Global Information Assurance Certification Paper

Intrusion Detection In Depth
GCIA Practical Assignment
Version 3.1

Steven L. Drew
January 17, 2005

Assignment 1: "The State of Intrusion Detection"

The Role of Security Event Correlation in Intrusion Detection

Introduction

Millions of dollars have been invested in security products such as firewalls, intrusion detection, and strong authentication over the past several years. However, system penetration attempts continue to occur and go unnoticed until it is too late. As a consequence financial losses continue to skyrocket for organizations. According to the 2002 CSI/FBI Computer Crime and Security Survey, average losses per respondent topped $2,000,000 for the year![1] It is not that security countermeasures are ineffective against intrusive activity. Indeed, they can be very effective within an organization where security policies and procedures require analysis of security events and appropriate incident response. However, as pointed out by Steven Northcutt of SANS, deploying and analyzing a single device in an effort to maintain situational awareness with respect to the state of security within an organization is the "computerized version of tunnel vision"[2]. Security events must be analyzed from as many sources as possible in order to assess threat and formulate appropriate response. Extraordinary levels of security awareness can be attained in an organization's network by simply listening to what its devices are telling you.

This paper will demonstrate to intrusion analysts why correlative analysis must occur in order to understand the complete scope of a security incident.

Correlation Simplified

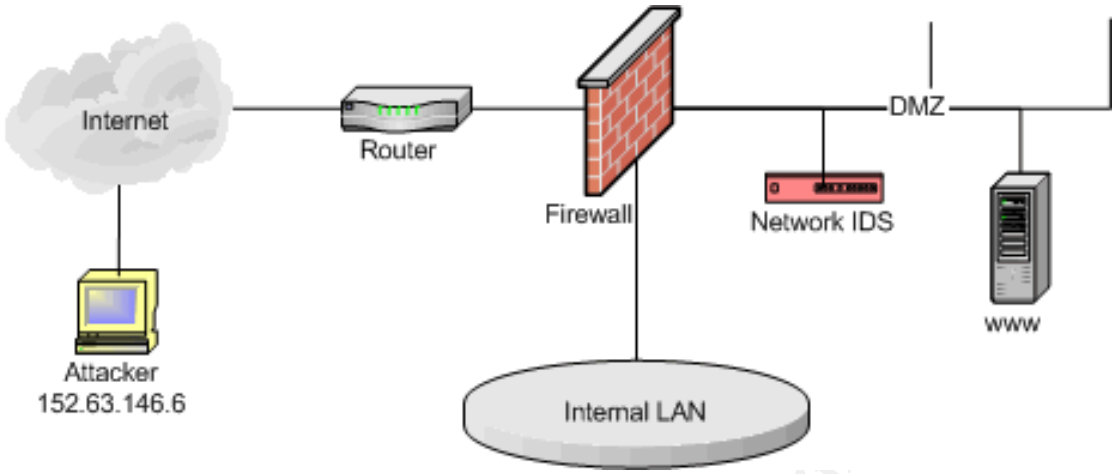
When law enforcement agents investigate a murder, they do more than examine the body for clues. The investigative process calls for searching the surrounding crime scene, interviewing individuals who know the victim, and soliciting requests to the public for anyone who might have information related to the crime.

A similar process should apply to intrusion analysis. If your web server is attacked, analyze more than the web server logs. Search the firewalls and intrusion detection systems protecting the web server for other activity from the source address. Share your log information about the activity with other analyst via websites such as incidents.org. Reviewing all of the information collectively provides a more complete picture of the incident and assists in answering the who, what, when, where, and why's of an attack.

Correlation Demonstrated

Understanding the concepts of correlation can be dramatically simplified if the responses of various network devices are examined in the face of a probe or attack. The following scenario demonstrates how independently obscure security events can be correlated from multiple logs, and in doing so provide the higher level of vision necessary for accurate and expeditious intrusion analysis. We will conduct intrusion analysis of the log data independently and the collectively to show how a more complete picture can be attained trough correlative analysis.
The network below depicts a typical network layout where common countermeasures such as firewalls and intrusion detection systems are deployed.

[1] Power, p. 4.
[2] Northcutt, p.11-8.



In this network, we have established multiple log generators of interest (moving from the perimeter inward):

- Router: Access control lists (ACL's) can provide perimeter packet filtering with (typically) syslog-style alerting. If properly configured ACL's provide network perimeters a first line of defense by defining policy for traffic. When attackers conduct reconnaissance against target networks, ACL's will typically deny at least one element of the attacker's probes and generate a log entry documenting the action. For this exercise, this will be a Cisco 2600 series router.
- Firewall: Depending on the type of firewall and its configuration, extensive visibility can be gained from firewalls. Application proxy firewalls can provide extensive logging and access control capabilities that allow extensive visibility into network traffic passing through the perimeter[3]. For this exercise, the firewall will be a Gauntlet (proxy) firewall.
- Network IDS: By inspecting network traffic, suspicious activity can be flagged and alerts generated. Depending on the type, network IDS typically monitors network traffic for suspicious activity against a database of well-known vulnerabilities and exposures. The alerts generated by network IDS provide valuable interpretative analysis into network activity. However, because of the high rate of false positives associated with network IDS, correlation with other log sources is a ***must*** for alert validation. For this exercise, the network IDS will be Snort running on Linux.
- Application servers (ie. www, ftp, email): Application servers house the data of interest within organizations. As the targets of malicious activity, application servers are the reasons the rest of the security infrastructure is deployed. Common Internet services typically log both successful and failed transactions. These logs provide valuable insight into the overall intent of an attacker along with the success and/or failure of attacks. For this exercise, we will be probing an Apache web server running on Linux.

For this discussion, we will assume the devices have been configured with full logging capabilities such that maximum visibility is attained. For example, the firewall is configured to log both accepted and denied attempts.

We will analyze the log response of all of the network devices while Attacker1 is launching a series of probes searching for exploitable CGI scripts. This activity is being conducted by an attacker at 152.63.146.6 against an Apache web server (www) running on a typical Linux distribution. For this exercise, we will confine the probes to three well known exploits:

- CVE-1999-0067: CGI phf program allows remote command execution through shell metacharacters.
- CVE-1999-0172: FormMail CGI program allows remote execution of commands.

[3] Curtin, Matt and Marcus Ranum. URL

- CVE-1999-0936: BNBSurvey survey.cgi program allows remote attackers to execute commands via shell metacharacters.

Independent Analysis

First, let's review the log activity related to the probe activity for each device in the path of the probes. We will first analyze the information independently and later we will correlate all of the log data for a more complete picture of the incident.

Router Logs (Cisco):

```
May 31 09:27:44 router.company.com 1410875: May 31 09:27:43: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1459) -> xxx.yyy.zzz.1(80), 1 packet

May 31 09:27:50 router.company.com 1410880: May 31 09:27:50: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1673) -> xxx.yyy.zzz.2(80), 1 packet

May 31 09:27:54 router.company.com 1410883: May 31 09:27:53: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1750) -> xxx.yyy.zzz.3 (80), 1 packet

May 31 09:27:57 router.company.com 1410885: May 31 09:27:56: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1722) -> xxx.yyy.zzz.5(80), 1 packet

May 31 09:27:58 router.company.com 1410886: May 31 09:27:57: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1930) -> xxx.yyy.zzz.6(80), 1 packet

May 31 09:28:01 router.company.com 1410888: May 31 09:28:00: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(1976) -> xxx.yyy.zzz.7(80), 1 packet

May 31 09:28:05 router.company.com 1410891: May 31 09:28:04: %SEC-6-IPACCESSLOGP: list from-internet
denied tcp 152.63.146.6(2167) -> xxx.yyy.zzz.8(80), 1 packet
.
. <data pruned>
.
```

For the source address 152.63.146.6, we observe that on May 31 at 09:27 a series of connect attempts occurred directed towards the xxx.yyy.zzz.0/24 network. This log data has been pruned but other entries show the activity directed towards the entire class C. By the destination TCP port 80 connection attempts, it appears as though 152.63.146.6 is conducting a broad scan searching for web servers. It is interesting to note that there was no denied log entry for an access attempt to xxx.yyy.zzz.4 because this is the web server in our network. Our router access control lists have been configured to allow inbound TCP port 80 traffic with ephemeral source ports to xxx.yyy.zzz.4 because this is our company web server.

By only looking at the router logs, the information presented to us suggests 152.63.146.6 swept the entire class C looking for web servers. Independently reviewed, we have no other insight into the intentions of the activity.

In summary for the router logs:

Who:	152.63.146.6
What:	Broad scanning of xxx.yyy.zzz.0/24 network for web servers. Likely found xxx.yyy.zzz.4.
When:	May 31 at 09:27-09:28
Where:	Company DMZ network
Why:	Likely reconnaissance.

Firewall Logs (Gauntlet):

```
Jun  1 06:08:50 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get dest=xxx.yyy.zzz.4 path=/cgi-bin/phf ID=29142174970
```

```
Jun  1 06:08:54 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get dest=xxx.yyy.zzz.4 path=/cgi-bin/formmail   ID=29142174971

Jun  1 06:08:58 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get dest=xxx.yyy.zzz.4 path=/cgi-bin/survey.cgi ID=29142174972
```

For the source address 152.63.146.6, we observe that on June 1st, a series of http connects were allowed to the corporate web server. We see that the URL path shows attempted access on three separate cgi scripts: phf,formmail, and survey.cgi. Reviewed independently, we have no way of knowing if the access attempt was successful. All we know is an attempt was allowed. And unless we are versed in known cgi vulnerabilities, we may simply overlook the activity as legitimate.

In summary for the firewall logs:

Who:	152.63.146.6
What:	Three http connects to xxx.yyy.zzz.4 with access attempts of cgi scripts: phf, formmail, and survey.cgi. Unknown if the scripts were accessed. There were no other http connections from this host so it appears as though this is malicious activity not associated with any other normal web traffic.
When:	June 1 at 06:08:50
Where:	Company DMZ network
Why:	Research shows that phf, formmail, and survey.cgi are all exploitable scripts. These access attempts in isolation suggest malicious activity because if accessed, these scripts could allow remote command execution.

IDS Logs (Snort):

```
 [**] [1:886:3] WEB-CGI phf access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:50.764332 152.63.146.6:3308 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:61884 IpLen:20 DgmLen:280 DF
***AP*** Seq: 0x591AF831  Ack: 0x92D23FAF  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 59902357 300726
[Xref => http://www.securityfocus.com/bid/629]
[Xref => http://www.whitehats.com/info/IDS128]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067]

[**] [1:884:2] WEB-CGI formmail access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:54.411065 152.63.146.6:3309 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:15383 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x85C51FDB  Ack: 0xC0D4B803  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 59974615 372988
[Xref => http://www.securityfocus.com/bid/1187]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0172]
[Xref => http://www.whitehats.com/info/IDS226]

[**] [1:871:2] WEB-CGI survey.cgi access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:58.609416 152.63.146.6:3310 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:32890 IpLen:20 DgmLen:295 DF
***AP*** Seq: 0x8B55C63C  Ack: 0xC624745D  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 59983434 381809
[Xref => http://www.securityfocus.com/bid/1817]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0936]
```

For the source address 152.63.146.6, we observe that on June 1st, a series of cgi access alerts occurred. The alerts point to vulnerabilities associated with these scripts that can be used for remote command execution.

