) should be blocked at the firewall to prevent reconnaissance of the NetBios table information. Related UDP port 128 (netbios-ns) should be blocked as well as TCP port 79 (finger) at the firewall or filtering router. Those boxes which are running SMB should be reviewed to ensure they are configured properly and only allow authorized access.

10. MULTIPLE CHOICE TEST QUESTION:

Port 137 (netbios-ns) activity on the Firewall means:

a. A possible attack to discover target server information.
b. A spread of an internet worm like network.vbs
c. More script kiddies have discovered how to use NBTSTAT
d. Normal Windows operating system behavior
e. All of the above

ANSWER: e. All of the above. Activity should be investigated.

NETWORK DETECTS - TRACE #5

```
[**] [1:937:2] WEB-FRONTPAGE _vti_rpc access [**]
[Classification: Attempted Information Leak] [Priority: 3]
11/27-22:17:57.931158 24.70.95.206:47639 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:10187 IpLen:20 DgmLen:468 DF
***AP*** Seq: 0xC1A10AB3  Ack: 0x85F4D5AD  Win: 0x8000  TcpLen: 20
[Xref => http://www.securityfocus.com/bid/2144]

Truncated …
11/27-22:17:59.660329 24.70.95.206:47831 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:13771 IpLen:20 DgmLen:468 DF
11/27-22:17:59.931447 24.70.95.206:47860 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:15307 IpLen:20 DgmLen:439 DF
11/27-22:18:00.128337 24.70.95.206:47876 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:16587 IpLen:20 DgmLen:468 DF
11/27-22:18:19.558792 24.70.95.206:49940 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:63435 IpLen:20 DgmLen:439 DF
11/27-22:18:19.730204 24.70.95.206:49967 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:64715 IpLen:20 DgmLen:468 DF
11/27-22:18:20.073792 24.70.95.206:50009 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:1996 IpLen:20 DgmLen:439 DF
11/27-22:18:20.245197 24.70.95.206:50041 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:9164 IpLen:20 DgmLen:468 DF
11/27-22:19:56.323386 24.70.95.206:50110 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:14802 IpLen:20 DgmLen:439 DF
11/27-22:19:56.551624 24.70.95.206:61175 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:16082 IpLen:20 DgmLen:468 DF
11/27-22:19:56.939997 24.70.95.206:61227 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:17618 IpLen:20 DgmLen:439 DF
11/27-22:19:57.114936 24.70.95.206:61246 -> OUR.WEB.SERVER:80
TCP TTL:58 TOS:0x0 ID:18898 IpLen:20 DgmLen:468 DF

 [**] [1:1201:1] WEB-MISC 403 Forbidden [**]
[Classification: Attempted Information Leak] [Priority: 3]
11/27-23:16:14.139195 OUR.WEB.SERVER:80 -> 24.70.95.206:61306
TCP TTL:127 TOS:0x0 ID:16799 IpLen:20 DgmLen:797 DF
***AP*** Seq: 0x87EDCC9E  Ack: 0x620E661B  Win: 0x1DAF  TcpLen: 20

[**] [1:1201:1] WEB-MISC 403 Forbidden [**]
[Classification: Attempted Information Leak] [Priority: 3]
11/27-23:43:55.068472 OUR.WEB.SERVER:80 -> 24.70.95.206:59039
TCP TTL:127 TOS:0x0 ID:4812 IpLen:20 DgmLen:797 DF
***AP*** Seq: 0xC2EFA9FE  Ack: 0x1C7820D4  Win: 0x1D77  TcpLen: 20
```

1. SOURCE OF TRACE:

All traffic was logged off our network with Windump. SNORT was run against the Windump log file and an alert was generated.

2. DETECT WAS GENERATED BY:

The alerts shown in this trace are standard SNORT alerts with field values as follows. This particular alert was based on the 'web-frontpage-rules' alert.

<table>
<tr><td colspan="6">Snort Rule alerted on</td></tr>
<tr><td colspan="2">Date</td><td>Time</td><td>Src IP and Port</td><td colspan="2">Dst IP and Port</td></tr>
<tr><td>Protocol</td><td>Time to Live</td><td>Type of Service</td><td>IP ID</td><td>Header Length</td><td>Datagram Length</td></tr>
</table>

TCP Flags	TCP Sequence	TCP ACK	TCP Window Size	TCP Header Length
Xref if provided in the rules file.				

The **WEB-FRONTPAGE _vti_rpc access** alert was generated by this SNORT rule.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-FRONTPAGE _vti_rpc
access"; flags: A+; uricontent:"/_vti_rpc"; nocase; reference:bugtraq,2144; classtype:web-application-
activity; sid:937; rev:3;)
```

3. PROBABILITY THE SOURCE ADDRESS WAS SPOOFED:

The Snort alert indicates attempted information leak. This Front Page Server Extensions (FPSE) vulnerability can be used for reconnaissance. Not only did the alert indicate a valid IP but we also saw significant legitimate traffic. This indicated that the IP was not spoofed.

4. DESCRIPTION OF ATTACK:

The offending IP was using FPSE vulnerabilities to attempt reconnaissance. The alert contained the _vti prefix. FrontPage was an original program developed by Vemeer Technologies Inc; hence the _vti_ prefixes. Some FPSE vulnerabilities can be used to orchestrate a denial of service attack using a malformed form or long URL. Other vulnerabilities can be used to gain unauthorized access to execute arbitrary commands.

MS00-100	'Malformed Web Form Submission' Vulnerability
CVE 2001-0096	FrontPage Server Extensions (FPSE) in IIS 4.0 and 5.0 allows remote attackers to cause a denial of service via a malformed form, aka the "Malformed Web Form Submission" vulnerability.
CVE 1999 - 0681	Buffer overflow in Microsoft FrontPage Server Extensions (PWS) 3.0.2.926 on Windows 95, and possibly other versions, allows remote attackers to cause a denial of service via a long URL
CVE 2001-0341	Buffer overflow in Microsoft Visual Studio RAD Support sub-component of FrontPage Server Extensions allows remote attackers to execute arbitrary commands via a long registration request (URL) to fp30reg.dll
CAN 1999-1376	Buffer overflow in fpcount.exe in IIS 4.0 with FrontPage Server Extensions allows remote attackers to execute arbitrary commands
CAN 2000-0114	**Frontpage Server Extensions allows remote attackers to determine the name of the anonymous account via an RPC POST request to shtml.dll in the /_vti_bin/ virtual directory.**
BUGTRAQ:20000203 CISADV000203	**2 MS Frontpage issues Cerberus Information Security Advisory (CISADV000203)**
CAN 2000-0122	Frontpage Server Extensions allows remote attackers to determine the physical path of a virtual directory via a GET request to the htimage.exe CGI program.

CAN 20000-0256	Buffer overflows in htimage.exe and Imagemap.exe in FrontPage 97 and 98 Server Extensions allow a user to conduct activities that are not otherwise available through the web site, aka the "Server-Side Image Map Components" vulnerability.
CAN 2000-0413	The shtml.exe program in the FrontPage extensions package of IIS 4.0 and 5.0 allows remote attackers to determine the physical path of HTML, HTM, ASP, and SHTML files by requesting a file that does not exist, which generates an error message that reveals the path
CAN 2000- 0709	The shtml.exe component of Microsoft FrontPage 2000 Server Extensions 1.1 allows remote attackers to cause a denial of service in some components by requesting a URL whose name includes a standard DOS device name.
CAN 2000-0710	The shtml.exe component of Microsoft FrontPage 2000 Server Extensions 1.1 allows remote attackers determine the physical path of the server components by requesting an invalid URL whose name includes a standard DOS device name.
BugTraq 2144	Refers to Summary of MS00-100

The puzzling piece of this attack was the volume of legitimate traffic from the same source IP as the offending FPSE alert. These alerts were detected on 27Nov2001 but traffic from this IP had been occurring for over a month. The traffic occurred several times a day as accepted HTTP (port 80) and HTTPS (port 443) events.

5. ATTACK MECHANISM:

These events were definitely *stimulus* from the source or offending IP. There was no record of traffic from our network prior to their stimulus as shown in the trace.

It appeared this offender tried to determine the name of the anonymous account via an RPC POST request to the shtml as seen in CVE 2000-0114. According to Bugtraq and Cerberous advisories it is possible to break outside of the web virtual root and gain unauthorized access to log files, to allow read access to the anonymous Internet account or the Everyone/guests group.

6. CORRELATIONS:

This detect really had us going. We dug into all the supporting evidence we could find in the IIS logs, FW logs and Named Pipe Logs (contains command/response transactions between the client and server). The logs indicate the offender was not successful in his attempt to access FPSE vulnerabilities.

However, due to the heavy and continuous volume of legitimate traffic from this IP we had to determine if other unauthorized activity was occurring. Our ISP was called and Shaw Cable was called about this activity discovered when investigating the one alert. The following correlate to the alert and activity from the offending IP.

DATE	TIME	ACTION	SERVICE	SCR IP	DST IP	S_PORT	Reason

28Nov2001	14:04:13	drop	48122	192.INSIDE.WEB	24.70.95.206	https	unknown established TCP packet
28Nov2001	14:34:35	drop	25548	192.INSIDE.WEB	24.70.95.206	https	unknown established TCP packet
28Nov2001	14:34:39	drop	25568	192.INSIDE.WEB	24.70.95.206	https	unknown established TCP packet
28Nov2001	14:34:39	drop	25569	192.INSIDE.WEB	24.70.95.206	https	unknown established TCP packet
1Dec2001	15:26:56	drop	25206	OUR.WEB.SERVER	24.70.95.206	https	unknown established TCP packet
1Dec2001	15:27:26	drop	25207	OUR.WEB.SERVER	24.70.95.206	https	unknown established TCP packet

SAM SPADE SAYS: Shaw Fiberlink ltd. (NETBLK-FIBERLINK-CABLE) 630 3rd Avenue SW, Suite 900 Calgary AB, 4L4 CA Netname: FIBERLINK-CABLE Netblock: 24.64.0.0 - 24.71.255.255
Coordinator: Shaw@Home (SH2-ORG-ARIN) internet.abuse@SHAW.CA

The IIS Log shows reams of successful traffic on both the 27Nov2001 and on the 28Nov2001. Here are the entries, which caused some of the alerts. This table shows TIME, Src IP, Dst IP, Action, Path or Client Server-uri-stem, IIS Status, Server Client-bytes, Client Server-bytes, Time-taken,

5:18:26	24.70.95.206	WEB.SER.VER	GET	/default.asp	**200**	2221	331	10	HTTP/1.1
5:18:26	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	344	10	HTTP/1.1
5:18:26	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	10	HTTP/1.1
5:18:28	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:18:28	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:18:28	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:18:28	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:18:47	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:18:49	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:18:49	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:18:49	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:18:50	24.70.95.206	WEB.SER.VER	GET	/default.asp	**200**	2221	302	0	HTTP/1.1
5:19:36	24.70.95.206	WEB.SER.VER	GET	/default.asp	**200**	2221	332	0	HTTP/1.1
5:20:25	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:20:25	24.70.95.206	WEB.SER.VER	GET	/_vti_inf.html	404	623	399	0	HTTP/1.1
5:20:25	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:20:25	24.70.95.206	WEB.SER.VER	**POST**	/_vti_bin/shtml.exe/_vti_rpc	405	851	469	0	HTTP/1.1
5:20:27	24.70.95.206	WEB.SER.VER	GET	/images/navigation/personalserv1.gif	**200**	1924	421	130	HTTP/1.1
5:21:33	24.70.95.206	WEB.SER.VER	GET	/default.asp	**200**	2221	357	11	HTTP/1.1
5:21:56	24.70.95.206	WEB.SER.VER	GET	/default.asp	**200**	2221	312	0	HTTP/1.1

Named Pipe Log:

What was bothersome was the volume of traffic which appeared normal all came from one IP with the exception of the few POST attempts around 5:18.

The Named Pipe Log is an ASCII based chronological file containing single line records for command/response transactions between the client and server. The Cookie field is one of many command transaction fields in this log.

The Named Pipe Log was matched to the IIS log using the session cookie. It quickly became apparent that many separate members were logging in through this same IP. It took some tracking at Shaw to get an answer. Finally someone in the Acceptable User Department determined that 24.70.95.206 is a proxy server which some home users opt to use to improvement connectivity speed.

7. EVIDENCE OF ACTIVE TARGETING:
This could have been a targeted attack by one offender sitting behind the proxy. There were several POST attempt to our web server within a short period of time. He quickly moved on when he was unsuccessful. All the other activity appears to be normal. We now know the offending IP is a proxy server.

8. **SEVERITY:**

(Critical	**+ Lethal)**	**-**	**(System**	**+ Network Countermeasure)**	**=**	**Severity**
Web server is a critical box.	Reconnaissance or subsequent unauthorized access could be very critical.		The box is hardened with latest patches and service packs and FPSE removed	Box is behind FW, monitored by Real Secure and located in DMZ		
5	5	**-**	4	5	=	1

9. DEFENSIVE RECOMMENDATION:
FPSE allow content management and processing of web forms. This functionality is shipped with Microsoft IIS. If FPSE is available on your server you could be vulnerable to a denial of service attack or reconnaissance. Remove all files with FPSE, which aren't in use.

Microsoft has a separate patch for both IIS 4.0 and IIS 5.0. Products like Microsoft's URL scan, an application layer firewall, can block malicious HTTP traffic which slips through port 80. Use of a vulnerability scanner would mitigate your web server's exposure. Cerberus has a vulnerability scanner, which detects FPSE. The scanner can be downloaded at http://www.cerberus-infosec.co.uk/cis.shtml

10. MULTIPLE CHOICE TEST QUESTION:
Front Page Server Extensions (FPSE) are:

a. Used for content managing
b. Used for processing of web forms
c. Used for denial of service via malformed forms.
d. Shipped with Microsoft IIS
e. All of the above

ANSWER: e. All of the above.

ASSIGNMENT 3
"ANALYZE THIS" SCENARIO

1. EXECUTIVE SUMMARY

I have prepared a security audit for UMBC University based on Snort data from 30Nov2001 to 4Dec2001. The report includes results of log crunching, log relationships, and top detects and talkers. Generally, there is a lot of traffic on services, which are normally restricted. There was evidence of ports used for file sharing, gnutela, napster, file transfers, and chat channels. On the one hand, this increases your risk, as there are many known vulnerabilities with these services. On the other hand, UMBC is committed to global classrooms, studying abroad, providing remote login for students and staff and most likely shared resources with other institutions. There is substantial traffic as noted within these five days. This amount of traffic creates visibility on the Internet and opportunity for reconnaissance attacks. The University will pay a price for allowing file-sharing programs by way of compromised machines, downtime and potential lost data. Recommendations for further securing the environment are included.

2. LOG RELATIONSHIP

Corroboration of logs provides more complete information and can be used to substantiate evidence in court. All the top IPs which were identified as sources of the MISC Large UDP Packet Alerts were also found in the scan logs. Correlations and examples are provided in Appendix B.

3. FILE LIST USED IN ANALYSIS

Alert_011130_gz.txt	17.8 MB	oos_Nov_30_2001_gz.txt	77 MB	Scans.0111130.txt	111 MB
Alert_011201_gz.txt	17.7 MB	oos_Dec_1_2001_gz.txt	45 MB	Scans.0111201.txt	43 MB
Alert_011202_gz.txt	15.4 MB	oos_Dec_2_2001_gz.txt	36 MB	Scans.0111202.txt	43 MB
Alert_011203_gz.txt	20.5 MB	oos_Dec_3_2001_gz.txt	25 MB	Scans.0111203.txt	51 MB
Alert_011204_gz.txt	17.4 MB	oos_Dec_4_2001_gz.txt	104 MB	Scans.0111204.txt	71 MB
Alert_ALL	89 MB	All OOS	287 MB	All Scans	319 MB

4. LIST OF DETECTS PRIORITIZED BY NUMBER OF OCCURRENCES

Top 10 Alert Destination Hosts

DST HOST	TOTAL	MAIN ALERT
MY.NET.100.165	58391	57559 - CS WEBSERVER - external web traffic
MY.NET.140.9	51582	47804 - MISC traceroute 2815 - ICMP Destination Unreachable (Host Unreachable 956 - ICMP Destination Unreachable (Administratively Prohibited)
MY.NET.111.221	48871	48427 - Misc Large UDP Packet
MY.NET.253.114	33880	32487 - WEB-MISC prefix-get //
MY.NET.70.134	32985	32954 - Misc Large UDP Packet
MY.NET.16.42	29095	29009 - Tiny Fragments - Possible Hostile Activity
MY.NET.70.148	27174	742 - MISC traceroute
MY.NET.70.148	27174	25833 - ICMP Echo Request BSDtype
MY.NET.1.3	20750	20694 - MISC source port 53 to <1024

MY.NET.1.5	17655	17634 - MISC source port 53 to <1024
MY.NET.1.4	17343	17282 - MISC source port 53 to <1024
MY.NET.70.42	15136	15112 - Watchlist 000220 IL-ISDNNET-990517
MY.NET.84.218	6004	6004 - Misc Large UDP Packet
207.207.132.1	4244	4244 - ICMP Echo Request BSDtype
MY.NET.163.85	1983	1883 - Watchlist 000220 IL-ISDNNET-990517

Top 10 Alert Source Hosts

SOURCE HOST	TOTAL	MAIN ALERT
61.153.17.188	40217	39801 - MISC Large UDP Packet
209.190.237.123	32986	32954 - MISC Large UDP Packet
MY.NET.8.1	29009	29009 - Tiny Fragments - Possible Hostile Activity
212.179.44.99	15112	15112 - Watchlist 000220 IL-ISDNNET-990517
61.150.5.19	14717	14717 - MISC Large UDP Packet
141.213.11.120	5113	4974 - ICMP Echo Request BSDtype
129.132.66.28	4639	4451 - ICMP Echo Request BSDtype
MY.NET.60.8	4375	4249 - ICMP Echo Request BSDtype
129.79.245.106	4310	4120 - ICMP Echo Request BSDtype
132.246.128.200	3743	3739 - CS WEBSERVER - external web traffic

Top 5 Scan Source Hosts	# Scans
MY.NET.5.75	327597
MY.NET.5.76	253339
MY.NET.87.50	68374
217.227.247.60	16867
MY.NET.	16056

The scan logs show that MY.NET.5.75 and MY.NET.5.76 are consistently scanning other internal addresses. Some activity from high ports in the 35,000 range but mostly all from src port 67 (Bootstrap Protocol) to dst port 68 (Bootstrap Protocol) using the bootstrap protocol server to client.

All of MY.NET.87.50 scan traffic was from either port 888 (UDP - access builder) or src port 999 (UDP - applix). Hacker uses of Port 999 includes chat power, deep throat, Foreplay and WinSatan. All the traffic on MY.NET.87.50 is destined for IP's off the network with a variety of dst ports. There was a high frequency of dst port 27005 (ephemeral). Some game monitoring programs communicate on port 27005. Here is a trace where 887 entries occurred within a short period of time. This traffic should be investigated.

```
Mth    Day  Time        SRC IP            SRC Port       DST IP             DST Port
Dec      1     15:14:58 MY.NET.87.50               999 ->   129.119.173.43          27005 UDP
Dec      1     15:15:15 MY.NET.87.50               999 ->   129.119.173.43          27005 UDP
Dec      1     15:15:19 MY.NET.87.50               999 ->   129.119.173.43          27005 UDP
Dec    1    15:15:23 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    15:15:28 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    15:15:31 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    15:15:35 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    15:15:39 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    15:15:47 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Truncated ….
Dec    1    16:13:22 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    16:13:26 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    16:13:30 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    16:13:34 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    16:13:38 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1    16:13:42 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1     4:13:46 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
Dec    1     4:13:46 MY.NET.87.50        999 ->   129.119.173.43        27005 UDP
```

This trace shows use of BattleNet (UDP) on Port 6112. The popular multiplayer game "Diablo" runs on this port.

```
Date      Time        Src IP and Port                    Dst IP and Port
Dec    1   15   45   43 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   45   47 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   45   51 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   45   53 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Truncated …
Dec    1   15   59   23 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   26 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   31 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   34 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   39 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   43 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   47 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   51 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   55 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   59   59 MY.NET.98.162       6112 ->    172.137.138.52           6112 UDP
Dec    1   15   26   27 MY.NET.98.162       6112 ->    172.137.244.235          6112 UDP
```

Top 5 Scan Destination Hosts	# Scans
MY.NET.152.45	5915
MY.NET.53.151	1637
209.205.178.3	3169
142.166.217.142	3376
24.180.10.152	1619

There were 749,960 scans on dst hosts. Some hosts had multiple scans but they were fast scans not over the period of 5 days. Most hosts didn't have multiple scans.

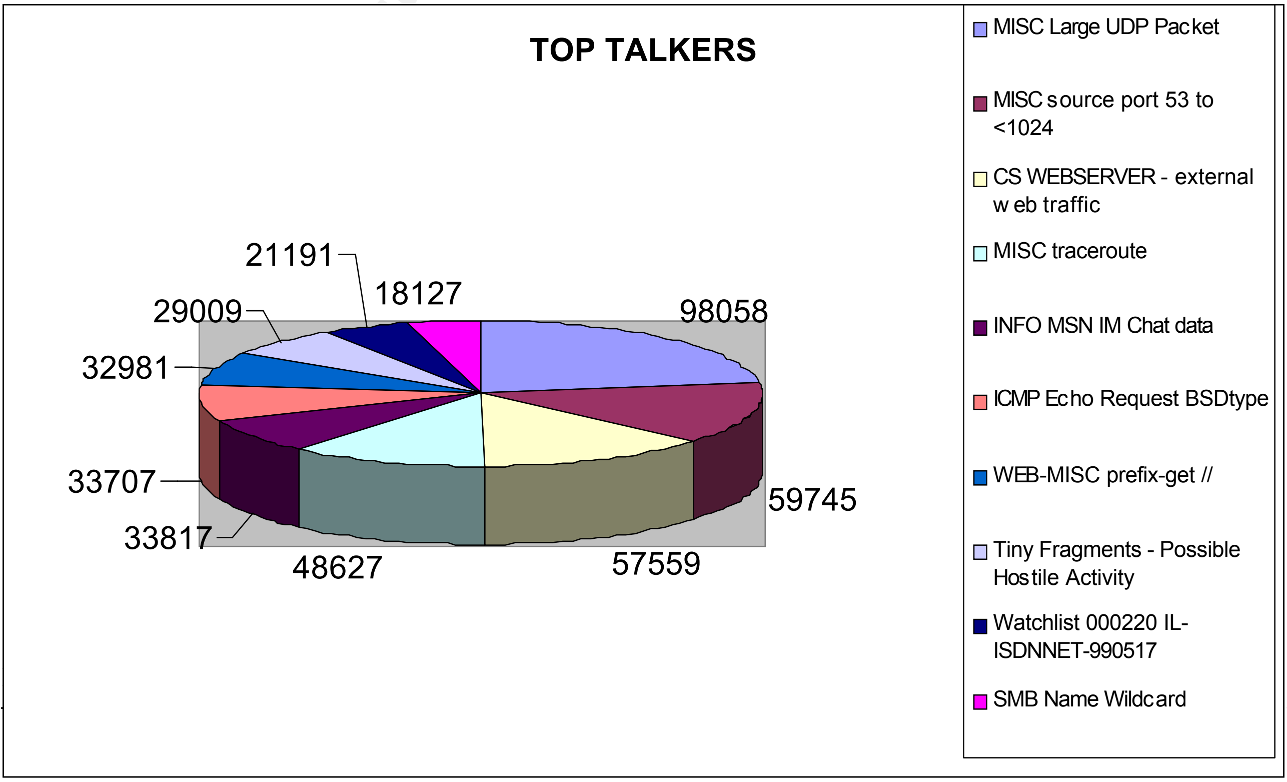
Some of the traffic to My Net.152.45 was on Port 0. This trace is part of 791 entries that occurred within less than 6 minutes. Source port of 0 is not normal and could be finger printing attempts.