These are the Snort rules that triggered these alerts:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI phf access";flags: A+;
uricontent:"/phf"; nocase; reference:bugtraq,629; reference:arachnids,128; reference:cve,CVE-
1999-0067;  classtype:attempted-recon; sid:886; rev:3;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI formmail access";flags: A+;
uricontent:"/formmail"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172;
reference:arachnids,226; classtype:attempted-recon; sid:884; rev:2;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI survey.cgi access";flags: A+;
uricontent:"/survey.cgi"; nocase; reference:bugtraq,1817; reference:cve,CVE-1999-0936;
classtype:attempted-recon; sid:871; rev:2;)
```

These alerts only trigger when certain strings occur in a URL. These types of alerts are known for false positive alerts. Reviewed independently from other devices, we have no way of knowing if these access attempts were associated with other legitimate access and therefore false positives. However, we can infer that this is malicious because it would be highly irregular for these three scripts to be accessed by back-to-back-to-back connection attempts as indicated by the ephemeral source ports. Even so, we do not know if the attempts were successful or unsuccessful. All we know is that the attempts occurred.

In summary for the IDS logs:

Who:	152.63.146.6
What:	Three http connects to xxx.yyy.zzz.4 with access attempts of cgi scripts: phf, formmail, and survey.cgi. Unknown if the scripts were accessed. There is no other log information available to evaluate if this is a false positive other than the fact these three scripts are unlikely to be accessed within this short of a time frame with incrementing ephemeral source ports.
When:	June 1 at 06:08:50
Where:	Company DMZ network
Why:	If these vulnerable scripts are in operation on the web server, they would allow remote command execution by an attacker.

Web Server Logs (Apache):

access_log

```
152.63.146.6 - - [01/Jun/2002:06:08:50 -0400] "GET /cgi-bin/phf HTTP/1.0" 404 304 "-" "Lynx/2.8.5dev.2
libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2002:06:08:54 -0400] "GET /cgi-bin/formmail HTTP/1.0" 404 309 "-"
"Lynx/2.8.5dev.2 libwww-FM/2.58 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2002:06:08:58 -0400] "GET /cgi-bin/survey.cgi HTTP/1.0" 404 311 "-"
"Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"
```

error_log

```
[Sat Jun  1 06:08:50 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/phf

[Sat Jun  1 06:08:54 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/formmail

[Sat Jun  1 06:08:58 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/survey.cgi
```

For source address 152.63.146.6, we find log entries in both the access_log and error_log. The access log shows that on June 1st at 06:08, attempts to access cgi scripts phf, formmail, and survey.cgi in the cgi-bin subdirectory occurred. The error_log shows that this activity generated errors because these scripts were not

in operation on this server. There were no other http connections from this host so it appears as though this is malicious activity not associated with any other normal web traffic.

In summary for the web server logs:

Who:	152.63.146.6. Likely a Unix/Linux host using Lynx v2.8.5dev.2 as the tool to conduct the activity.
What:	Three http connects to xxx.yyy.zzz.4 with access attempts of cgi scripts: phf, formmail, and survey.cgi. The scripts were not accessed because they could not be found on the server. There were no other http connections from this host so it appears as though this is malicious activity not associated with any other normal web traffic. No other access log entries for 152.63.146.6 suggests this activity is malicious.
When:	June 1 at 06:08:50
Where:	Company DMZ network

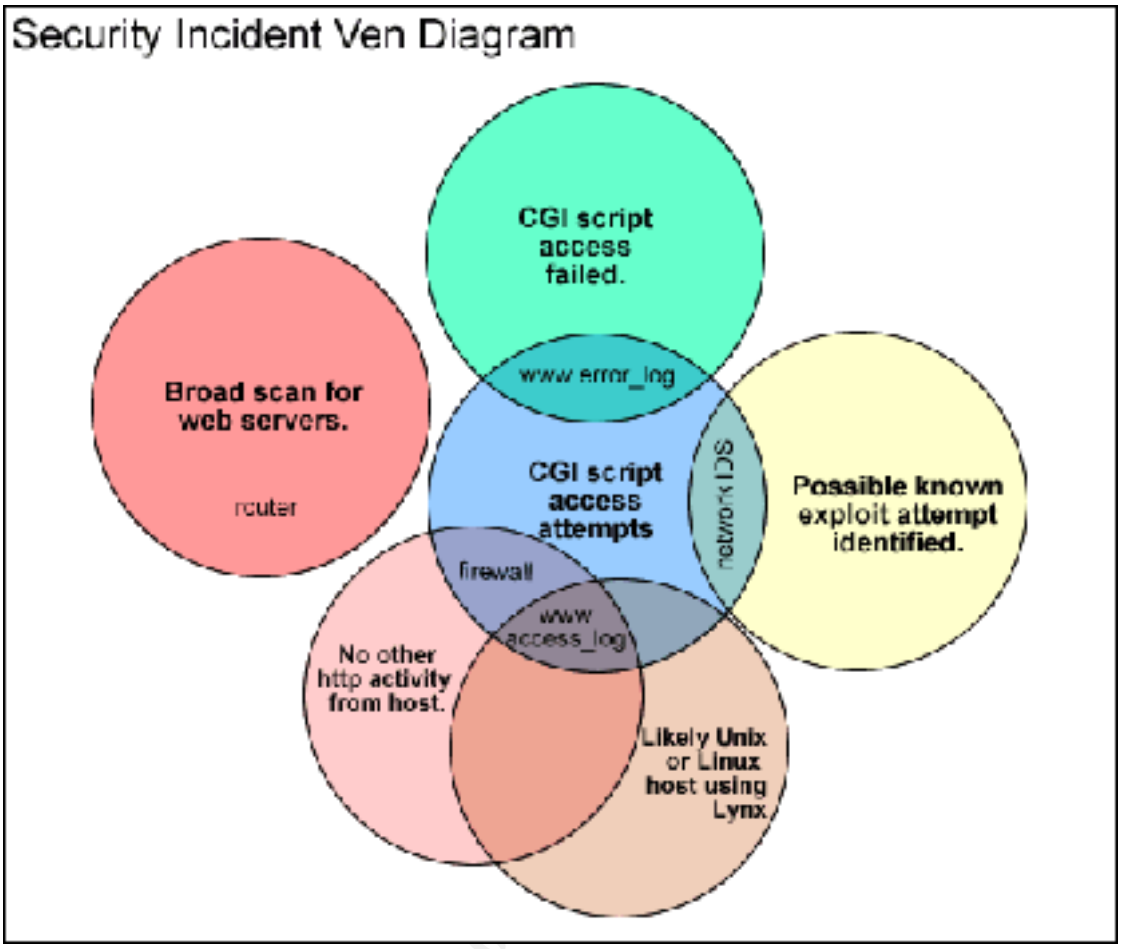
Correlative Analysis

We demonstrated above that attempting to understand the full scope of a security incident is encumbered if logs and alerts from only a single device are analyzed. Each device has its own limits as to what it can tell us in the analysis process. However, collectively analyzed, the picture becomes much clearer. Let's take a look at what we can determine.

There are two separate episodes of activity that comprise the total picture of the security incident perpetrated by 152.63.146.6.

1. On May 31st, host 152.63.146.6 conducted a broad scan of the xxx.yyy.zzz.0/24 network likely in search of web servers (confirmed by router). The interior devices would not have seen this activity because of strong access control lists on the router. The xxx.yyy.zzz.0/24 network is the only public IP address space assigned to the company so it uncertain if this scanning activity is targeted at this company. The logs could be shared with third parties such as via the incidents.org mailing list. This effort can reveal if this activity has been seen by others or if it is perhaps specifically targeted at the company.
2. On June 1st, host 152.63.146.6 attempted three distinct, and only three, http access attempts against the company web server xxx.yyy.zzz.4 (confirmed by the firewall and web server access_log).
    a. These connection attempts requested the phf, formmail, and survey.cgi CGI scripts (confirmed by firewall, web server access_log, and network IDS).
    b. These connection attempts failed (confirmed by web server error_log). It is therefore unlikely that a system compromise has occurred on the company web server.

The following Ven Diagram depicts how the individual network devices contributed to the overall situational awareness achieved through correlative analysis. It shows that removing the analysis of even just one of the device's log data, our understanding of the incident can drop dramatically.



The diagram shows that removing the analysis of even just one of the device's log data, our understanding of the incident can drop dramatically. For example, if we remove the analysis of the web server error_log, we would not have known that the script access attempt failed. If we had not analyzed the router, we would not have known the probing host scanned the entire class C of addresses for web servers. If we had not analyzed the www access_log, we would not have known that the probing host was likely using Lynx as the web browser to check for the scripts. If we had not analyzed the network IDS logs, we may not have known that the activity was related to well known exploit attempts.

Conclusion

Analyzing a single device to in an attempt to conduct intrusion analysis is the "computerized version of tunnel vision"[4]. Security events must be analyzed from as many sources as possible in order to assess threat and formulate appropriate response. Extraordinary levels of security awareness can be attained in an organization's network by simply listening to what its devices are telling you. This concept was demonstrated by examining how security events reviewed independently only paint part of the picture. However, when the correlation of event data across platforms occurs, a more clear understanding of the scope of security incidents is attained.

[4] Northcutt, p.11-8

References

Curtin, Matt and Marcus Ranum. "Firewalls FAQ" URL: http://www.faqs.org/faqs/firewalls-faq/ (May 31, 2002).

"Interpret Syslog and Console Messages Generated by Context-Based Access Control." The Cisco IOS Firewall Feature Set and Context-Based Access Control. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/firewall.htm (May 31, 2002).

"Log Files." Apache HTTP Server Version 2.0. URL: http://httpd.apache.org/docs-2.0/logs.html (June 1, 2002).

Northcutt, Steven. "Coordinated Attacks." IDS Signatures and Analysis-GCIA Courseware. 2001

Power, Richard. 2002 CSI/FBI Computer Crime and Security Survey. Vol. III, No. 1, Spring 2002.

Snort Users Manual – Snort Release: 1.9.x. URL: http://www.snort.org/docs/writing_rules/index.html (June 1, 2002).

Assignment 2: Network Detects

Detect 1: SQLSnake a.k.a. Spida Worm

Note to reader: Since this detect is related to a new worm, I have included an extensive amount of log data (with white space preserved for readability) for other intrusion analyst's benefit and interest. There are a total of eleven conversations documented. There are three basic connection patterns: connection with no data pushed, a connection with data pushed from client with no response from server, and a connection with data pushed from both client and server.

Conversation #1:

```
05/21-06:10:50.840245 63.217.100.34:3228 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:15703 IpLen:20 DgmLen:60 DF
******S* Seq: 0x45B76C5D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47599882 0 NOP WS: 0