```
Date         Time                Src IP and Port                  Dst IP and Port
Dec          1          15  14   47 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          15  14   50 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          15  14   55 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          15  14   59 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          15  15   40 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          15  15   44 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Truncated ….
Dec          1          16  20   14 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          16  20   17 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          16  20   22 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          16  20   26 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          16  20   30 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
Dec          1          16  20   34 212.58.231.119          0 ->  MY.NET.152.45          0 UDP
```

5. TOP TALKERS LIST

The complete summary of alerts is found in Appendix A.

Signature	Details	# Alerts	# Sources	# Destinations
MISC Large UDP Packet	Appendix B	98058	32	33
MISC source port 53 to <1024	Appendix C	59745	10694	16
CS WEBSERVER - external web traffic	Appendix D	57559	9727	1
MISC traceroute	Appendix E	48627	161	27
INFO MSN IM Chat data	Appendix F	33817	430	516
ICMP Echo Request BSDtype	Appendix G	33707	35	43
WEB-MISC prefix-get //	Appendix H	32981	1679	6
Tiny Fragments - Possible Hostile Activity	Appendix I	29009	1	1
Watchlist 000220 IL-ISDNNET-990517	Appendix J	21191	49	40
SMB Name Wildcard	Appendix K	18127	447	6399



6. EXTERNAL SOURCE ADDRESSES

SOURCE HOST	WHO IS
61.153.17.188	inetnum: 61.153.17.0 - 61.153.17.255 netname: NINGBO-ZHILAN-NET descr: NINGBO TELECOMMUNICATION CORPORATION ,ZHILAN APPLICATION SERVICE PROVIDER descr: Ningbo, Zhejiang Province country: CN admin-c: CZ61-AP tech-c: CZ61-AP mnt-by: MAINT-CHINANET-ZJ changed: master@dcb.hz.zj.cn 20010512 source: APNIC person: CHINANET ZJMASTER address: no 378,yan an road,hangzhou,zhejiang country: CN phone: +86-571-7015441 fax-no:+86-571-7027816 e-mail: master@dcb.hz.zj.cn nic-hdl: CZ61-AP mnt-by: MAINT-CHINANET-ZJ source: APNIC
209.190.237.123	Atlantech Online, Inc. (NETBLK-AOI1999B) 1010 Wayne Avenue, Suite 630 Silver Spring, MD 20910 US Netname: AOI1999B Netblock: 209.190.192.0 - 209.190.255.255 Coordinator: Center, Network Operations (EF105-ARIN) noc@atlantech.net 301-589-3060 (FAX) 301-593-9897
212.179.44.99	inetnum: 212.179.44.96 - 212.179.44.127 netname: MASHABE-SADEH descr: MASHABE-SADEH-LAN country: IL admin-c: ZV140-RIPE tech-c: ZV140-RIPE status: ASSIGNED PA notify: hostmaster@isdn.net.il mnt-by: RIPE-NCC-NONE-MNT source: RIPE route: 212.179.0.0/17 descr: ISDN Net Ltd. origin: AS8551 notify: hostmaster@isdn.net.il mnt-by: AS8551-MNT 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
61.150.5.19	inetnum: 61.150.0.0 - 61.150.31.255 netname: SNXIAN descr: xi'an data branch,XIAN CITY SHAANXI PROVINCE country: CN admin-c: WWN1-AP tech-c: WWN1-AP mnt-by: MAINT-CHINANET-SHAANXI source: APNIC person: WANG WEI NA address: Xi Xin street 90# XIAN country: CN phone: +8629-724-1554 fax-no: +8629-324-4305 e-mail: xaipadm@public.xa.sn.cn nic-hdl: WWN1-AP MAINT-CN-SNXIAN source: APNIC
141.213.11.120	University of Michigan (NET-UMNET3) Computer Aided Engineering Network (CAEN) 229 Chrysler Center Ann Arbor, MI 48109-2092 US Netname: UMNET3 Netblock: 141.213.0.0 - 141.213.255.255 Coordinator: Killey, Paul M. (PMK5-ARIN) paul@ENGIN.UMICH.EDU (734) 763-4910 (FAX) (734) 936-3107 Domain System inverse mapping provided by: SRVR8.ENGIN.UMICH.EDU 141.212.2.81/69 DNS2.ITD.UMICH.EDU 141.211.125.15
129.132.66.28	Swiss Federal Institute of Technology (NET-ETH-ETHER) Clausiusstr. 55 Zurich, 8092 CH Netname: ETH-ETHER Netblock: 129.132.0.0 - 129.132.255.255 Coordinator: Brunner, Armin (AB99-ARIN) brunner@KOM.ID.ETHZ.CH +41 1 632 3538 (FAX) +41 1 632 1225 Domain System inverse mapping provided by: DNS1.ETHZ.CH 129.132.98.12 DNS2.ETHZ.CH 129.132.250.220 SCSNMS.SWITCH.CH 130.59.1.30 130.59.10.30
MY.NET.60.8	INTERNAL IP - ICMP Echo Request BSDtype
129.79.245.106	Indiana University (NET-INDIANA-NET) 2711 E 10th St Bloomington, IN 47408 US Netname: INDIANA-NET Netblock: 129.79.0.0 - 129.79.255.255 Coordinator: Indiana University Computing Services (IUD-ORG-ARIN) dns-admin@indiana.edu 812 855-9255 Domain System inverse mapping provided by: NS.INDIANA.EDU 129.79.1.1 NS2.INDIANA.EDU 129.79.5.100 DNS1.CSO.UIUC.EDU 128.174.5.103
132.246.128.200	National Research Council of Canada (NET-NRC) 1200 Montreal Road, Bldg M60, Rm B21A Ottawa ON, 0R6 CA Netname: NRC Netblock: 132.246.0.0 - 132.246.255.255 Coordinator: Haria, Ratilal (RH3120-ARIN) Ratilal.Haria@NRC.CA (613) 993-1153 (FAX) (613) 993-1089

7. CORRELATION FROM STUDENT PRACICALS

I reviewed many other student's practicals. This was a tremendous tool to build on their research and learn from their analysis process. I learned that many students found duplicates within the log files and that MY NET should be replaced. I read through many different approaches before tackling this paper. In a way it was comforting to see others had experienced failed attempts at log crunching and some difficulty with finding the right tools for an NT environment. One specific correlation in Wade Dauphine's paper where he had also identified traffic from Israel as possible Gnutella traffic. Anther student, Tom Jones also found indications of compromised internal machines. Richard Hayler analysed traffic by hour of the day as well. He showed similar patterns where the scan log peaked in the afternoon between 15:00 and 17:00 hours and the alerts peaked later in the day between 19:00 - 21:00 hours. I was directed to an excellent article on egress filtering by Jeff Holland.

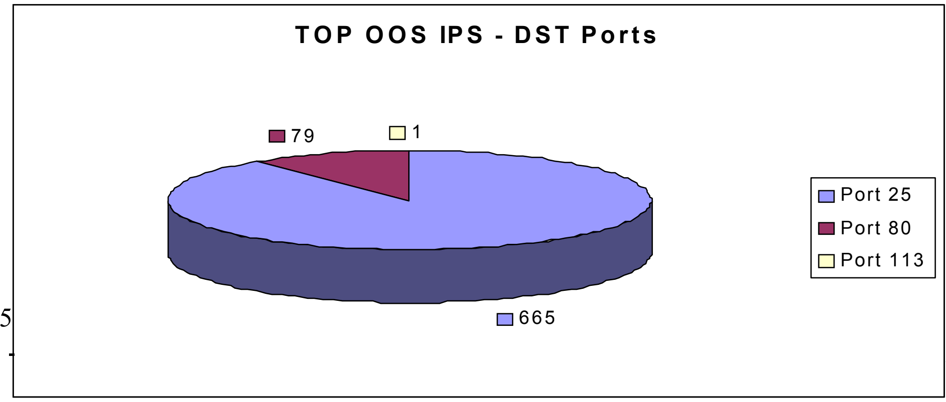
8. DATA ANALYSIS - OOS FILES AND LINK GRAPHS

Top Sources of OUT OF SPEC packets	# Entries
66.187.233.194	372
199.183.24.194	263
202.95.38.3	55
66.114.106.22	32
193.231.20.21	24

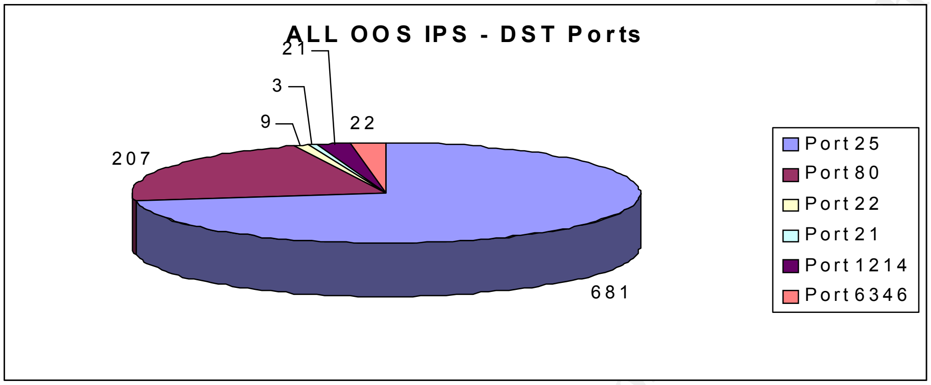
Top Destinations of OUT OF SPEC packets	# Entries
MY.NET.100.217	408
MY.NET. 253.43	139
MY.NET.253.42	60
MY.NET.253.41	48
MY.NET.253.125	40

The top Out of Spec Dst IPs showed almost all port 25 (SMTP) and port 80 (HTTP) traffic. There was only one entry destination to port 113 (Identd/auth**).** Traffic on this port can be used to identify the owner of a connection. This can reveal information to hackers. More information on this vulnerability can be found at www.cis.ohio-state.edu/cgi-bin/rfc/rfc1413.html. This traffic originated from 66.187.233.194 on src port 55231 (ephemeral) to MY.NET.253.53 on DST port 113 (Identd/auth**).**

Nslookup on 66.187.233.194 = vger.kernel.org
GeekTools says this block of IP's belongs to Red Hat Inc.



When ALL IP's in the OOS logs are sorted by dst port the results are similar with proportionate traffic to port 25 and port 80. Other traffic is noted to dst port 1214 (KaZaA), dst port 6346 (Gnutella), dst port 20/21 (FTP) and dst port 22 (SSH).



Gnutella is a peer to peer file-sharing tool using port 6346. Files generally include JPG, MP3, QuickTime and other files. Google returns references to Gnutella as a peer to peer model and software that acts both as client and server. Gnutella software is installed on some of the internal machines. According to www.dsheild.org this is one of the top 10 target ports. As a general rule the more ports that are shut down the more secure the infrastructure. Use of Gnutella allows opportunity for malicious hackers to exploit unsuspecting users. I would check hosts MY.NET.182.91, MY.NET.115.178, MY.NET.181.180, MY. NET.179.186, MY.NET.99.39, MY.NET. 70.174 and MY.NET.70.42 for possible Gnutella activity.

Date	Time	Src IP	Src Port	Dst IP	Dst Port
30-Nov-01	10:51:46	217.82.121.163	1963	MY.NET.163.107	6348
30-Nov-01	11:50:41	212.204.149.106	187	MY.NET.105.247	6346
01-Dec-01	6:35:57	194.112.10.56	4424	MY.NET.182.91	6346
01-Dec-01	10:39:53	24.150.228.250	53722	MY.NET.115.178	6346
01-Dec-01	10:44:30	217.227.54.192	34993	MY.NET.182.91	6346
01-Dec-01	11:31:14	64.41.43.39	61804	MY.NET.182.91	6346
01-Dec-01	12:49:21	134.58.253.225	40411	MY.NET.163.107	6348
01-Dec-01	12:52:01	134.58.253.225	40462	MY.NET.163.107	6348
01-Dec-01	19:53:06	24.158.32.82	33044	MY.NET.181.180	6346
01-Dec-01	21:32:23	24.21.233.246	0	MY.NET.179.86	6346
02-Dec-01	1:52:06	195.132.27.12	4854	MY.NET.99.39	6346

02-Dec-01	1:52:52	195.132.27.12	4854	MY.NET.99.39	6346
02-Dec-01	4:50:09	24.24.57.3	46812	MY.NET.182.91	6346
02-Dec-01	5:22:39	130.83.177.189	32848	MY.NET.182.91	6346
03-Dec-01	8:37:52	24.17.8.210	54387	MY.NET.70.174	6346
03-Dec-01	10:55:04	62.153.37.152	61062	MY.NET.163.107	6348
03-Dec-01	17:11:39	62.153.37.152	64938	MY.NET.182.91	6346
03-Dec-01	23:49:12	195.71.130.200	60079	MY.NET.70.174	6346
04-Dec-01	4:17:01	163.162.136.73	33231	MY.NET.162.198	6348