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

05/21-06:10:50.890887 my.biz.net.34:1433 -> 63.217.100.34:3228
TCP TTL:114 TOS:0x0 ID:37619 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x64C03372  Ack: 0x45B76C5E  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-06:10:50.891160 63.217.100.34:3228 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:15704 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x45B76C5E  Ack: 0x64C03373  Win: 0x16D0  TcpLen: 20

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

05/21-06:10:50.892341 63.217.100.34:3228 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:15705 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x45B76C5E  Ack: 0x64C03373  Win: 0x16D0  TcpLen: 20

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

05/21-06:10:50.945306 my.biz.net.34:1433 -> 63.217.100.34:3228
TCP TTL:114 TOS:0x0 ID:38643 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x64C03373  Ack: 0x45B76C5F  Win: 0x2238  TcpLen: 20

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

05/21-06:10:51.559123 my.biz.net.34:1433 -> 63.217.100.34:3228
TCP TTL:114 TOS:0x0 ID:45811 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x64C03373  Ack: 0x45B76C5F  Win: 0x2238  TcpLen: 20

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

05/21-06:10:51.559336 63.217.100.34:3228 -> my.biz.net.34:1433
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x45B76C5F  Ack: 0x64C03374  Win: 0x16D0  TcpLen: 20

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

Conversation #2:

```
05/21-06:32:49.201570 63.217.100.34:3229 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:41589 IpLen:20 DgmLen:60 DF
******S* Seq: 0x9825F673  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47731718 0 NOP WS: 0

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

05/21-06:32:49.251952 my.biz.net.34:1433 -> 63.217.100.34:3229
TCP TTL:114 TOS:0x0 ID:14474 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x658F46C9  Ack: 0x9825F674  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460
```

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

05/21-06:32:49.252230 63.217.100.34:3229 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:41590 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x9825F674  Ack: 0x658F46CA  Win: 0x16D0  TcpLen: 20

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

05/21-06:32:49.664225 63.217.100.34:3229 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:41591 IpLen:20 DgmLen:92 DF
***AP*** Seq: 0x9825F674  Ack: 0x658F46CA  Win: 0x16D0  TcpLen: 20
12 01 00 34 00 00 00 00 00 00 15 00 06 01 00 1B  ...4............
00 01 02 00 1C 00 0C 03 00 28 00 04 FF 08 00 00  .........(......
C2 00 00 00 4D 53 53 51 4C 53 65 72 76 65 72 00  ....MSSQLServer.
08 08 00 00                                      ....

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

05/21-06:32:49.791951 my.biz.net.34:1433 -> 63.217.100.34:3229
TCP TTL:114 TOS:0x0 ID:14730 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x658F46CA  Ack: 0x9825F6A8  Win: 0x2204  TcpLen: 20

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

05/21-06:32:49.792835 63.217.100.34:3229 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:41592 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x9825F6A8  Ack: 0x658F46CB  Win: 0x16D0  TcpLen: 20

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

05/21-06:32:49.843811 my.biz.net.34:1433 -> 63.217.100.34:3229
TCP TTL:114 TOS:0x0 ID:14986 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x658F46CB  Ack: 0x9825F6A9  Win: 0x2204  TcpLen: 20

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

Conversation #3:

```
05/21-06:32:50.346895 63.217.100.34:3230 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:47272 IpLen:20 DgmLen:60 DF
******S* Seq: 0x98F6ECD0  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47731832 0 NOP WS: 0

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

05/21-06:32:50.437698 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:21386 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x658F46CB  Ack: 0x98F6ECD1  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-06:32:50.437907 63.217.100.34:3230 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:47273 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x98F6ECD1  Ack: 0x658F46CC  Win: 0x16D0  TcpLen: 20

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

05/21-06:32:50.438629 63.217.100.34:3230 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:47274 IpLen:20 DgmLen:250 DF
***AP*** Seq: 0x98F6ECD1  Ack: 0x658F46CC  Win: 0x16D0  TcpLen: 20
10 01 00 D2 00 00 01 00 CA 00 00 00 00 00 00 71  ...............q
00 10 00 00 00 00 00 07 E4 09 00 00 00 00 00 00  ................
E0 03 10 00 20 FE FF FF 04 0C 00 00 56 00 06 00  .... .......V...
62 00 02 00 00 00 00 00 66 00 21 00 A8 00 0C 00  b.......f.!.....
00 00 00 00 C0 00 05 00 CA 00 00 00 CA 00 00 00  ................
00 C0 DF 04 B9 51 00 00 00 00 CA 00 00 00 53 00  .....Q........S.
45 00 52 00 56 00 45 00 52 00 73 00 61 00 4D 00  E.R.V.E.R.s.a.M.
69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00  i.c.r.o.s.o.f.t.
20 00 28 00 72 00 29 00 20 00 57 00 69 00 6E 00   .(.r.). .W.i.n.
64 00 6F 00 77 00 73 00 20 00 53 00 63 00 72 00  d.o.w.s. .S.c.r.
69 00 70 00 74 00 20 00 48 00 6F 00 73 00 74 00  i.p.t. .H.o.s.t.
32 00 34 00 2E 00 33 00 31 00 2E 00 32 00 30 00  2.4...3.1...2.0.
34 00 2E 00 38 00 32 00 4F 00 4C 00 45 00 44 00  4...8.2.O.L.E.D.
42 00                                            B.
```

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

05/21-06:32:50.783856 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:41098 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x658F46CC  Ack: 0x98F6EDA3  Win: 0x2166  TcpLen: 20

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

05/21-06:32:50.900766 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:41354 IpLen:20 DgmLen:126 DF
***AP*** Seq: 0x658F46CC  Ack: 0x98F6EDA3  Win: 0x2166  TcpLen: 20
04 01 00 56 00 00 00 00 AA 42 00 18 48 00 00 01  ...V.....B..H...
0E 1B 00 4C 00 6F 00 67 00 69 00 6E 00 20 00 66  ...L.o.g.i.n. .f
00 61 00 69 00 6C 00 65 00 64 00 20 00 66 00 6F  .a.i.l.e.d. .f.o
00 72 00 20 00 75 00 73 00 65 00 72 00 20 00 27  .r. .u.s.e.r. .'
00 73 00 61 00 27 00 2E 00 00 00 00 00 FD 02 00  .s.a.'.........
00 00 00 00 00 00                                ......

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

05/21-06:32:50.900962 63.217.100.34:3230 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:47275 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x98F6EDA3  Ack: 0x658F4722  Win: 0x16D0  TcpLen: 20

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

05/21-06:32:50.904319 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:41610 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x658F4722  Ack: 0x98F6EDA3  Win: 0x2166  TcpLen: 20

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

05/21-06:32:50.905849 63.217.100.34:3230 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:47276 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x98F6EDA3  Ack: 0x658F4723  Win: 0x16D0  TcpLen: 20

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

05/21-06:32:50.961482 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:42122 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x658F4723  Ack: 0x98F6EDA4  Win: 0x2166  TcpLen: 20

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

Conversation #4:

```
05/21-06:36:02.393667 63.217.100.34:3231 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57283 IpLen:20 DgmLen:60 DF
******S* Seq: 0xA3F040BE  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47751037 0 NOP WS: 0

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

05/21-06:36:02.443649 my.biz.net.34:1433 -> 63.217.100.34:3231
TCP TTL:114 TOS:0x0 ID:48034 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x65D2050C  Ack: 0xA3F040BF  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-06:36:02.443875 63.217.100.34:3231 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57284 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA3F040BF  Ack: 0x65D2050D  Win: 0x16D0  TcpLen: 20

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

05/21-06:36:02.445035 63.217.100.34:3231 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57285 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xA3F040BF  Ack: 0x65D2050D  Win: 0x16D0  TcpLen: 20

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

05/21-06:36:02.504770 my.biz.net.34:1433 -> 63.217.100.34:3231
TCP TTL:114 TOS:0x0 ID:48546 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x65D2050D  Ack: 0xA3F040C0  Win: 0x2238  TcpLen: 20
```

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

05/21-06:36:02.560684 my.biz.net.34:1433 -> 63.217.100.34:3231
TCP TTL:114 TOS:0x0 ID:48802 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x65D2050D  Ack: 0xA3F040C0  Win: 0x2238  TcpLen: 20

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

05/21-06:36:02.560891 63.217.100.34:3231 -> my.biz.net.34:1433
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA3F040C0  Ack: 0x65D2050E  Win: 0x16D0  TcpLen: 20

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

Conversation #5:

```
05/21-06:50:54.402909 63.217.100.34:3232 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:14294 IpLen:20 DgmLen:60 DF
******S* Seq: 0xDCF6CC38  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47840238 0 NOP WS: 0

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

05/21-06:50:54.452270 my.biz.net.34:1433 -> 63.217.100.34:3232
TCP TTL:114 TOS:0x0 ID:12819 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x668158B1  Ack: 0xDCF6CC39  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-06:50:54.452524 63.217.100.34:3232 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:14295 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xDCF6CC39  Ack: 0x668158B2  Win: 0x16D0  TcpLen: 20

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

05/21-06:50:54.453712 63.217.100.34:3232 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:14296 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xDCF6CC39  Ack: 0x668158B2  Win: 0x16D0  TcpLen: 20

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

05/21-06:50:54.506301 my.biz.net.34:1433 -> 63.217.100.34:3232
TCP TTL:114 TOS:0x0 ID:13075 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x668158B2  Ack: 0xDCF6CC3A  Win: 0x2238  TcpLen: 20

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

05/21-06:50:55.012491 my.biz.net.34:1433 -> 63.217.100.34:3232
TCP TTL:114 TOS:0x0 ID:14611 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x668158B2  Ack: 0xDCF6CC3A  Win: 0x2238  TcpLen: 20

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

05/21-06:50:55.012722 63.217.100.34:3232 -> my.biz.net.34:1433
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xDCF6CC3A  Ack: 0x668158B3  Win: 0x16D0  TcpLen: 20
```

Conversation #6:

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

05/21-07:00:35.096310 63.217.100.34:3233 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:48160 IpLen:20 DgmLen:60 DF
******S* Seq: 0x24762E3  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47898307 0 NOP WS: 0