04-Dec-01	9:30:05	202.229.61.141	50486	MY.NET.70.42	6346
04-Dec-01	19:40:29	80.105.35.98	14484	MY.NET.111.157	6346
04-Dec-01	19:41:36	213.123.162.217	2960	MY.NET.111.157	6346
04-Dec-01	21:43:16	24.169.80.72	2108	MY.NET.111.157	6346
04-Dec-01	21:53:37	24.169.80.72	2108	MY.NET.111.157	6346
04-Dec-01	21:59:05	24.169.80.72	2108	MY.NET.111.157	6346
04-Dec-01	22:03:46	24.169.80.72	2108	MY.NET.111.157	6346
04-Dec-01	22:38:22	213.67.148.103	0	MY.NET.111.157	6346

SRC IP	**Who is originating Gnutella Traffic**
130.83.177.189	Technical University Darmstadt (NET-THD-NET) Petersenstrasse 30 D-6100 Darmstadt DE
134.58.253.225	Katholieke Universiteit Leuven (NET-KULNET) KULNET - de Croylaan 52A Leuven, B-3001 BE
163.162.136.73	netname: TILAB-NET descr: Telecom Italia Lab country: IT
194.112.10.56	inetnum: 194.112.10.0 - 194.112.10.255 netname: ALCOM-11 descr: ALCOM dynamic DHCP adresses for ADSL country: FI
195.132.27.12	netname: FR-CYBERCABLE-960620 descr: LYONNAISE COMMUNICATIONS PROVIDER Local Registry country: FR
195.71.130.200	netname: CONRAD-ELEKTRONIK-GMBH descr: Conrad_Elektronik_GmbH descr: Klaus-Conrad-Str. 1 descr: 92240 Hirschau country: DE
202.229.61.141	SUBA-029-173 g. [Organization] InfoSphere (NTT PC Communications, Inc.)
212.204.149.106	BENELUX-1 descr: @Home Benelux Deventer Headend block descr: BENELUX-CASTEL-DEVENTER-2 country: NL
213.123.162.217	netname: BT-ADSL descr: IP Pools country: GB
213.67.148.103	netname: TELIANET descr: Telia Network services descr: ISP country: SE Sweden
217.227.54.192	netname: DTAG-DIAL15 descr: Deutsche Telekom AG country: DE
217.82.121.163	netname: DTAG-DIAL14 descr: Deutsche Telekom AG country: DE

24.150.228.250	Cogeco Cable Systems (NETBLK-CGOC-2BLK) 950 Syscon Road Burlington, ON CA
24.158.32.82	Charter Communications, Inc. (NETBLK-CHARTER-NET-2BLK) 12405 Powerscourt St. Louis, MO 63131 US
24.169.80.72	ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-5) 13241 Woodland Park Road Herndon, VA 20171 US
24.17.8.210	Home Network (NETBLK-ATHOME) 450 Broadway Street Redwood City, CA 94063 US
24.21.233.246	Home Network (NETBLK-ATHOME) 450 Broadway Street Redwood City, CA 94063 US
24.24.57.3	ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-1) 13241 Woodland Park Road Herndon, VA 20171 US
62.153.37.152	netname: DTAG-DIAL11 descr: Deutsche Telekom AG country: DE
64.41.43.39	netname: IANA-BLK descr: The whole IPv4 address space country: NL
80.105.35.98	netname: TIWS-NETECONOMY-BOLOGNA descr: Telecom Italia country: IT Italy

In particular, check MY.NET.111.157, which received incoming traffic on port 6346 (gnutella) with an unusual TCP Flag combination. Additionally, 2 external host sent traffic on source port 0 (reserved) to this same machine. Technically, port 0 is illegal but is sometimes used to fingerprint a machine.

9 different signatures are present for *MY.NET.111.157* as a destination

- 1 instances of *SCAN Synscan Portscan ID 19104*
- 1 instances of *EXPLOIT x86 setgid 0*
- 1 instances of *Queso fingerprint*
- 1 instances of *NMAP TCP ping!*
- 2 instances of *X11 outgoing*
- 4 instances of *High port 65535 tcp - possible Red Worm - traffic*
- 8 instances of *Null scan!*
- 22 instances of *INFO MSN IM Chat data*
- 322 instances of *INFO Outbound GNUTella Connect accept*

KaZaA: KaZaA is another file sharing protocol that uses HTTP over port 1214 by default. This accounted for almost as much traffic as Gnutella in the Out of Spec logs. The next OOS log extract, shows 14 internal IP's received port 1214 (KaZaA) traffic form a variety of sources.

Date	Time	Src IP	Src Port	Dst IP	Dst Port
30-11-01	6:00:41	131.215.19.205	1	MY.NET.53.67	1214
30-11-01	6:01:13	131.215.19.205	31	MY.NET.53.67	1214
30-11-01	10:56:53	217.225.225.236	3023	MY.NET.130.69	1214
01-Dec-01	17:39:20	217.80.10.56	4959	MY.NET.98.173	1214
01-Dec-01	17:39:22	217.80.10.56	4959	MY.NET.98.173	1214
01-Dec-01	17:50:30	217.80.10.56	1101	MY.NET.98.173	1214
01-Dec-01	21:13:48	131.211.121.26	63686	MY.NET.70.70	1214
02-Dec-01	0:39:22	24.169.185.42	21	MY.NET.98.177	1214
02-Dec-01	6:18:29	66.8.217.130	1	MY.NET.88.162	1214
03-Dec-01	5:55:10	200.67.133.18	33584	MY.NET.82.131	1214
03-Dec-01	5:55:12	200.67.133.18	33584	MY.NET.82.131	1214
03-Dec-01	11:56:43	62.163.0.120	1086	MY.NET.88.162	1214
04-Dec-01	2:04:36	216.132.186.66	1591	MY.NET.53.164	1214

04-Dec-01	2:16:24	216.132.186.66	1731	MY.NET.53.164	1214
04-Dec-01	7:35:56	134.130.48.60	1826	MY.NET.150.133	1214
04-Dec-01	12:33:23	158.75.57.4	55268	MY.NET.88.162	1214
04-Dec-01	13:14:26	217.3.21.93	1476	MY.NET.150.133	1214
04-Dec-01	16:08:46	148.4.54.139	1343	MY.NET.150.133	1214
04-Dec-01	18:14:51	24.65.3.129	1439	MY.NET.70.70	1214
04-Dec-01	21:56:52	24.156.172.100	39445	MY.NET.83.53	1214
04-Dec-01	22:05:29	24.156.172.100	40033	MY.NET.83.53	1214

SOURCE HOST	WHO originated KaZaA traffic.
131.215.19.205	Name: DHCP-19-205.caltech.edu California Institute of Technology (NET-CALTECH-NET) 1200 East California Pasadena, CA 91125 US
217.225.225.236	netname: DTAG-DIAL15 descr: Deutsche Telekom AG country: DE
217.80.10.56	Name: pD9500A38.dip.t-dialin.net netname: DTAG-DIAL14 descr: Deutsche Telekom AG country: DE
131.211.121.26	Universiteit Utrecht (NET-RUUNET) Budapestlaan 8, NL- 3584 CD Utrecht NL
24.169.185.42	Name: syr-24-169-185-42.twcny.rr.com ServiceCo LLC - Road Runner (NET-ROAD-RUNNER-5) 13241 Woodland Park Road Herndon, VA 20171 US
66.8.217.130	Name: a66b8n217client130.hawaii.rr.com ROADRUNNER-HAWAII (NETBLK-ROADRUNNER-HAWAII) 13241 Woodland Park Road Herndon, VA 20171 US
200.67.133.18	Nslookup - DNS request timed out. Network Information Center Mexico (NETBLK-NIC-MEXICO-6) NIC-MEXICO-6
62.163.0.120	Name: a0120.upc-a.chello.nl netname: UPC-BRT-HM5 descr: Brabant country: NL The Netherlands
216.132.186.66	DNS request timed out Epoch Networks (NETBLK-ENI-BLK5)ENI-BLK5
134.130.48.60	Name: ip1-60.halifax.RWTH-Aachen.DE Rechenzentrum der RWTH Aachen (NET-ACHSE) Seffenter Weg 2352072 DE
158.75.57.4	Name: hetman.loiv.torun.pl POLIP (NET-TORUNPOLIP2) Computer Centre, Nicolaus Copernicus University ul. Chopina 12/18, 87-100 Torun, Poland
217.3.21.93	Name: hetman.loiv.torun.pl netname: DTAG-DIAL13 descr: Deutsche Telekom AG country: DE
148.4.54.139	Long Island University/C.W. Post Campus (NET-LIUNET1) 700 Northern Boulevard Brookville, NY 11548 US
24.65.3.129	Name: h24-65-3-129.gv.shawcable.net Shaw Fiberlink ltd. (NETBLK-FIBERLINK-CABLE) Suite 800, 630 3rd Avenue SW Calgary, Alberta T2P 4L4 CA
24.156.172.100	Rogers@Home (NETBLK-ROGERS-6-BLOCK

FTP: Some internal hosts are seen using File Transfer Protocol (FTP) on port 21 to pass data between the client and the server. Some companies restrict FTP traffic to specific hosts to reduce risks of downloading malicious code. Block port 21 (FTP - control) and port 20 (FTP - data) on the Firewall and only allow to boxes designated for ftp. Approved boxes can then be specifically monitored for vulnerabilities when using this service.

Date	Time	Src IP	Src Port	Dst IP	Dst Port
02-Dec-01	11:46:22	80.11.36.130	32774	MY.NET.100.165	21
02-Dec-01	11:46:31	80.11.36.130	32774	MY.NET.100.165	21
04-Dec-01	20:58:38	141.157.91.196	64101	MY.NET.60.8	21

SOURCE HOST	WHO originated FTP traffic.
80.11.36.130	IP2000-ADSL-BAS BSPoI102 Poitiers Blocl Country: Fr France Telecom Wanadoo interactive
204.152.189.120	Bell Altanitc 1880 Campus Commons Drive Reston, VA US

SSH and TelNet: Some SSH Remote Login Protocol traffic (port 22) was identified to MY.NET.60.38/39and MY.NET.1.3/4/5. Use of port 22 potentially allows hackers access to well-know holes. Upon reviewing the University site I noted they were using Kerberos tickets and AFS tokens with expiring logon times to secure connections.

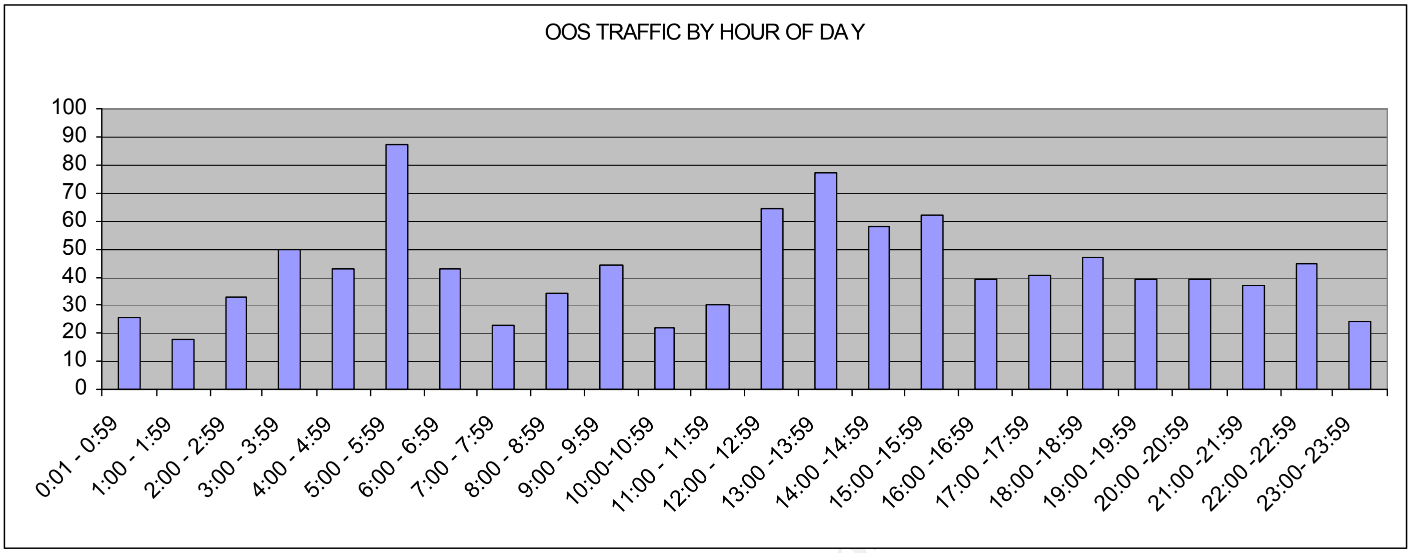
Both Kerberos (an authentication system allowing confidentially over the Internet) and the Andrew File System (file sharing using tokens which grants permissions for a period of time) decrease the risk of hackers activity.

There was only one instance of TelNet in the OOS logs. SSH is better than Telnet in that the session is encrypted. TelNet should not be used as the password is passed in clear text.

Date	Time	Src IP	Src Port	Dst IP	Dst Port
02-Dec-01	6:28:10	203.147.61.20	34715	MY.NET.1.3	22
02-Dec-01	6:28:28	203.147.61.20	34715	MY.NET.1.3	22
02-Dec-01	6:28:07	203.147.61.20	34716	MY.NET.1.4	22
02-Dec-01	6:28:10	203.147.61.20	34716	MY.NET.1.4	22
02-Dec-01	6:28:21	203.147.61.20	34716	MY.NET.1.4	22
02-Dec-01	6:28:07	203.147.61.20	34717	MY.NET.1.5	22
02-Dec-01	6:28:10	203.147.61.20	34717	MY.NET.1.5	22
04-Dec-01	17:28:05	24.6.147.104	863	MY.NET.60.38	22
03-Dec-01	16:45:02	208.232.200.59	40510	MY.NET.60.39	22
04-Dec-01	10:20:29	MY.NET.70.38	34304	207.136.8.17	23

SOURCE HOST	WHO originated SSH traffic.
203.147.61.20	Name: mail.geccorp.com netname: JI-NET descr: Jasmine Internet Co, Ltd.Subsidiary Company of Jasmine International PLC country: TH
24.6.147.104	Name: cx722605-a.msnv1.occa.home.com @Home Network (NETBLK-ATHOME) ATHOME