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

05/21-07:00:35.144847 my.biz.net.34:1433 -> 63.217.100.34:3233
TCP TTL:114 TOS:0x0 ID:23644 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x66A76668  Ack: 0x24762E4  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

```
05/21-07:00:35.145123 63.217.100.34:3233 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:48161 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x24762E4  Ack: 0x66A76669  Win: 0x16D0  TcpLen: 20

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

05/21-07:00:36.029132 63.217.100.34:3233 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:48162 IpLen:20 DgmLen:92 DF
***AP*** Seq: 0x24762E4  Ack: 0x66A76669  Win: 0x16D0  TcpLen: 20
12 01 00 34 00 00 00 00 00 00 15 00 06 01 00 1B  ...4............
00 01 02 00 1C 00 0C 03 00 28 00 04 FF 08 00 00  .........(......
C2 00 00 00 4D 53 53 51 4C 53 65 72 76 65 72 00  ....MSSQLServer.
74 04 00 00                                      t...

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

05/21-07:00:36.112483 my.biz.net.34:1433 -> 63.217.100.34:3233
TCP TTL:114 TOS:0x0 ID:43356 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x66A76669  Ack: 0x2476318  Win: 0x2204  TcpLen: 20

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

05/21-07:00:36.113364 63.217.100.34:3233 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:48163 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x2476318  Ack: 0x66A7666A  Win: 0x16D0  TcpLen: 20

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

05/21-07:00:36.173043 my.biz.net.34:1433 -> 63.217.100.34:3233
TCP TTL:114 TOS:0x0 ID:43612 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x66A7666A  Ack: 0x2476319  Win: 0x2204  TcpLen: 20

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

Conversation #7:

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

05/21-07:00:36.604556 63.217.100.34:3234 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:62831 IpLen:20 DgmLen:60 DF
******S* Seq: 0x1932A35  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47898458 0 NOP WS: 0

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

05/21-07:00:36.654538 my.biz.net.34:1433 -> 63.217.100.34:3234
TCP TTL:114 TOS:0x0 ID:44124 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x66BAF151  Ack: 0x1932A36  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-07:00:36.654772 63.217.100.34:3234 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:62832 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1932A36  Ack: 0x66BAF152  Win: 0x16D0  TcpLen: 20

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

05/21-07:00:36.655534 63.217.100.34:3234 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:62833 IpLen:20 DgmLen:264 DF
***AP*** Seq: 0x1932A36  Ack: 0x66BAF152  Win: 0x16D0  TcpLen: 20
10 01 00 E0 00 00 01 00 D8 00 00 00 00 00 00 71  ...............q
00 10 00 00 00 00 00 07 3C 04 00 00 00 00 00 00  ........<.......
E0 03 10 00 E4 FD FF FF 12 04 00 00 56 00 0E 00  ............V...
72 00 02 00 00 00 00 00 76 00 20 00 B6 00 0C 00  r.......v. .....
00 00 00 00 CE 00 05 00 D8 00 00 00 D8 00 00 00  ................
00 03 47 BD 63 0C 00 00 00 00 D8 00 00 00 4A 00  ..G.c.........J.
55 00 4E 00 47 00 53 00 4F 00 46 00 54 00 2D 00  U.N.G.S.O.F.T.-.
49 00 4E 00 54 00 52 00 41 00 73 00 61 00 4D 00  I.N.T.R.A.s.a.M.
69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00  i.c.r.o.s.o.f.t.
28 00 52 00 29 00 20 00 57 00 69 00 6E 00 64 00  (.R.). .W.i.n.d.
6F 00 77 00 73 00 20 00 53 00 63 00 72 00 69 00  o.w.s. .S.c.r.i.
70 00 74 00 20 00 48 00 6F 00 73 00 74 00 32 00  p.t. .H.o.s.t.2.
34 00 2E 00 33 00 31 00 2E 00 32 00 30 00 34 00  4...3.1...2.0.4.
2E 00 38 00 32 00 4F 00 4C 00 45 00 44 00 42 00  ..8.2.O.L.E.D.B.
```

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

05/21-07:00:36.843743 my.biz.net.34:1433 -> 63.217.100.34:3234
TCP TTL:114 TOS:0x0 ID:44380 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x66BAF152  Ack: 0x1932B16  Win: 0x2158  TcpLen: 20

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

05/21-07:00:37.165326 my.biz.net.34:1433 -> 63.217.100.34:3234
TCP TTL:114 TOS:0x0 ID:44892 IpLen:20 DgmLen:126 DF
***AP*** Seq: 0x66BAF152  Ack: 0x1932B16  Win: 0x2158  TcpLen: 20
04 01 00 56 00 00 00 00 AA 42 00 18 48 00 00 01  ...V.....B..H...
0E 1B 00 4C 00 6F 00 67 00 69 00 6E 00 20 00 66  ...L.o.g.i.n. .f
00 61 00 69 00 6C 00 65 00 64 00 20 00 66 00 6F  .a.i.l.e.d. .f.o
00 72 00 20 00 75 00 73 00 65 00 72 00 20 00 27  .r. .u.s.e.r. .'
00 73 00 61 00 27 00 2E 00 00 00 00 00 FD 02 00  .s.a.'..........
00 00 00 00 00 00                                ......

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

05/21-07:00:37.165535 63.217.100.34:3234 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:62834 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1932B16  Ack: 0x66BAF1A8  Win: 0x16D0  TcpLen: 20

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

05/21-07:00:37.170190 my.biz.net.34:1433 -> 63.217.100.34:3234
TCP TTL:114 TOS:0x0 ID:45148 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x66BAF1A8  Ack: 0x1932B16  Win: 0x2158  TcpLen: 20

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

05/21-07:00:37.171013 63.217.100.34:3234 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:62835 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1932B16  Ack: 0x66BAF1A9  Win: 0x16D0  TcpLen: 20

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

05/21-07:00:37.221991 my.biz.net.34:1433 -> 63.217.100.34:3234
TCP TTL:114 TOS:0x0 ID:45404 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x66BAF1A9  Ack: 0x1932B17  Win: 0x2158  TcpLen: 20

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

Conversation #8:

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

05/21-07:12:37.530589 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57297 IpLen:20 DgmLen:60 DF
******S* Seq: 0x2EB32726  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 47970551 0 NOP WS: 0

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

05/21-07:12:37.579245 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:1207 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x672B7708  Ack: 0x2EB32727  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-07:12:37.579515 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57298 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x2EB32727  Ack: 0x672B7709  Win: 0x16D0  TcpLen: 20

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

05/21-07:12:37.580342 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57299 IpLen:20 DgmLen:552 DF
***AP*** Seq: 0x2EB32727  Ack: 0x672B7709  Win: 0x16D0  TcpLen: 20
02 00 02 00 00 00 01 00 43 58 33 34 32 39 39 38  ........CX342998
2D 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00  -B..............
00 00 00 00 00 00 0A 73 61 00 00 00 00 00 00 00  .......sa.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00  ................
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 30 30 30 30 30 36 39 63 00 00 00  .....0000069c...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 B3  ................
2F 58 4E 08 03 01 06 0A 09 01 01 00 00 00 00 00  /XN.............
00 00 00 00 4D 69 63 72 6F 73 6F 66 74 20 28 72  ....Microsoft (r
29 20 57 00 00 00 00 00 00 00 00 00 00 00 00 00  ) W.............
00 00 0F 32 34 2E 33 31 2E 32 30 34 2E 38 32 00  ...63.217.100.34.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 02 04 02 00 00 4F 4C 45 44 42 00 00 00 00 00  ......OLEDB.....
05 06 00 00 00 00 0D 11 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

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

05/21-07:12:37.848950 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:1975 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x672B7709  Ack: 0x2EB32927  Win: 0x2038  TcpLen: 20

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

05/21-07:12:37.849163 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57300 IpLen:20 DgmLen:111 DF
***AP*** Seq: 0x2EB32927  Ack: 0x672B7709  Win: 0x16D0  TcpLen: 20
02 01 00 47 00 00 02 00 00 00 00 00 00 00 00 01  ...G............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 34 30 39  .............409
36 00 00 04 00 00 00                             6......

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

05/21-07:12:38.056300 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:2487 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x672B7709  Ack: 0x2EB3296E  Win: 0x1FF1  TcpLen: 20

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

05/21-07:12:38.242640 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:3511 IpLen:20 DgmLen:99 DF
***AP*** Seq: 0x672B7709  Ack: 0x2EB3296E  Win: 0x1FF1  TcpLen: 20
04 01 00 3B 00 00 00 00 AA 27 00 18 48 00 00 01  ...;.....'..H...
0E 1B 00 4C 6F 67 69 6E 20 66 61 69 6C 65 64 20  ...Login failed
66 6F 72 20 75 73 65 72 20 27 73 61 27 2E 00 00  for user 'sa'...
00 00 FD 02 00 00 00 00 00 00                    ..........

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

05/21-07:12:38.242828 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57301 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x2EB3296E  Ack: 0x672B7744  Win: 0x16D0  TcpLen: 20

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

05/21-07:12:38.246146 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:3767 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x672B7744  Ack: 0x2EB3296E  Win: 0x1FF1  TcpLen: 20

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

```
05/21-07:12:38.246987 63.217.100.34:3235 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:57302 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x2EB3296E  Ack: 0x672B7745  Win: 0x16D0  TcpLen: 20

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

05/21-07:12:38.299310 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:4023 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x672B7745  Ack: 0x2EB3296F  Win: 0x1FF1  TcpLen: 20

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

Conversation #9:

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

05/21-07:51:31.137443 63.217.100.34:3236 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:13180 IpLen:20 DgmLen:60 DF
******S* Seq: 0xC21FBBFB  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48203911 0 NOP WS: 0

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

05/21-07:51:31.192513 my.biz.net.34:1433 -> 63.217.100.34:3236
TCP TTL:114 TOS:0x0 ID:55002 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x687D5A9D  Ack: 0xC21FBBFC  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-07:51:31.192760 63.217.100.34:3236 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:13181 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC21FBBFC  Ack: 0x687D5A9E  Win: 0x16D0  TcpLen: 20

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

05/21-07:51:31.193942 63.217.100.34:3236 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:13182 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xC21FBBFC  Ack: 0x687D5A9E  Win: 0x16D0  TcpLen: 20

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

05/21-07:51:31.270836 my.biz.net.34:1433 -> 63.217.100.34:3236
TCP TTL:114 TOS:0x0 ID:55770 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x687D5A9E  Ack: 0xC21FBBFD  Win: 0x2238  TcpLen: 20

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

05/21-07:51:31.675789 my.biz.net.34:1433 -> 63.217.100.34:3236
TCP TTL:114 TOS:0x0 ID:57562 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x687D5A9E  Ack: 0xC21FBBFD  Win: 0x2238  TcpLen: 20

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

05/21-07:51:31.676014 63.217.100.34:3236 -> my.biz.net.34:1433
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC21FBBFD  Ack: 0x687D5A9F  Win: 0x16D0  TcpLen: 20

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

Conversation #10:

```
05/21-08:13:29.630429 63.217.100.34:3237 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:60418 IpLen:20 DgmLen:60 DF
******S* Seq: 0x14356793  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48335761 0 NOP WS: 0

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

05/21-08:13:29.686471 my.biz.net.34:1433 -> 63.217.100.34:3237
TCP TTL:114 TOS:0x0 ID:62591 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x6902604B  Ack: 0x14356794  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

```
05/21-08:13:29.686756 63.217.100.34:3237 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:60419 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x14356794  Ack: 0x6902604C  Win: 0x16D0  TcpLen: 20

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

05/21-08:13:29.848762 63.217.100.34:3237 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:60420 IpLen:20 DgmLen:92 DF
***AP*** Seq: 0x14356794  Ack: 0x6902604C  Win: 0x16D0  TcpLen: 20
12 01 00 34 00 00 00 00 00 00 15 00 06 01 00 1B  ...4............
00 01 02 00 1C 00 0C 03 00 28 00 04 FF 08 00 00  .........(......
C2 00 00 00 4D 53 53 51 4C 53 65 72 76 65 72 00  ....MSSQLServer.
8C 03 00 00                                      ....

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

05/21-08:13:30.007976 my.biz.net.34:1433 -> 63.217.100.34:3237
TCP TTL:114 TOS:0x0 ID:62847 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6902604C  Ack: 0x143567C8  Win: 0x2204  TcpLen: 20

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

05/21-08:13:30.345803 my.biz.net.34:1433 -> 63.217.100.34:3237
TCP TTL:114 TOS:0x0 ID:3968 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x6902604C  Ack: 0x143567C8  Win: 0x2204  TcpLen: 20

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

05/21-08:13:30.346689 63.217.100.34:3237 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:60421 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x143567C8  Ack: 0x6902604D  Win: 0x16D0  TcpLen: 20

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

05/21-08:13:30.401727 my.biz.net.34:1433 -> 63.217.100.34:3237
TCP TTL:114 TOS:0x0 ID:4224 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6902604D  Ack: 0x143567C9  Win: 0x2204  TcpLen: 20

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

Conversation #11:

```
05/21-08:13:30.642811 63.217.100.34:3238 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:4006 IpLen:20 DgmLen:60 DF
******S* Seq: 0x144C8450  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48335862 0 NOP WS: 0

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

05/21-08:13:30.696502 my.biz.net.34:1433 -> 63.217.100.34:3238
TCP TTL:114 TOS:0x0 ID:4480 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x69026053  Ack: 0x144C8451  Win: 0x2238  TcpLen: 24
TCP Options (1) => MSS: 1460

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

05/21-08:13:30.696714 63.217.100.34:3238 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:4007 IpLen:20 DgmLen:40 DF
Snort received signal 3, exiting
***A**** Seq: 0x144C8451  Ack: 0x69026054  Win: 0x16D0  TcpLen: 20

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

05/21-08:13:30.697424 63.217.100.34:3238 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:4008 IpLen:20 DgmLen:248 DF
***AP*** Seq: 0x144C8451  Ack: 0x69026054  Win: 0x16D0  TcpLen: 20
10 01 00 D0 00 00 01 00 C8 00 00 00 00 00 00 71  ...............q
00 10 00 00 00 00 00 07 14 03 00 00 00 00 00 00  ................
E0 03 10 00 C4 FF FF FF 10 04 00 00 56 00 05 00  ............V...
60 00 02 00 00 00 00 00 64 00 21 00 A6 00 0C 00  `.......d.!.....
00 00 00 00 BE 00 05 00 C8 00 00 00 C8 00 00 00  ................
00 30 84 40 F3 DD 00 00 00 00 C8 00 00 00 56 00  .0.@..........V.
49 00 4F 00 4C 00 41 00 73 00 61 00 4D 00 69 00  I.O.L.A.s.a.M.i.
63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00  c.r.o.s.o.f.t. .
28 00 72 00 29 00 20 00 57 00 69 00 6E 00 64 00  (.r.). .W.i.n.d.
6F 00 77 00 73 00 20 00 53 00 63 00 72 00 69 00  o.w.s. .S.c.r.i.
70 00 74 00 20 00 48 00 6F 00 73 00 74 00 32 00  p.t. .H.o.s.t.2.
```

```
34 00 2E 00 33 00 31 00 2E 00 32 00 30 00 34 00  4...3.1...2.0.4.
2E 00 38 00 32 00 4F 00 4C 00 45 00 44 00 42 00  ..8.2.O.L.E.D.B.

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

05/21-08:13:30.910318 my.biz.net.34:1433 -> 63.217.100.34:3238
TCP TTL:114 TOS:0x0 ID:5504 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x69026054  Ack: 0x144C8521  Win: 0x2168  TcpLen: 20

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

05/21-08:13:31.239161 my.biz.net.34:1433 -> 63.217.100.34:3238
TCP TTL:114 TOS:0x0 ID:12160 IpLen:20 DgmLen:126 DF
***AP*** Seq: 0x69026054  Ack: 0x144C8521  Win: 0x2168  TcpLen: 20
04 01 00 56 00 00 00 00 AA 42 00 18 48 00 00 01  ...V.....B..H...
0E 1B 00 4C006F00670069006E00200066  ...L.o.g.i.n. .f
00610069006C00650064002000660066006F  .a.i.l.e.d. .f.o
0072002000750073006500720020002700 .r. .u.s.e.r. .'
007300610027002E 00 00 00 00 00 FD 02 00  .s.a.'.........
00 00 00 00 00 00                                ......

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

05/21-08:13:31.239362 63.217.100.34:3238 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:4009 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x144C8521  Ack: 0x690260AA  Win: 0x16D0  TcpLen: 20

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

05/21-08:13:31.242641 my.biz.net.34:1433 -> 63.217.100.34:3238
TCP TTL:114 TOS:0x0 ID:12416 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x690260AA  Ack: 0x144C8521  Win: 0x2168  TcpLen: 20

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

05/21-08:13:31.243428 63.217.100.34:3238 -> my.biz.net.34:1433
TCP TTL:64 TOS:0x0 ID:4010 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x144C8521  Ack: 0x690260AB  Win: 0x16D0  TcpLen: 20

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

05/21-08:13:31.301831 my.biz.net.34:1433 -> 63.217.100.34:3238
TCP TTL:114 TOS:0x0 ID:12672 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x690260AB  Ack: 0x144C8522  Win: 0x2168  TcpLen: 20

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


Snort Alerts:
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
 [**] [1:688:3] MS-SQL sa login failed [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1]
05/21-07:12:38.242640 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:3511 IpLen:20 DgmLen:99 DF
***AP*** Seq: 0x672B7709  Ack: 0x2EB3296E  Win: 0x1FF1  TcpLen: 20
```


1. Source of Trace

The source of this trace is from my workplace network where a Microsoft SQL server is setup in a DMZ. *Tcpdump* captured raw packets in binary format and they were subsequently processed by *Snort* for decoding and analysis. It should be noted that the *Snort* rule set only triggered a single alert for this traffic. This is addressed further in the analysis with proposed new *Snort* rules offered under "Defensive Recommendations" to trigger on all of the attempts.

2. Detect was generated by:

This detect was generated by Snort Version 1.9-dev (Build 93).

The packet traces were originally written to file in binary format by *tcpdump* using the following command:

```
tcpdump -n -w dumpfile.20020521
```

Snort was subsequently used in both sniffer and IDS mode for anaylsis.

```
Packet Decodes:
snort -dva -r dumpfile.20020521 host 63.217.100.34

IDS Alerts:
snort  -r dumpfile.20020521 -A full -O -c /etc/snort/snort.conf
```

The following Snort rule triggered the single alert generated by this traffic.

```
alert tcp $SQL_SERVERS 1433 -> $EXTERNAL_NET any (msg:"MS-SQL sa login failed"; content: "Login
failed for user |27|sa|27|"; flags:A+; classtype:unsuccessful-user; sid:688; rev:3;)
```

This was of interest because it identified a potential gap in the Snort IDS signature set. Snort only triggered on one of four failed sa login attempts. New signatures are proposed under "Defensive Recommendations"of this section.

3. Probability source address was spoofed:

This appears to be an attempt to gain administrative access to a Microsoft SQL database. A 3-way TCP handshake is required to negotiate communication so authentication can occur. This makes spoofing unlikely. In addition, as discussed further under "Attack Mechanism", this detect is believed to associated with worm activity. If this is the SQLSnake worm, the source address is not spoofed.

The likelihood of a spoofed source address is further mitigated by the firewall being configured not to accept source routed packets.

4. Description of attack:

According to the Neohapsis port list[1], Microsoft SQL Server uses port 1433 for communication. Analysis of the data payload confirms this is indeed Microsoft SQL Server traffic.

There are many known vulnerabilities for Microsoft SQL Server found on the cve.mitre.org web database including the following:

- CVE-2001-0344
- CVE-2000-0603
- CVE-2000-0485
- CVE-2000-0402
- CVE-2000-0202
- CVE-2000-0161
- CVE-1999-0999

Review of the detect show repetitive password attempts on the 'sa' account which is used for server administration.

[1] Neohapsis Ports List. URL: http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html (May 26, 2002).

5. Attack mechanism:

This appears to be an attempt to gain "sa" (administrator) access to the database through password guessing. Because of the date of the detect, this is likely associated with the SQLSnake a.k.a. SQL Spida Worm outbreak that occurred the week of May 20, 2002[2].

The attack does not exploit code vulnerabilities as much as it exploits server administrator ignorance and/or carelessness. Microsoft SQL Server allows you to configure the server with no 'sa' password subsequently allowing anyone to remotely take control of the SQL server. As so eloquently stated on the SQL Security website[3], "There is no 'patch' for stupidity."

Other default passwords were attempted that may be associated with third party application communication with SQL servers. The following passwords were identified as a part of this exploit attempt:

Conversation 3:	SERVER
Conversation 7:	JUNGSOFT-INTRA
Conversation 8:	<blank password>
Conversation 11:	VIOLA

6. Correlations

While the source address was not cited on DShield or other incident related web sites, there is substantial correlative evidence that suggests this is a part of the SQLSnake worm activity. The major incidents mailing lists have been buzzing regarding port 1433 traffic[4].

Major CERT and industry advisories are as follows:

- NIPC: http://www.nipc.gov/warnings/advisories/2002/02-003.htm
- CERT: http://www.cert.org/incident_notes/IN-2002-04.html
- Internet Security Systems: http://www.iss.net/security_center/alerts/advise118.php
- Computer Associates: http://www3.ca.com/virus/virus.asp?ID=11903
- Trend Micro:http://antivirus.com/vinfo/virusencyclo/default5.asp?VName=BAT_SQLSPIDA.B

7. Evidence of active targeting:

Once the SQLSnake (or Spida) worm infects a host, it begins scanning for new targets.[5] This suggests that host 63.217.100.34 randomly chose my.biz.net.34 as its target as a part of the worm logic. If this is indeed worm traffic, it is very unlikely targeted.

8. Severity:

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

Criticality: 5

The targeted system is a Microsoft SQL database server with sensitive information in a DMZ. This host also has trust relationships with internal hosts that could position it as a jump point if compromised.

---

[2] SQL Security. URL: http://www.sqlsecurity.com/ (May 27, 2002).
[3] SQL Security. URL: http://www.sqlsecurity.com/ (May 27, 2002).
[4] "Strange scan on 1433." URL: http://archives.neohapsis.com/archives/incidents/2002-05/0103.html (May 29, 2002).
[5] "Microsoft SQL Spida Worm Propagation." Internet Security Systems Security Alert: May 21, 2002. URL:http://www.iss.net/security_center/alerts/advise118.php (May 27, 2002).

Lethality: 5
Successful password guess would result in complete database compromise.

System Countermeasures: 5
The operating system and server software is patched with the latest fixes. The SQL 'sa' account is configured with a strong password consisting of a mix of eight or more alphanumeric characters.

Network Countermeasures: 2
The perimeter security mechanisms (router and/or firewall) allowed a random connection to the SQL server. Snort only generated one alert for four distinct password guesses.

(5 + 5) – (5 + 2) = 3

9. Defensive recommendations:

- Block port 1433 traffic at the firewall and router.
- Verify that all internal Microsoft SQL servers are patched and properly password protected.
- There is a false negative issue with the existing Snort rule. The existing rule does not account for interleaved null bytes found in the client/server communication.

  For example, the following packet generated an alert. This packet was in response to a null password attempt.