208.232.200.59	UUNET Technologies, Inc. (NETBLK-UUNET1996B) UUNET1996B 208.192.0.0 - 208.255.255.255 Fedworld/NTIS/Deptment of Commerce

The University offers many WEB-enable services and dial up access which require services of FTP (20/21) and SSH (22), unfortunately this exposes them to many well know vulnerabilities on those ports. Mitigation of these vulnerabilities includes hardening of boxes, application of patches, proper authentication and appropriate computer usage policies.



TRAFFIC BY HOUR

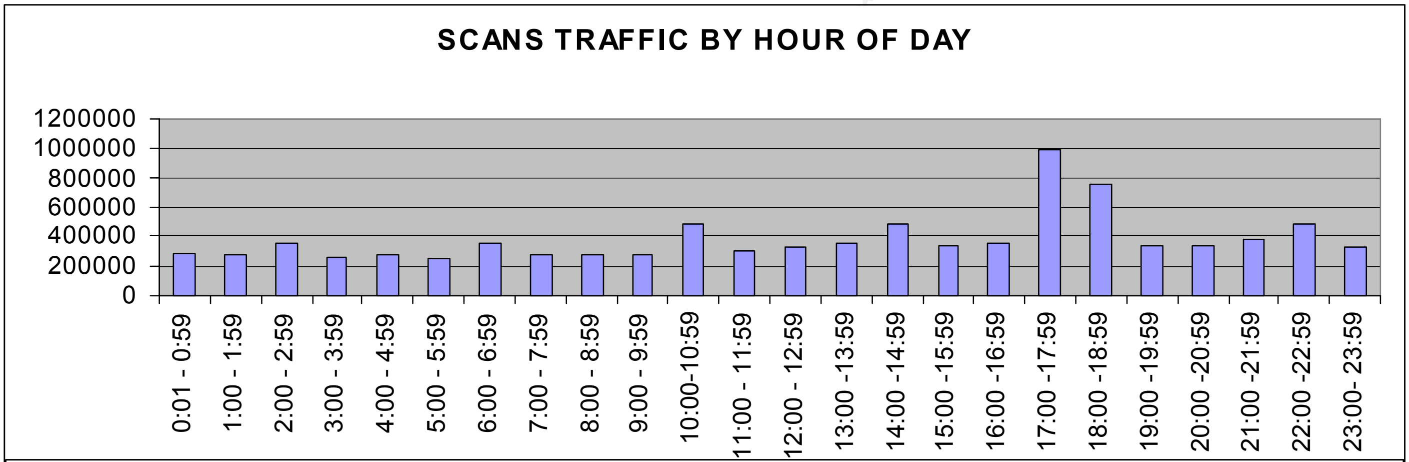
A three link graphs above display OOS, Scans and Alert traffic by hour of the day. The OOS events show an increase just before 6:00 am and increases again during a staggered lunch hour. The majority if this traffic is SMTP and HTTP and reflects student or staff usage. The first spike seems a bit early for normal activity. This activity was generated mostly between 5:45 - 5:59 during the 5-day period.

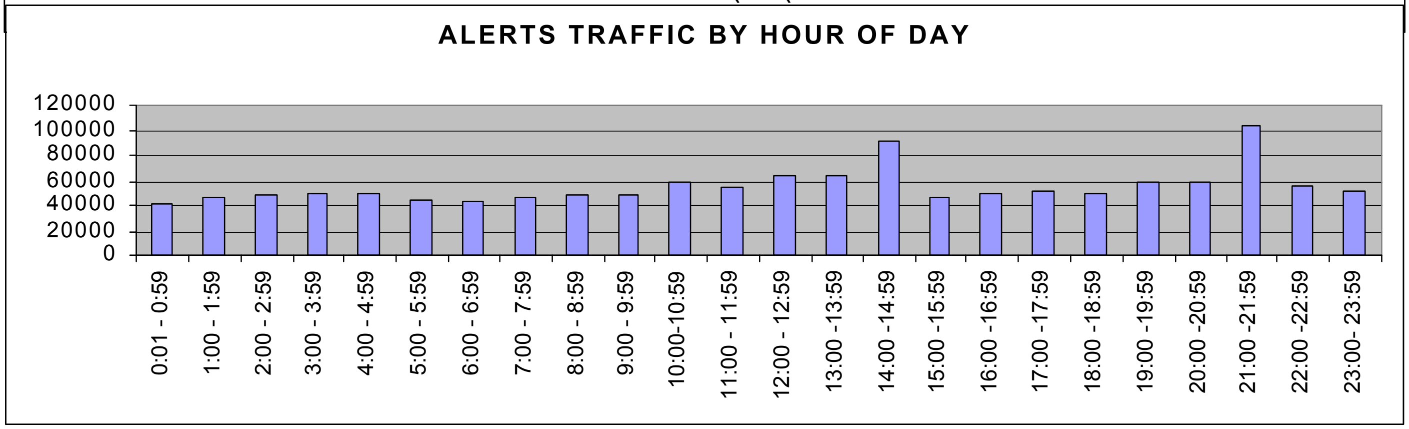
A similar graph on scans shows the peak in traffic between 17:00 and 19:00 hours.

The same representation of alerts by hour of the day shows the peaks of suspicious activity between 14:00 - 15:00 and 21:00 - 22:00.

9. INTERNAL MACHINE ANALYSIS

Here are a couple of internal machines that warrant further investigation. There is a clear indication that several internal machines are most likely compromised.





MY.NET.70.148	15 different signatures are present for MY.NET.70.148 as a destination. Possible compromised machine. Indicators of possible reconnaissance and then compromise as shown in Appendix E.
MY.NET.140.9	Possible hardware issue see Appendix E
MY.NET.98.149	Possible use of MSN which may not be acceptable use. See Appendix F

MY.NET.16.42	Tiny Fragments, possible hostile activity. There are 8 different signatures present for *MY.NET.16.42* as a destination. There are sufficient alerts on both of these machines (MY.NET.8.1 and MY.NET.16.42) to investigate a compromised machine. See Appendix I.
MY.NET.111.157	Possible gnutella activity as discussed in #8.
MY.NET.70.42	Possible gnutella traffic from Israel as described in Appendix J.
MY.NET.100.165	This is your busiest web server, which qualified as the TOP DST host for alerts. There were 57559 alerts in 5 days. There were 33 different types of alerts. There is substantial cleanup required, as it is impossible to follow-up on this many alerts. Start by following up on each of the 33 different types. Determine if this web server is vulnerable to that particular alert or if it could be a false positive. Stop non-applicable alerts. Investigate other alerts by looking at correlating logs. Follow-up on other types of alerts to see if damage has been done. Remove vulnerabilities where possible and clean the machine if compromised. Appendix D
MY.NET.253.114	This web sever was not hit as hard as MY.NET.100.165. There were a total of 32487 alerts in 5 days with 23 different signatures. Both are critical and should be reviewed and hardened to mitigate potential defacement, denial of service or compromise. Appendix H
MY.NET.1.3/4/5	DNS servers are critical as well. Ensure zone transfers are only from trusted servers and restrict traffic by firewall rules. Appendix C
MY.NET.111.221	The TOP Src Host generating Misc Large UDP Packets sent 40217 packets within 5 days. The majority of this traffic from port 1073 (bridgecontrol) to port 2646 (AND License Manager) was targeted to MY.NET.111.221. This volume of traffic should be justified. Also this particular internal machine was constantly scanned from 61.150.5.19 (another IP from Asia) and potentially fingerprinted through use of port 0 (reserved). See Appendix B

10. DEFENCE RECOMMENDATION

- All well secured Infrastructures are based on an IT Security Policy and defense in depth. Use of a firewall, hardening of boxes and configuration of your infrastructure can enforce most of the policies. Additionally important are computer usage policies and awareness campaigns.
- I did not have the benefit of any network diagrams. Ideally traffic to the network is controlled through a 'single point of entry'. If there are other points of entry they should be documented. Firewall or ACL on routers should secure all points of entry.
- Firewalls should only allow required traffic like HTTP (port 80), HTTPS (port 443), SMTP (port 25), etc. The Firewall policy would be enforcing the IT Security Policy which states which inbound and outbound services are allowed. Outbound (or egress) filtering is nicely described in this article. http://www.sans.org/infosecFAQ/firewall/egress.htm.
- Determine a policy about dial up Internet access. If this is allowed on University equipment ensure the user understands the risks. A desktop firewall product should be installed and anti virus must be kept current. The user must understand the risks of using dial up and ensure they aren't dialing up while on the network.
- Follow-up on those machines that may be compromised.

- Several internal machines have downloaded and installed copies of KaZaA, Napster and Gnutella. These are peer-to-peer file sharing software. The users are probably not aware of the potential risks of lost data, lost bandwidth, lost productivity and potential for compromised machine. Vulnerabilities are continually being discovered with these file sharing software products. KaZaA among others programs, has just been found to contain a new Trojan horse that tracks users' web surfing habits without their permission. The Trojan was bundled with advertising within the open-source product.
- A packet logger like Windump can be used to follow up on an alert and provide more conclusive information.
- Consider placing an application firewall on your webserver. This will filter out some of the port 80 (HTTP) traffic that passes any perimeter filters but could be stopped before the application layer. Products like Microsoft's URLScan can allow GET, HEAD and POST for example. All other verbs would be denied and logged outside the IIS log. This would effectively block "All other post methods than GET and POST" as indicated in your web statistics.
- Penetration tests can be costly but provide management with a comfort of knowing how secure you are. The other alternative is to facilitate regular vulnerability scans. There are many open source products which allow analysis and are more likely to detect malicious activity if used regularly.
- Consideration can be given to running your own scanning tools on the network. There are many scans each day searching for vulnerabilities. Knowledge of the existing vulnerabilities would allow the University to patch the holes before they are exploited.
- There was some information on the University website about current viruses and desktop virus applications. Continued security awareness and improved anti virus protection will reduce the exposure. Protect is most effective when applied in layers. Based on your network configuration, there should be anti virus on every server that emails and files reside. This could include an anti virus gateway server, mail server and desktop server antivirus solutions. There are different products that verify that updates are done regularly. Alternatively, a simple logon script can report if dat version, engine version and product version are not current. Have a virus eradication procedure in place.
- All boxes should be hardened before moving into Production. This includes a build with the latest fixes and service packs, limited services to only those required. Follow-up by regularly applying appropriate patches and service packs after testing. All boxes should be hardened but boxes directly connected to the Internet are of the greatest risk. Review and ensure that the web servers, the firewalls, the DNS servers are hardened.
- Review firewall, intrusion detection and other network monitoring logs regularly. Regular review enables the administrator to know 'normal traffic' and therefore more like to be alerted to undesirable issues.

11. ANALYSIS PROCESS STEPS

- Researching: Other students solutions, tools which may work on NT, tools which wouldn't require too long a learning curve, solutions which would run on my laptop. Looked at Logger, Spade, Spice, Snortsnarf, Perl, Axman split file, filecomb

- Downloading: Impossible on a dial-up connection. Difficult on restricted network at work. Ended up connecting my laptop to an ADSL home connection.
- Determining Content: I discovered notepad and word were not the tools to handle files this size. I was glad to find a text editor, ConText, that could handle the job.
- Sorting Data: An export of even one file to excel resulted in an incomplete file due to the file restriction. I knew I needed to 'parse data'. Many students provided scripts for Perl or batch files but I wasn't sure I'd have the time to learn these tools as I'd had no experience in either. Several times I considered splitting the files into manageable sizes then manually extracting the data.