```
05/21-07:12:38.242640 my.biz.net.34:1433 -> 63.217.100.34:3235
TCP TTL:114 TOS:0x0 ID:3511 IpLen:20 DgmLen:99 DF
***AP*** Seq: 0x672B7709  Ack: 0x2EB3296E  Win: 0x1FF1  TcpLen: 20
04 01 00 3B 00 00 00 00 AA 27 00 18 48 00 00 01  ...;.....'..H...
0E 1B 00 4C 6F 67 69 6E 20 66 61 69 6C 65 64 20  ...Login failed
66 6F 72 20 75 73 65 72 20 27 73 61 27 2E 00 00  for user 'sa'...
00 00 FD 02 00 00 00 00 00 00 00                 ...........
```

  This packet was a response to a non-null password attempt. Yet, Snort did not generate an alert.

```
05/21-06:32:50.900766 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:41354 IpLen:20 DgmLen:126 DF
***AP*** Seq: 0x658F46CC  Ack: 0x98F6EDA3  Win: 0x2166  TcpLen: 20
04 01 00 56 00 00 00 00 AA 42 00 18 48 00 00 01  ...V.....B..H...
0E 1B 00 4C 00 6F 00 67 00 69 00 6E 00 20 00 66  ...L.o.g.i.n. .f
00 61 00 69 00 6C 00 65 00 64 00 20 00 66 00 6F  .a.i.l.e.d. .f.o
00 72 00 20 00 75 00 73 00 65 00 72 00 20 00 27  .r. .u.s.e.r. .'
00 73 00 61 00 27 00 2E 00 00 00 00 00 FD 02 00  .s.a.'..........
00 00 00 00 00 00                                ......
```

  Clearly this is a failed login attempt that Snort did not catch. A new Snort rule should be deployed to eliminate the false negative issue with existing Snort rule. The following rule added to the local.rules file eliminates the false negative condition.

```
alert tcp $SQL_SERVERS 1433 -> $EXTERNAL_NET any (msg:"MS-SQL sa login failed";
content:"|4C006F00670069006E00200066006100690066C006500640020006600 6F007200200075007300650072
0200027007300610027|"; flags:A+; classtype:unsuccessful-user; sid:688; rev:3;)
```

  This rule alerts, in conjunction with the existing rule, on all four failed logins.

10. Multiple choice test question:

Packet trace:

```
05/21-06:32:50.900766 my.biz.net.34:1433 -> 63.217.100.34:3230
TCP TTL:114 TOS:0x0 ID:41354 IpLen:20 DgmLen:126 DF
***AP*** Seq: 0x658F46CC  Ack: 0x98F6EDA3  Win: 0x2166  TcpLen: 20
04 01 00 56 00 00 00 00 AA 42 00 18 48 00 00 01  ...V.....B..H...
0E 1B 00 4C 00 6F 00 67 00 69 00 6E 00 20 00 66  ...L.o.g.i.n. .f
```

```
00 61 00 69 00 6C 00 65 00 64 00 20 00 66 00 6F  .a.i.l.e.d. .f.o
00 72 00 20 00 75 00 73 00 65 00 72 00 20 00 27  .r. .u.s.e.r. .'
00 73 00 61 00 27 00 2E 00 00 00 00 00 FD 02 00  .s.a.'..........
00 00 00 00 00 00                                ......
```

Snort rule:

```
alert tcp $SQL_SERVERS 1433 -> $EXTERNAL_NET any (msg:"MS-SQL sa login failed"; content:
"Login failed for user |27|sa|27|"; flags:A+; classtype:unsuccessful-user; sid:688; rev:3;)
```

The packet trace above documents a failed administrator account login attempt to a MS-SQL server. What is the MOST LIKELY condition to occur with Snort operating in IDS mode if the above packet trace is processed by the above Snort rule?

a) Alert will be generated.
b) False negative because null characters in the packet trace prevented a match.
c) False negative because the "Nocase" helper option was not specified in the rule.
d) False negative because insertion tactic blinded the IDS sensor.

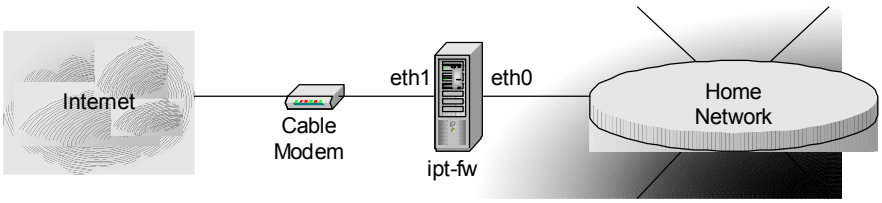
Answer: B. The rule set above failed to account for a condition where client/server communication is interleaved by null character bytes.

Detect 2: PCAnywhere Ping

```
(MAC address info cut from trace)

Apr 15 20:18:41 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=65024 PROTO=UDP SPT=1039 DPT=5632 LEN=10

Apr 15 20:19:49 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=3074 PROTO=UDP SPT=1040 DPT=5632 LEN=10

Apr 15 20:20:41 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=15363 PROTO=UDP SPT=1042 DPT=5632 LEN=10

Apr 15 20:21:40 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=37643 PROTO=UDP SPT=1044 DPT=5632 LEN=10

Apr 15 20:25:02 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=6938 PROTO=UDP SPT=1046 DPT=5632 LEN=10

Apr 15 20:25:18 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=8475 PROTO=UDP SPT=1047 DPT=5632 LEN=10

Apr 15 20:25:30 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=8732 PROTO=UDP SPT=1048 DPT=5632 LEN=10

Apr 15 20:26:44 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=10269 PROTO=UDP SPT=1049 DPT=5632 LEN=10

Apr 15 20:27:23 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=11038 PROTO=UDP SPT=1050 DPT=5632 LEN=10

Apr 15 20:27:48 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=11039 PROTO=UDP SPT=1051 DPT=5632 LEN=10

Apr 15 20:28:08 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=11296 PROTO=UDP SPT=1052 DPT=5632 LEN=10

Apr 15 20:33:01 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=52992 PROTO=UDP SPT=1028 DPT=5632 LEN=10

Apr 15 20:33:43 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=52737 PROTO=UDP SPT=1029 DPT=5632 LEN=10

Apr 15 20:35:06 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=62210 PROTO=UDP SPT=1031 DPT=5632 LEN=10

Apr 15 20:36:36 ipt-fw kernel: netfilter: INPUT(drop) IN=eth1 OUT=  SRC=MY.NET.175.101
DST=MY.NET.175.169 LEN=30 TOS=0x00 PREC=0x00 TTL=123 ID=40202 PROTO=UDP SPT=1033 DPT=5632 LEN=10
.
. <data pruned>
.
```

1. Source of Trace:

These logs were taken from a Mandrake Linux system running kernel 2.4.8-26mdk configured as an iptables firewall (ipt-fw) to protect my home network. The external interface eth1 connects to a cable modem and has a public address and performs network address translation for client systems behind the firewall. The internal interface is eth0 and has a private address.



2. Detect was generated by:

The system is configured as a stateful firewall using iptables v1.2.2. The iptables rule set is very restrictive and is configured to log via syslog all dropped (ie. blocked) packets destined for the firewall on the external interface (eth1). This is achieved with the following command:

```
iptables -A INPUT -i eth1 -j LOG --log-level warning --log-prefix "netfilter: INPUT(drop) "
```

Log format: source: http://logi.cc/linux/netfilter-log-format.php3

<date> <time> <server name> <logging process>: netfilter: <chain>(drop) IN=<inbound interface> OUT=<outbound interface> SRC=<source addr> DST=<destination addr> LEN=<IP packet length> TOS=<type of service> PREC=<precedence> TTL=<time to live> ID=<packet id> PROTO=<protocol> SPT=<source port> DPT=<destination port> LEN=<UDP total length>

date: Date the log entry was generated.
time: Time the log entry was generated.
server name: Name of the system generating the entry.
logging process: Linux process that generated the entry. In the case of this detect, it will always be "kernel:" because iptables is a part of the Linux kernel process.
netfilter: <chain>(drop): This is logging information that I chose to include as a part of the iptables configuration in order to determine which chain (input, forward, output) dropped the packet. This is very important when analyzing log entries.
inbound interface: Interface the packet entered the system. This is empty for packets generated by localhost.
outbound interface: Interface the packet exited the system. This is empty for packets received by localhost.
source addr: Source address identified by the IP header.
destination addr: Destination address identified by the IP header.
IP packet length: Length of IP packet in bytes.
type of service: Type of Service "Type" field.
precedence: Type of Service "Precedence" field.
time to live: Remaining time to live for the packet.
packet id: IP datagram ID number.
protocol: Protocol name or number.
source port: For TCP/UDP packets, source port.
destination port: For TCP/UDP packets, destination port.
UDP total length: Length of UDP packet in bytes.

3. Probability the source address was spoofed:

Although this is a UDP packet and easily spoofed, it is unlikely that it is spoofed. Because of the nature of the attack, the potential attacker would be interested in the response.

In addition, the odds of a spoofed source address are further reduced by configuring the Linux kernel not to accept packets with source routing. This is achieved by the following command in the firewall script:

```
echo 0 > /proc/sys/net/ipv4/conf/eth1/accept_source_route
```

4. Description of attack:

PCAnywhere is remote control software manufactured by Symantec Corporation. PCAnywhere is software designed to allow users to have full remote control over a host. PCAnywhere requires that

ports 5631 and 5632 be open in both directions for TCP and UDP. More detail regarding PCAnywhere can be found at http://service4.symantec.com/SUPPORT/pca.nsf/docid/199792482420.

This detect could be indicative of a slow, brute force attempt to craft UDP traffic on destination port 5632 from varying source ports in an attempt to determine if the PCAnywhere server is in operation. This crafting could be accomplished using the hping2 program. In consideration of this theory, it is important to note that no other evidence of packet crafting was found in the detect. All packet lengths, type of service, id's, etc. were found to be within specification.

Discovery of a PCAnywhere server would likely be followed up with subsequent attempts to connect to the PCAnywhere server with the objective of taking control of the targeted system. Because of weak default security settings for the PCAnywhere server, fresh installs are favorite targets for attackers.

This activity, however, is very likely being generated by a neighboring host on the cable modem network. Because the host MY.NET.175.101 is on the same class C subnet as my firewall MY.NET.175.169, it is very likely a naïve user using PCAnywhere to search the "network" for agents. This hypothesis is supported by the PCAnywhere Ping document found on the Internet Security Systems web site at http://www.iss.net/security_center/advice/Intrusions/2001507/default.htm. The incrementing source ports is consisistent with subsequent connect attempts in this scenario.

5. Attack mechanism:

The apparent goal of the detected activity is reconnaissance. The goal is to identify an operating PCAnywhere server by scanning for open UDP port 5632 with incrementing source ports. If this is truly malicious traffic, the incrementing source port number is likely an attempt by the attacker to subvert static packet filters. However, as noted above, because this firewall is attached to a cable modem on a common class C network, this is very likely being generated by a neighboring host naively generating this traffic.

6. Correlations

No host-specific correlations were found. However, there is substantial information regarding the PCAnywhere "feature" that generates these packets noted in the above detect.

http://service4.symantec.com/SUPPORT/pca.nsf/pfdocs/2001020515021912
http://www.mynetwatchman.com/kb/security/ports/6/5632.htm
http://www.august.net/just_about_anywhere.html

All of this information leads me to the final conclusion that this is indeed a naïve PCAnywhere user broadcasting these "pings".

7. Evidence of active targeting

Because the routable address space assigned to this firewall is confined to a single external IP address, sufficient visibility needed to assess if this activity is targeted is not available. PCAnywhere is commonly targeted and subjected to broad sweeps of Internet address space for unprotected servers. However, most broad scans for the service consists of a single connect attempt to a single host. If the connect is not successful, the attacker moves onto the next host in the scanning queue.

However, there is overwhelming evidence for this detect that it is simply a "wrong number". As noted previously, it is very likely that PCAnywhere has been loaded on a neighboring computer system on my Class C and is broadcasting this traffic to the entire /24 subnet.

8. Severity

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

Criticality: 5
The targeted system is a firewall. If the firewall is compromised, the internal network is susceptible to attack.

Lethality: 1
The firewall is running on a Linux platform without PCAnywhere loaded. It is not vulnerable to this attack.

System Countermeasures: 5
The host is running an IPtables firewall that restricts connection attempts directed to and through it. Port 5632 connections are not allowed to the firewall. The system is up-to-date with latest security patches.

Network Countermeasures: 5
The host is running an IPtables firewall that restricts connection attempts directed to and through it. Port 5632 connections are not allowed through the firewall to the internal network. The system is up-to-date with latest security patches.

(5 + 1) – (5 + 5) = -4

9. Defensive recommendation

The best defense against PCAnywhere compromise is not to run it at all. PCAnywhere is not running anywhere on this network. The firewall rule set is already very restrictive as to egress and ingress traffic. Appropriate countermeasures are already in place.

The source address originates from the same class C network as my cable modem. Being familiar with the acceptable use policies for my ISP, I know this type of scanning activity is not permitted. One action that can be taken is to notify the abuse contact for the address block. If this host were compromised and being used for such unauthorized activity, this step could prevent me and other future targets from nuisance probes from this host.

10. Multiple choice test question

A firewall's logs are showing repeatedly denied UDP connection attempts within a small span of time from the same source address with incrementing source ports over a broad range with a constant destination port set. This activity is MOST LIKELY indicative of what type of activity?

a. SYN flood attack.
b. Distributed denial of service attack.
c. Use of slow, interleaved scanning for available services on a given host with the intent of evading intrusion detection systems.
d. Attempt to determine if a specific service is running on a given port with the intent of subverting packet filters.

Answer: D. If the attacker believes a service is running on a host that is protected solely by a static packet filter, he/she may increment source ports in an attempt to discover if the packet filter is allowing communication through on a given port. This information can be used for a follow-up attack.

Detect 3: SOCKS Probes

```
.
. <data pruned>
.
May 25 12:55:58 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:1861 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 00:41:46 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:3343 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 00:41:46 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:3343 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 01:20:05 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2717 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 01:28:54 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2545 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 01:48:56 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2091 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 01:48:56 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2091 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 02:08:16 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:1718 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 02:45:27 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:1297 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 03:14:32 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:4827 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 03:24:32 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:4662 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 04:05:34 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:3604 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 04:25:06 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:3477 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 04:46:15 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:4214 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 05:04:34 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2304 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 05:47:39 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2314 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 06:13:34 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:4262 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 06:45:12 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:2286 to xxx.yyy.zzz.92 on
unserved port 1080
May 25 07:23:37 fw.my.net unix: securityalert: tcp if=hme0 from 209.134.35.59:4215 to xxx.yyy.zzz.92 on
unserved port 1080
.
. <data pruned>
.
```

1. Source of Trace

This detect was taken from a firewall on the network perimeter at my workplace. It protects the internal network and a DMZ. The DMZ address space (applicable to this detect) is xxx.yyy.zzz.0/24. It is interesting to note that there is no host at xxx.yyy.zzz.92.

2. Detect was generated by:

These log entries were taken from a Gauntlet 5.5 firewall running on Solaris 2.6 operating system.

The log format is as follows:

```
Mmm dd hh:mm:ss [hostname] unix: securityalert: [protocol] if=[interface] from [srcaddr:srcport] to
[destaddr] on unserved port [destport]
```

3. Probability the source address was spoofed:

The probability is very low because the source is attempting to connect to the SOCKS proxy service which runs over TCP. To negotiate a successful connection, the attacker must receive the response packets. Further investigative work established a honey pot style session with the source host and captured requests. This makes the possibility of spoofed activity almost zero.

4. Description of attack:

The detect documents a persistent number of TCP connection attempts from 209.134.35.59 to host xxx.yyy.zzz.92 in the DMZ address space on port 1080. This activity continued intermittently over a period of several days.

TCP port 1080 is known for SOCKS proxy activity along with trojan communications for SubSeven v2.2 and Winhole[6]. Intrigued by the persistent nature of this traffic, a homemade, honey pot style SOCKS server was configured on the firewall and configured to accept connections and solicit transaction attempts. This confirmed that SOCKS4 was the protocol in use and proved to be very revealing as to *why* these connection attempts were occurring.

But before we get to the *why*, we let's review the *who*, *what*, *when*, and *where* of the activity.

We have already eliminated the likelihood of address spoofing occurring with this attack in the previous section. So, we believe 209.134.35.59 is very likely the originating host. This host reverse DNS resolves to the name 35-59.worldsite.net. The worldsite.net domain belongs to the following registrant:

```
Registrant:
 Webcountry, Inc
 18653 Ventura Blvd
 Suite 303
 Tarzana, CA 90356
 US

Technical Contact:
    Webcountry, Inc, Webcountry, Inc  steve@webcountry.net
    18653 Ventura Blvd
    Suite 303br