- Manipulating Files: I used the Find and Copy commands to merge the files into one. Find *.txt > alertall.txt copy 1.txt 2.txt 3.txt all.txt I used Find and Sed to replace MY.NET with MY.NET and to extract the portscans from the alert file.
- Splitting Files: I used hjsplit to split the files into manageable sizes.
- Analyzed Data: Used Snortsnarf to analyze the data in the alert files, OSS and scan file separately.
- Running Snortsnarf: I was again challenged by "out of memory" errors. I was able to use a server at work for the extra horsepower. When it finally did complete after the 4 try and after 8 hours I was dismayed to find that the alerts displayed as time stamps. Long story short, I started all over again with new downloaded files saved as .txt, combined with copy, extracted portscans with find, replace MY.NET with Context and ran snortsnarf. The portscan files were split and totaled in Excel using Data/Subtotal options.
- Summary: I'm glad to have had the opportunity to take the course and write the practical. It was an excellent method to learn.

Support Sites

www.sans.org	www.arin.net	http://www.fixedsys.com/context
http://www.ripe.net	http://www.google.com	http://www.securityfocus.com
http://cve.mitre.org	www.silicondefense.com	http://networkice.com
www.incidents.org	http://bugtraq.com	http://www.freebyte.com/hjsplit
		http://www.simovits.com/nyheter9902.html

APPENDIX A: All Snortsnarf Alerts

Signature	# Alerts	# Sources	# Destinations
MISC Large UDP Packet	98058	32	33
MISC source port 53 to <1024	59745	10694	16
CS WEBSERVER - external web traffic	57559	9727	1
MISC traceroute	48627	161	27
INFO MSN IM Chat data	33817	430	516
ICMP Echo Request BSDtype	33707	35	43
WEB-MISC prefix-get //	32981	1679	6
Tiny Fragments - Possible Hostile Activity	29009	1	1
Watchlist 000220 IL-ISDNNET-990517	21191	49	40
SMB Name Wildcard	18127	447	6399
ICMP Destination Unreachable (Host Unreachable)	7506	734	70
ICMP Echo Request Nmap or HPING2	5955	65	505
ICMP Echo Request CyberKit 2.2 Windows	3772	80	10
ICMP Destination Unreachable (Communication Administratively Prohibited)	3002	201	113
INFO Napster Client Data	2974	41	84
NMAP TCP ping!	2788	42	966
ICMP Echo Request L3retriever Ping	2233	15	17
SCAN Proxy attempt	1937	117	193
Watchlist 000222 NET-NCFC	1887	27	19
SUNRPC highport access!	1722	13	12
Incomplete Packet Fragments Discarded	1520	8	8
ICMP Fragment Reassembly Time Exceeded	1437	47	59
External RPC call	1379	8	949
ICMP Destination Unreachable (Network Unreachable)	1348	16	22
ICMP Echo Request Sun Solaris	1315	12	1033
INFO FTP anonymous FTP	1271	296	211
WEB-MISC 403 Forbidden	1244	11	682
Queso fingerprint	933	74	43
ICMP traceroute	919	256	534
INFO Inbound GNUTella Connect accept	803	31	710
Null scan!	774	165	40
ICMP Echo Request Windows	769	197	102
ICMP Destination Unreachable (Protocol Unreachable)	754	26	27
INFO Outbound GNUTella Connect accept	527	464	33
WEB-MISC Attempt to execute cmd	452	60	33
spp_http_decode: CGI Null Byte attack detected	409	11	7
WEB-MISC http directory traversal	381	123	6
TELNET login incorrect	370	8	272
INFO Possible IRC Access	342	89	72
TCP SRC and DST outside network	342	43	150
spp_http_decode: IIS Unicode attack detected	340	91	45
High port 65535 tcp - possible Red Worm - traffic	303	34	36
RPC tcp traffic contains bin_sh	300	12	11
ICMP Source Quench	268	97	10
TFTP - Internal TCP connection to external tftp server	265	5	5
WEB-IIS view source via translate header	249	46	9
X11 outgoing	246	13	17
CS WEBSERVER - external ftp traffic	240	67	1

Possible trojan server activity	232	23	119
Port 55850 tcp - Possible myserver activity - ref. 010313-1	213	47	52
WEB-MISC count.cgi access	203	90	2
WEB-FRONTPAGE _vti_rpc access	198	114	12
WEB-IIS _vti_inf access	194	117	12
FTP DoS ftpd globbing	188	6	6
ICMP Destination Unreachable (Fragmentation Needed and DF bit was set)	166	118	9
Virus - Possible scr Worm	140	14	46
High port 65535 udp - possible Red Worm - traffic	131	39	34
INFO - Possible Squid Scan	130	10	100
FTP MKD . - possible warez site	119	2	48
connect to 515 from outside	95	2	89
WEB-MISC compaq nsight directory traversal	85	28	26
EXPLOIT x86 NOOP	84	28	31
WEB-CGI scriptalias access	83	5	5
connect to 515 from inside	83	3	3
MISC Large ICMP Packet	78	24	18
WEB-CGI redirect access	74	48	7
Port 55850 udp - Possible myserver activity - ref. 010313-1	74	6	7
beetle.ucs	73	7	10
BACKDOOR NetMetro Incoming Traffic	60	4	4
SCAN Synscan Portscan ID 19104	52	52	22
MISC Source Port 20 to <1024	45	1	45
Virus - Possible pif Worm	42	9	17
INFO - Web Cmd completed	34	1	12
ICMP Echo Request Broadscan Smurf Scanner	31	3	26
WEB-CGI formmail access	29	17	10
WEB-CGI csh access	26	20	3
TELNET access	25	1	19
SMTP relaying denied	20	8	16
EXPLOIT x86 setuid 0	19	16	16
SCAN FIN	17	7	12
WEB-IIS Unauthorized IP Access Attempt	14	2	12
RFB - Possible WinVNC - 010708-1	13	7	6
ICMP redirect (Host)	13	3	2
EXPLOIT x86 setgid 0	11	8	8
EXPLOIT x86 stealth noop	11	5	10
Virus - Possible MyRomeo Worm	11	5	9
WEB-MISC Lotus Domino directory traversal	10	9	2
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	10	6	6
WEB-IIS asp-dot attempt	9	1	1
SMTP chameleon overflow	8	8	5
MISC PCAnywhere Startup	8	5	3
INFO Inbound GNUTella Connect request	8	5	4
BACKDOOR NetMetro File List	8	2	2
X11 xopen	8	1	3
IDS50/trojan_trojan-active-subseven [arachNIDS]	7	4	4
WEB-CGI ksh access	6	4	2
Attempted Sun RPC high port access	6	4	4
INFO - Web Dir listing	6	3	5

ICMP SRC and DST outside network	5	5	5
WEB-CGI rsh access	5	4	2
ICMP Redirect (Undefined Code!)	5	3	3
DNS zone transfer	5	2	1
SYN-FIN scan!	5	1	1
TCP SMTP Source Port traffic	4	3	3
IDS475/web-iis_web-webdav-propfind [arachNIDS]	4	2	2
Virus - Possible NAIL Worm	4	2	3
WEB-MISC guestbook.cgi access	4	2	1
WEB-FRONTPAGE fpcount.exe access	3	2	2
RPC portmap request rstatd	3	2	2
FTP passwd attempt	3	2	2
SNMP public access	3	1	1
External FTP to HelpDesk MY.NET.70.49	3	1	1
WEB-CGI finger access	2	2	1
TFTP - Internal UDP connection to external tftp server	2	2	2
ICMP IPV6 Where-Are-You	2	2	2
WEB-CGI glimpse access	2	2	1
EXPLOIT NTPDX buffer overflow	2	2	2
WEB-CGI w3-msql access	2	2	1
Probable NMAP fingerprint attempt	2	1	1
External FTP to HelpDesk MY.NET.53.29	2	1	1
DDOS mstream handler to client	2	1	1
WEB-IIS File permission canonicalization	2	1	1
HelpDesk MY.NET.83.197 to External FTP	2	1	2
INFO - Web Command Error	2	1	2
WEB-CGI survey.cgi access	2	1	1
INFO Outbound GNUTella Connect request	2	1	1
Back Orifice	1	1	1
HelpDesk MY.NET.70.50 to External FTP	1	1	1
WEB-MISC L3retriever HTTP Probe	1	1	1
External FTP to HelpDesk MY.NET.83.197	1	1	1
IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	1	1	1
External FTP to HelpDesk MY.NET.70.50	1	1	1
DDOS - TFN client command LE	1	1	1
CS WEBSERVER - external cmd traffic	1	1	1
Tiny Fragments - Possible Hostile Activity [**] MY.NET.8.112/04-19:44:32.070566 [**] INFO MSN IM Chat data	1	1	1
WEB-CGI tsch access	1	1	1
EXPLOIT FTP passwd retrieval retr path	1	1	1
WEB-FRONTPAGE fourdots request	1	1	1
SCAN - wayboard request - allows reading of arbitrary files as http service	1	1	1
WEB-FRONTPAGE form_results access	1	1	1
CS WEBSERVER - external ssh traffic	1	1	1
DNS SPOOF query response with ttl	1	1	1
WEB-IIS encoding access	1	1	1
WEB-FRONTPAGE writeto.cnf access	1	1	1
ICMP Timestamp Reply (Undefined Code!)	1	1	1
WEB-MISC webdav search access	1	1	1

Virus - SnowWhite Trojan Incoming	1	1	1
WEB-MISC whisker head	1	1	1
ICMP IPV6 Where-Are-You (Undefined Code!)	1	1	1
WEB-MISC Invalid URL	1	1	1
WEB-MISC /etc/passwd	1	1	1
TFTP - External UDP connection to internal tftp server	1	1	1
MISC Cisco Catalyst Remote Access	1	1	1
HelpDesk MY.NET.70.49 to External FTP	1	1	1
Security 000516-1	1	1	1

APPENDIX B - MISC Large UDP Packet

Sources triggering this attack signature

Source		THIS Alert	Total Alerts	Alert Breakdown
61.153.17.188	Asia Pacific Network Information Center	39801	40217	• 416 instances of *Incomplete Packet Fragments Discarded* • 39801 instances of *MISC Large UDP Packet* • Lots from Port 1073 to Port 2646 • Lots from Port 3047 to Port 1066 • Lots from Port 3800 to Port 1265 • Lots from Port 2699 to Port 3497 • 1% from Port 0 to Port 0 sometimes used to fingerprint a machine.

	`SCAN LOG Extract  There were 3367 Scans from this source IP.`
	`Dec  1 11:55:19 61.153.17.188:0 -> MY.NET.111.221:0 UDP`
	`Dec  1 11:55:14 61.153.17.188:55222 -> MY.NET.111.221:23501 UDP`
	`Dec  1 11:55:16 61.153.17.188:21067 -> MY.NET.111.221:57441 UDP`
	`Dec  1 11:55:18 61.153.17.188:3800 -> MY.NET.111.221:1265 UDP`
	`Dec  1 11:55:16 61.153.17.188:3513 -> MY.NET.111.221:4116 UDP`
	`Dec  1 11:55:23 61.153.17.188:0 -> MY.NET.111.221:0 UDP  …`			

209.190.237.123	Atlantech Online, Inc 7b.edbed1.client.atlantech.net	32954	32986	• 1 instances of *TFTP - Internal UDP connection to external tftp server* • 1 instances of *Attempted Sun RPC high port access* • 4 instances of *ICMP Fragment Reassembly Time Exceeded* • 26 instances of *High port 65535 udp - possible Red Worm - traffic* • 32954 instances of *MISC Large UDP Packet* • Lots of Port 65535 to high port numbers • Lots of Port 0 to Port 0 sometimes used to fingerprint a machine. • Lots of Port 33475 to Port 39778 • Lots of Port 33296 to Port 7825 • Possible On-line Gaming or Trojan on Port 7000

	SCAN LOG EXTRACT: There was 17,550 Scans from or to this source IP. [901999]Dec 2 04:51:30 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1282517]Dec 2 16:37:51 MY.NET.60.39:7001 -> 209.190.237.123:7000 UDP [1330111]Dec 2 18:08:19 MY.NET.60.38:7001 -> 209.190.237.123:7000 UDP [1409054]Dec 2 20:48:02 MY.NET.60.39:7001 -> 209.190.237.123:7000 UDP [1415212]Dec 2 20:59:00 MY.NET.60.38:7001 -> 209.190.237.123:7000 UDP [1642118]Dec 3 04:45:14 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1647537]Dec 3 04:55:15 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1656917]Dec 3 05:15:18 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1659603]Dec 3 05:20:19 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1664252]Dec 3 05:30:21 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [1678998]Dec 3 06:06:29 MY.NET.60.43:7000 -> 209.190.237.123:7001 UDP [2378925]Dec 3 23:54:13 MY.NET.162.189:7001 -> 209.190.237.123:7000 UDP [2787544]Dec 4 11:20:47 MY.NET.60.182:7001 -> 209.190.237.123:7000 UDP [2827772]Dec 4 12:21:12 209.190.237.123:0 -> MY.NET.70.134:0 UDP [2827773]Dec 4 12:21:07 209.190.237.123:1347 -> MY.NET.70.134:3242 UDP [2827774]Dec 4 12:21:07 209.190.237.123:65535 -> MY.NET.70.134:39657 UDP [2827775]Dec 4 12:21:09 209.190.237.123:4275 -> MY.NET.70.134:1743 UDP [2827776]Dec 4 12:21:10 209.190.237.123:20601 -> MY.NET.70.134:45266 UDP [2827777]Dec 4 12:21:12 209.190.237.123:7905 -> MY.NET.70.134:51345 UDP [2827778]Dec 4 12:21:12 209.190.237.123:55847 -> MY.NET.70.134:38183 UDP [2827831]Dec 4 12:21:17 209.190.237.123:0 -> MY.NET.70.134:0 UDP [2827870]Dec 4 12:21:21 209.190.237.123:0 -> MY.NET.70.134:0 UDP [2827871]Dec 4 12:21:18 209.190.237.123:35379 -> MY.NET.70.134:62724 UDP [2827872]Dec 4 12:21:21 209.190.237.123:19429 -> MY.NET.70.134:4694 UDP			
61.150.5.19	Asia Pacific Network Information Center	14717	14717	• 14717 instances of *MISC Large UDP Packet* • Port 3322 to 1379 • Port 0 to Port 0 sometimes used to fingerprint a machine. • Port 4961 to Port 3901 • Port 3485 to Port 4907
	SCAN LOG EXTRACT: There was consistent scanning targeted at this IP over the 5-day period. [2313924]Dec 3 22:14:04 61.150.5.19:4961 -> MY.NET.111.221:3901 UDP [2313925]Dec 3 22:14:03 61.150.5.19:2699 -> MY.NET.111.221:3497 UDP [2313979]Dec 3 22:14:08 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314006]Dec 3 22:14:12 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314007]Dec 3 22:14:12 61.150.5.19:4961 -> MY.NET.111.221:3901 UDP [2314037]Dec 3 22:14:17 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314038]Dec 3 22:14:15 61.150.5.19:4961 -> MY.NET.111.221:3901 UDP [2314072]Dec 3 22:14:20 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314099]Dec 3 22:14:25 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314100]Dec 3 22:14:23 61.150.5.19:4961 -> MY.NET.111.221:3901 UDP [2314135]Dec 3 22:14:28 61.150.5.19:0 -> MY.NET.111.221:0 UDP [2314136]Dec 3 22:14:28 61.150.5.19:4961 -> MY.NET.111.221:3901 UDP			

216.231.14.226	Cox Communications, Inc.	2533	2534	• 1 instances of *High port 65535 udp - possible Red Worm - traffic* • 2533 instances of *MISC Large UDP Packet* • Port 31704 to Port 4011 • Port 31716 to Port 4014 • Port 0 to Port 0 sometimes used to fingerprint a machine. • Lots ICMP Fragment Reassembly Time Exceeded [**] MY.NET.10.62 -> 216.231.14.226
	SCAN LOG EXTRACT: There were 972 scans from this source IP to Internal destination MY NET.10.62 (MY.NET.10.62). The scan log corroborates the alert log. [1301630]Dec 2 17:13:08 216.231.14.226:0 -> MY.NET.10.62:0 UDP [1301631]Dec 2 17:13:09 216.231.14.226:31704 -> MY.NET.10.62:4011 UDP [1301632]Dec 2 17:13:06 216.231.14.226:8448 -> MY.NET.10.62:37994 UDP [1301633]Dec 2 17:13:07 216.231.14.226:60914 -> MY.NET.10.62:30616 UDP [1301634]Dec 2 17:13:08 216.231.14.226:24298 -> MY.NET.10.62:60668 UDP [1301819]Dec 2 17:13:31 216.231.14.226:31716 -> MY.NET.10.62:4014 UDP ….. [1311162]Dec 2 17:30:38 216.231.14.226:0 -> MY.NET.10.62:0 UDP [1311163]Dec 2 17:30:37 216.231.14.226:31716 -> MY.NET.10.62:4014 UDP [1311200]Dec 2 17:30:39 216.231.14.226:48292 -> MY.NET.10.62:25771 UDP [1311201]Dec 2 17:30:42 216.231.14.226:0 -> MY.NET.10.62:0 UDP [1311202]Dec 2 17:30:41 216.231.14.226:31716 -> MY.NET.10.62:4014 UDP [1311203]Dec 2 17:30:40 216.231.14.226:5001 -> MY.NET.10.62:16728 UDP [1311204]Dec 2 17:30:41 216.231.14.226:51346 -> MY.NET.10.62:42358 UDP [1311242]Dec 2 17:30:44 216.231.14.226:0 -> MY.NET.10.62:0 UDP [1311243]Dec 2 17:30:44 216.231.14.226:32059 -> MY.NET.10.62:4043 UDP			
210.76.63.49	Asia Pacific Network Information Center	2273	2273	• 2273 instances of *MISC Large UDP Packet* • 4609 -> MY.NET.163.135:4087 • 1123 -> MY.NET.163.135:4264

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.111.221	48427	48871	2	10
MY.NET.70.134	32954	32985	1	4
MY.NET.84.218	6004	6004	1	1
MY.NET.10.62	2533	2534	1	1
MY.NET.163.135	2387	3064	2	3

APPENDIX C – MISC source port 53 to <1024

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.66.147.34	839	839	1	1
134.93.19.12	565	565	1	1
192.88.193.144	294	294	4	4
207.69.200.240	252	252	4	4
63.118.174.239	251	251	3	3

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.1.3	20694	20750	6548	6580
MY.NET.1.5	17634	17655	4967	4972
MY.NET.1.4	17282	17343	4945	4954
MY.NET.130.122	1600	1601	8	9
MY.NET.1.2	1330	1331	276	277

Port 53 (Domain Name server) can be vulnerable to the ADM worm and Lion, which can affect Unix machines. There is significant DNS traffic, which could be Zone Transfers. Controls should be in place to only accept zone transfers from trusted servers. There is always potential for corruption of DNS table by a malicious zone transfer.

Name:	**ADM worm**
Ports:	23, 53, 31337
Files:	Admw0rm-v1.tar.gz - 7,427 bytes ADMw0rm - 1,725 bytes GimmeIP - 545 bytes GimmeRAND.c - 314 bytes Incremental - 765 bytes Named_ADMv2.c - 5,892 bytes Remotecmd.c - 4,098 bytes Scanconnect.c - 1,483 bytes Startup - 670 bytes Testvuln.c - 4,299 bytes
Created:	May 1998
Actions:	Worm / Rootkit / Backdoor The worm is a collection of scripts and hacks aimed toautomatically exploit BIND systems on Linux servers.
Notes:	Works on Unix (Linux). Affects Linux RedHat 4.0 to 5.2

APPENDIX D - CS WEBSERVER - external web traffic

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
132.246.128.200	3739	3743	1	1
140.239.126.13	2657	2673	1	2
210.142.50.148	1903	1930	1	1
209.73.162.12	1056	1060	1	1
193.220.126.253	432	437	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.100.165	57559	58391	9727	9803

33 different signatures are present for *MY.NET.100.165* as a destination

- 1 instances of *spp_http_decode: CGI Null Byte attack detected*
- 1 instances of *WEB-MISC L3retriever HTTP Probe*
- 1 instances of *WEB-MISC whisker head*
- 1 instances of *ICMP IPV6 Where-Are-You*
- 1 instances of *CS WEBSERVER - external ssh traffic*
- 1 instances of *WEB-MISC prefix-get //*
- 1 instances of *CS WEBSERVER - external cmd traffic*
- 2 instances of *WEB-CGI finger access*
- 2 instances of *Null scan!*
- 2 instances of *Probable NMAP fingerprint attempt*
- 2 instances of *SUNRPC highport access!*
- 3 instances of *IDS475/web-iis_web-webdav-propfind*
- 3 instances of *WEB-MISC Attempt to execute cmd*
- 4 instances of *WEB-CGI scriptalias access*
- 4 instances of *NMAP TCP ping!*
- 5 instances of *WEB-CGI ksh access*
- 6 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 7 instances of *INFO FTP anonymous FTP*
- 8 instances of *WEB-IIS _vti_inf access*
- 9 instances of *spp_http_decode: IIS Unicode attack detected*
- 9 instances of *WEB-MISC Lotus Domino directory traversal*
- 9 instances of *WEB-IIS asp-dot attempt*
- 11 instances of *WEB-CGI formmail access*
- 11 instances of *WEB-IIS view source via translate header*
- 13 instances of *WEB-FRONTPAGE _vti_rpc access*
- 20 instances of *WEB-CGI csh access*
- 28 instances of *Watchlist 000222 NET-NCFC*
- 34 instances of *Watchlist 000220 IL-ISDNNET-990517*
- 38 instances of *WEB-CGI redirect access*
- 67 instances of *Queso fingerprint*
- 240 instances of *CS WEBSERVER - external ftp traffic*

- 288 instances of *WEB-MISC http directory traversal*
- 57559 instances of *CS WEBSERVER - external web traffic*

APPENDIX E - MISC traceroute

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
152.2.254.247	777	777	1	1
128.182.61.50	757	757	1	1
130.215.5.33	753	753	1	1
18.201.0.122	749	749	1	1
205.253.57.100	747	747	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.140.9	47804	51582	117	128
MY.NET.70.148	742	27174	9	136
MY.NET.1.1	15	15	1	1
MY.NET.1.9	10	38	5	9
MY.NET.1.4	6	17343	1	4954

6 different signatures are present for *MY.NET.140.9* as a destination Possible hardware issue.

- 1 instances of *DDOS - TFN client command LE*
- 1 instances of *ICMP Echo Request Sun Solaris*
- 5 instances of *Port 55850 udp - Possible myserver activity - ref. 010313-1*
- 956 instances of *ICMP Destination Unreachable (Communication Administratively Prohibited)*
- 2815 instances of *ICMP Destination Unreachable (Host Unreachable)*
- 47804 instances of *MISC traceroute*

15 different signatures are present for *MY.NET.70.148* as a destination. Possible compromised machine. Indicators of possible reconnaissance and then compromise.

- 1 instances of *SMB Name Wildcard*
- 1 instances of *FTP passwd attempt*
- 3 instances of *ICMP Destination Unreachable (Host Unreachable)*
- 3 instances of *INFO - Possible Squid Scan*
- 3 instances of *ICMP Echo Request Windows*
- 4 instances of *Queso fingerprint*
- 4 instances of *SCAN Proxy attempt*
- 5 instances of *ICMP traceroute*
- 6 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 7 instances of *ICMP Destination Unreachable (Communication Administratively Prohibited)*
- 8 instances of *High port 65535 tcp - possible Red Worm - traffic*
- 16 instances of *EXPLOIT x86 NOOP*
- 538 instances of *INFO FTP anonymous FTP*
- 742 instances of *MISC traceroute*
- 25833 instances of *ICMP Echo Request BSDtype*

APPENDIX F - INFO MSN IM Chat data

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
64.4.12.164	693	693	35	35
64.4.12.182	651	651	39	39
MY.NET.98.149	617	633	9	22
64.4.12.186	605	605	29	29
64.4.12.154	602	602	45	45

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
64.4.12.174	894	894	47	47
64.4.12.154	878	878	46	46
64.4.12.182	862	862	47	47
64.4.12.152	800	800	39	39
64.4.12.168	724	724	45	45

5 different signatures are present for *MY.NET.98.149* as a source

- 1 instances of *INFO Napster Client Data*
- 2 instances of *ICMP traceroute*
- 3 instances of *ICMP Echo Request Windows*
- 10 instances of *INFO Inbound GNUTella Connect accept*
- 617 instances of *INFO MSN IM Chat data*

Many of these alerts originated from the 64.4.12.XXX network which belong to MS Hotmail (NETBLK-HOTMAIL) 1065 La Avenida Mountain View, CA 94043 US . Policies should determine appropriate use of MSN Chat.

Appendix G - ICMP Echo Request BSD type

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
141.213.11.120	4974	5113	1	1
129.132.66.28	4451	4639	1	1
5.5.60.8	4249	4375	3	102
129.79.245.106	4120	4310	1	1
147.46.59.144	3607	3738	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
5.5.70.148	25833	27174	11	136
207.207.132.1	4244	4244	2	2
67.161.54.205	1782	1783	1	1
67.160.0.130	1147	1147	1	1
199.172.146.99	486	486	1	1

15 different signatures are present for *5.5.70.148* as a destination

- 1 instances of *SMB Name Wildcard*
- 1 instances of *FTP passwd attempt*
- 3 instances of *ICMP Destination Unreachable (Host Unreachable)*
- 3 instances of *INFO - Possible Squid Scan*
- 3 instances of *ICMP Echo Request Windows*
- 4 instances of *Queso fingerprint*
- 4 instances of *SCAN Proxy attempt*
- 5 instances of *ICMP traceroute*
- 6 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 7 instances of *ICMP Destination Unreachable (Communication Administratively Prohibited)*
- 8 instances of *High port 65535 tcp - possible Red Worm - traffic*
- 16 instances of *EXPLOIT x86 NOOP*
- 538 instances of *INFO FTP anonymous FTP*
- 742 instances of *MISC traceroute*
- 25833 instances of *ICMP Echo Request BSDtype*

Significant traffic from these other institutions to Destination 5.5.70.1.48. Investigation of traffic would determine if this substantial volume is warranted.

129.79.245.106

Indiana University (NET-INDIANA-NET) 2711 E 10th St Bloomington, IN 47408 US Netname: INDIANA-NET Netblock: 129.79.0.0 - 129.79.255.255 Coordinator: Indiana University Computing Services (IUD-ORG-ARIN) dns-admin@indiana.edu 812 855-9255

129.132.66.28

Swiss Federal Institute of Technology (NET-ETH-ETHER) Clausiusstr. 55 Zurich, 8092 CH Netname: ETH-ETHER Netblock: 129.132.0.0 - 129.132.255.255 Coordinator: Brunner, Armin (AB99-ARIN) brunner@KOM.ID.ETHZ.CH +41 1 632 3538 (FAX) +41 1 632 1225

Appendix H - WEB-MISC prefix-get //

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
208.39.140.18	347	416	1	4
24.3.48.210	341	341	1	1
206.196.188.55	270	270	1	1
134.192.66.182	261	261	1	1
207.252.43.130	235	235	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.253.114	32487	33880	1653	1699
MY.NET.253.115	485	504	73	83

23 different signatures are present for *MY.NET.253.114* as a destination. Web servers can be the most visible to the public and should be hardened extensively. The perimeter Firewall should block all but essential services like HTTP (port 80), HTTPS (port 443), SMTP (port 25), etc. An application firewall or filter on the web server can filter GET requests.

- 1 instances of *WEB-IIS view source via translate header*
- 1 instances of *WEB-CGI rsh access*
- 1 instances of *WEB-MISC Lotus Domino directory traversal*
- 1 instances of *IDS475/web-iis_web-webdav-propfind*
- 1 instances of *NMAP TCP ping!*
- 2 instances of *WEB-CGI survey.cgi access*
- 2 instances of *ICMP Echo Request L3retriever Ping*
- 2 instances of *ICMP Echo Request Windows*
- 3 instances of *SCAN Synscan Portscan ID 19104*
- 3 instances of *MISC traceroute*
- 4 instances of *WEB-MISC http directory traversal*
- 4 instances of *WEB-IIS _vti_inf access*
- 5 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 5 instances of *SMB Name Wildcard*
- 5 instances of *Possible trojan server activity*
- 6 instances of *spp_http_decode: IIS Unicode attack detected*
- 6 instances of *WEB-CGI formmail access*
- 7 instances of *WEB-FRONTPAGE _vti_rpc access*
- 9 instances of *WEB-CGI redirect access*
- 15 instances of *Queso fingerprint*
- 28 instances of *ICMP Echo Request Sun Solaris*
- 1282 instances of *Watchlist 000222 NET-NCFC*
- 32487 instances of *WEB-MISC prefix-get //*

Appendix I - Tiny Fragments - Possible Hostile Activity

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.8.1	29009	29009	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.16.42	29009	29095	1	8

Packets are fragmented if they are larger than a network can handle. At destination, the fragmented parts are reassembled. Attacks can occur by "tiny fragments'. The packet is so small that some of the header information is forced into more than one packet creating incomplete header information. Not all firewalls will detect this and therefore allow the packet through.

For this type of attack, the intruder uses IP fragmentation and creates extremely small fragments. This can force the TCP header information into a separate packet fragment. These attacks are successful if they pass the firewall. Many firewalls only examine the first fragment and allow all other fragments to pass. To prevent a tiny fragment attack, configure the firewall to drop packets where the protocol type is TCP and the IP Fragment Offset is equal to 1.

There were 8 different signatures are present for *MY.NET.16.42* as a destination. There are sufficient alerts on both of these internal machines (MY.NET.8.1 and MY.NET.16.42) to investigate a compromise.

- 1 instances of *Tiny Fragments - Possible Hostile Activity [**] MY.NET.8.112/04-19:44:32.070566 [**] INFO MSN IM Chat data*
- 5 instances of *ICMP Echo Request BSDtype*
- 9 instances of *ICMP Destination Unreachable (Communication Administratively Prohibited)*
- 11 instances of *Possible trojan server activity*
- 15 instances of *Port 55850 tcp - Possible myserver activity - ref. 010313-1*
- 22 instances of *High port 65535 tcp - possible Red Worm - traffic*
- 23 instances of *SUNRPC highport access!* 1

APPENDIX J - Watchlist 000220 IL-ISDNNET-990517

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.44.99	15112	15112	1	1
212.179.7.248	1883	1883	1	1
212.179.35.118	1751	1751	4	4
212.179.112.100	1397	1397	15	15
212.179.35.8	620	620	2	2

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.70.42	15112	15136	1	15
MY.NET.163.85	1883	1983	1	9
MY.NET.153.177	615	728	1	5
MY.NET.130.135	614	615	1	2
MY.NET.153.185	486	504	1	4

Significant traffic from 212.179.44.99 using src port 61377 and dst port 6346 (Gnutella) specifically targeted to MY.NET.70.42. The source addresses all come from Israel and could be Gnutella. Gnutella is a peer to peer file-sharing tool using port 6346. Wade Dauphinee had also identified traffic from Israel as possible Gnutella traffic.

APPENDIX K - SMB Name Wildcard

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.228.190	1674	1674	592	592
MY.NET.236.134	1660	1660	977	977
216.150.152.145	1260	2486	1	1
MY.NET.206.238	1254	1254	713	713
MY.NET.230.62	1186	1186	721	721

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.5.44	1260	2514	1	9
MY.NET.5.118	829	1100	2	3
MY.NET.200.222	163	163	1	1
MY.NET.5.76	120	219	1	9
MY.NET.1.4	46	17343	2	4954

There was significant traffic between internal hosts on port 137 to port 137. This is most likely normal traffic. However I would investigate external traffic from 216.150.152.145 to internal hosts. In most cases this service should not be allowed from the outside into a network. It should be dropped at the firewall. Unless absolutely required, MS Network Client should be disabled and removed.