    Tarzana, CA, 90356
    US
    818-728-1128
```

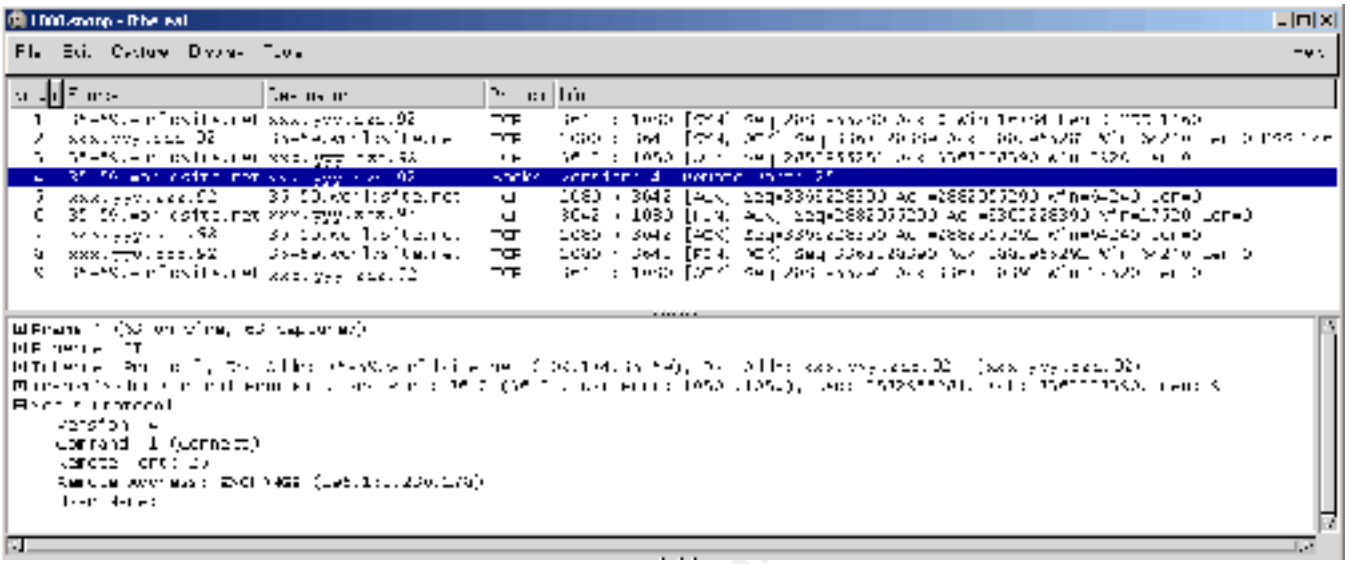
This company appears to be an ISP according to the webcountry.net web site. This suggests the perpetrator of this activity is possibly a customer using a dynamic address. Reverse resolution of the 209.134.35.59 to the 35-59.worldsite.net name is typical of ISP reverse naming conventions. The logs were searched for any other activity from the 209.134.0.0 network. Only this source address logged activity. The activity persisted from 2002-05-24 16:52:31 until 2002-05-27 10:27:37.

The host was attempting to connect to an open SOCKS proxy. According to an online SOCKS FAQ, "SOCKS is a networking proxy mechanism that enables hosts in one side of SOCKS server to gain full access to hosts in the other side of the SOCKS server without requiring direct IP reachability."[7] This capability can be beneficial to a malicious person for a variety of reasons including achieving anonymity for the purpose of conducting unauthorized activity. We will see a bit further down in the analysis that this is indeed likely the case.

As previously stated, this persistence was intriguing enough to warrant some creative analysis. First, *snoop*, a Sun Solaris tcpdump-style tool, was setup to capture traffic from the source address. The aforementioned "fake" SOCKS server was setup to listen on port 1080 and bound to an alias of xxx.yyy.zzz.92 on the firewall and the ruleset was modified to allow this host to talk to it.

[6] "Neohapsis Ports List". URL: http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html (May 26, 2002).
[7] Kuris, Ron, et. al. "SOCKS-FAQ". URL: http://www.unix.org.ua/unix/socks-faq.html (May 29, 2002).

The binary *snoop* captures were analyzed using *Ethereal*, a free network protocol analyzer. This performed the decoding of the SOCKS protocol. The following screenshot shows the decoding of the conversation (destination IP graphically obfuscated).



This specific conversation reveals that once a three-way handshake is negotiated, the remote host attempts to execute a proxied connection to 195.152.230.198 via port 25. TCP port 25 is well-known as simple mail transport protocol (SMTP) traffic. Numerous other conversations were reviewed and port 25 connections were attempted on many different destination IP addresses.

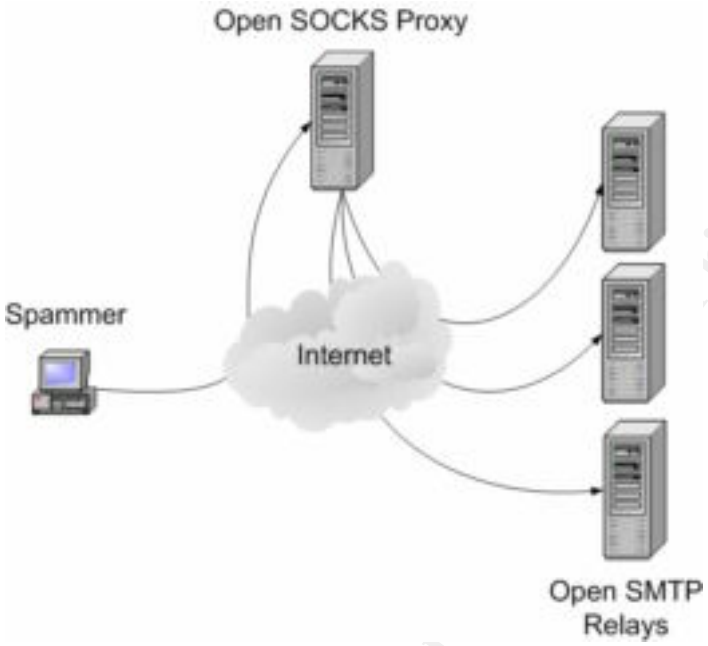
This reveals to us the *why*! There are two hypotheses that come to mind when considering the motive for this activity:

- Host at 209.134.35.59 is attempting to conceil his/her identity in order to anonymously execute exploit attempts against remote SMTP servers.
- Host at 209.134.35.59 is a spammer attempting to use open SOCKS proxies to inject unsolicited email (spam) into the Internet and in doing so, concealing his/her identity so that the activity cannot be tracked back to his/her ISP account. Most ISPs have strict rules against the use of accounts for transmitting unsolicited email traffic and being caught would almost certainly result in loss of service.

Anti-spam sites are reporting the activity described in the second hypothesis. According to Spamcop.net, "spammers have increasingly been hijacking SOCKS proxy servers to send their spam out. Because SOCKS works at a lower level, there is no trace of the true origin of the spam in the header, and it will appear to originate from the proxy IP."[8]

[8] "SOCKS Proxy Servers." SpamCop FAQ. URL: http://spamcop.net/fom-serve/cache/278.html (May 29, 2002).

5. Attack mechanism:



A successful attack involves negotiating a three-way handshake with an open SOCKS proxy server. The SOCKS connection is then used to proxy SMTP sessions to third party mail servers where unsolicited email is sent. This creates a scenario where it appears the originator of the spam is the open SOCKS proxy instead of the real spammer.

6. Correlations:

Other firewall administrators via the DShield service have reported this same host over the same time period.

DShield.org IP Info Report

IP Address: 209.134.35.59

HostName: 35-59.worldsite.net

DShield Profile:

Country:	
Contact E-mail:	
Total Records against IP:	379
Number of targets:	1
Date Range:	2002-05-22 to 2002-05-27

Ports Attacked (up to 10):

Port	Attacks
1080	103

As previously noted, the use of SOCKS proxies for the purpose of anonymous spamming has been confirmed by antispam sites. According to Spamcop.net, "spammers have increasingly been hijacking

SOCKS proxy servers to send their spam out. Because SOCKS works at a lower level, there is no trace of the true origin of the spam in the header, and it will appear to originate from the proxy IP."[9]

7. Evidence of active targeted:

Finding an open SOCKS proxy would typically be accomplished through a broad scanning exercise. Upon completion of a scan, the identified servers would subsequently be used for malicious intentions. The IP address xxx.yyy.zzz.92 does not and has never operated a SOCKS proxy. On the basis that the host 209.134.35.59 repeated attempted to connect to the host on our network for several days without success, I attribute the activity to a "wrong number" episode. Somehow, xxx.yyy.zzz.92 made it into this attacker's database of proxies in error.

8. Severity:

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

Criticality: 1
The targeted system xxx.yyy.zzz.92 does not even exist. It simply lies in the DMZ address range for the firewall.

Lethality: 1
If successful, this attack is a nuisance more than anything. It provides anonymity for a spammer.

System Countermeasures: 5
The best defense for any host is not to exist at all. ☺

Network Countermeasures: 5
The DMZ is behind a Gauntlet firewall that is not configured to allow any port 1080 traffic.

(1 + 1) – (5 + 5) = -8

9. Defensive recommendations:

Collect sufficient evidence against this host in order to notify the ISP of the abuse being perpetrated by this host on their network. Always ensure any proxy server setup in the future does not allow unauthenticated or non-ACL'ed access.

10. Multiple choice test question:

An unauthorized email distributor (a.k.a. spammer) targets SOCKS proxies with what PRIMARY purpose in mind?

a. Compromise the operating system of the SOCKS proxy host.
b. Achieve anonymity for transmitting spam.
c. Use the SOCKS proxy to attack other hosts.
d. To use it as an open relay for spam distribution.

Answer: B.

[9] "SOCKS Proxy Servers." SpamCop FAQ. URL: http://spamcop.net/fom-serve/cache/278.html (May 29, 2002).

Assignment 3: "Analyze This" Scenario

1. Executive Summary and Overview

Five days of log data accumulated by one or more Snort network intrusion detection sensor(s) located at GIAC University was analyzed in this scenario. The log data covered the period of time between March 27th, 2002 and March 31st, 2002. Log files are archived at http://www.incidents.org/logs/ and contained in the following files:

Alert Logs	Scan Logs	Out-of-Spec Logs
alert.020327.gz	scans.020327.gz	oos_Mar.27.2002.gz
alert.020328.gz	scans.020328.gz	oos_Mar.28.2002.gz
alert.020329.gz	scans.020329.gz	oos_Mar.29.2002.gz
alert.020330.gz	scans.020330.gz	oos_Mar.30.2002.gz
alert.020331.gz	scans.020331.gz	oos_Mar.31.2002.gz

This document constitutes a security audit based on the extensive analysis of these log files in conjunction with correlative analysis with outside sources. Findings along with defensive recommendations are documented.

Major findings that require immediate action are as follows:

- Trojan activity across multiple hosts including MY.NET.70.177. Based on analysis, this host appears to be a network management station. If this host is compromised, it may have unauthorized control of many of the University's critical hosts including: MY.NET.5.29, MY.NET.5.44, MY.NET.5.45,MY.NET.5.50, MY.NET.5.55, MY.NET.5.77, MY.NET.5.83, MY.NET.5.88, MY.NET.70.177, MY.NET.191.20. This and other Trojan activity is detailed in Section 6: Suspicious Internal Host activity.
- Perimeter protection needs to be implemented (ie. via firewalls and/or router access control lists) that restricts the flow of unauthorized services and information to the outside world. Currently, a significant quantity of Windows networking traffic is flowing to the outside world. Because of insecure aspects of Windows networking, steps should be taken at the perimeter to control external access. Significant MSN-Instant Messenger, GNUTella, Kazaa, and eDonkey filesharing are occurring. This can lead to Wide Area Networking bandwidth consumption issues along with classic entry points for Trojans, viruses, or other malicious entities on University computing resources.
- A significant amount of SNMP (Simple Network Management Protocol) activity is occurring on the network using the "public" community string. Community strings are effectively passwords for SNMP activity. Because "public" is a well known default setting for community strings, this allows unauthorized entities to execute SNMP activity on hosts. The University should consider upgrading all hosts requiring management via SNMP to SNMP v3.0 which offers a much higher level of security.

Other recommendations can be found within this audit.

2. Host Profile

In an effort to provide a context for analyzing the data, the log files were used to build a host profile table based in inferences found in common, repetitive traffic patters to and from specific hosts on the network. A *host-profiler.sh* shell script was written to analyze the *alert*, *scans*, and *oos* data sets in an attempt to identify

most frequently occurring log entries associated with services on particular hosts. This mined the data by analyzing top destination hosts with the following destination well-known ports:

Port	Service
20,21	ftp
22	ssh
23	telnet
25	smtp
53	dns
67	bootp
80	www
110	pop3

Port	Service
111	rpc
119	nntp
123	ntp
143	imap
220	imap3
443	ssl
514	syslog
515	printer

The results of the mining produced data that I inspected for relatively high levels of activity associated with log data directed towards the specified host. Further detail into this mining process is addressed in "Section 7: Analysis Process" of this audit.

Because this method of analysis uses data triggered by activity deemed abnormal by the Snort engine, it cannot be considered a complete picture since other "normal" traffic occurred within protocols that went undetected. However, the data gathered is provides necessary insight into the nature of hosts identified as sources and targets by the Snort engine. This insight assisted in the intrusion analysis procedures conducted in this audit.

The following table identifies the findings of the profiling exercise. Other hosts were added after the fact based on investigation.

Host	Service
MY.NET.1.3	dns
MY.NET.1.4	dns
MY.NET.1.5	dns
MY.NET.1.7	syslog
MY.NET.1.63	printer
MY.NET.11.4	ftp, http
MY.NET.5.4	http
MY.NET.5.74	bootp
MY.NET.5.29	http, https
MY.NET.5.31	rpc
MY.NET.5.44	http
MY.NET.5.79	http, rpc
MY.NET.5.95	http
MY.NET.5.96	http
MY.NET.6.7	http, imap
MY.NET.6.39	pop3, imap

Host	Service
MY.NET.6.59	pop3, imap
MY.NET.60.8	telnet
MY.NET.60.11	telnet
MY.NET.60.14	http
MY.NET.60.16	telnet
MY.NET.60.38	telnet
MY.NET.70.177	Net Mgr
MY.NET.88.163	ftp
MY.NET.88.187	http
MY.NET.99.202	ssh
MY.NET.100.165	http
MY.NET.150.46	ftp
MY.NET.150.59	http
MY.NET.150.83	http
MY.NET.150.142	http
MY.NET.150.143	http

Host	Service
MY.NET.150.195	http
MY.NET.150.197	http
MY.NET.150.198	printer
MY.NET.150.231	http
MY.NET.151.79	8080
MY.NET.152.19	8080
MY.NET.153.191	ftp
MY.NET.253.51	smtp
MY.NET.253.52	smtp
MY.NET.253.53	smtp
MY.NET.253.112	http, https
MY.NET.253.114	http
MY.NET.253.115	http
MY.NET.253.119	https
MY.NET.253.125	http

3. Alert Summary

All alerts from the *alert* data set were analyzed by shell scripts to identify the most frequently occurring event signatures. In addition, frequency analysis was performed to identify the source and destination address scopes of the attacks. This frequency analysis helped identify potential threats that are worthy of deeper analysis. It is also beneficial in identifying IDS signatures that need tuning as evidenced by a high count of potential false positives.

The following table summarizes the quantitative analysis of the *alert* log files sorted by the number occurrence for each unique alert. Qualitative analysis will be performed later in this document.

Signature	Number of Detects	Unique Src Addr	Unique Dest Addr
spp_http_decode: IIS Unicode attack detected	57675	100	595
SMB Name Wildcard	47283	153	139
connect to 515 from inside	44979	73	3
SNMP public access	37562	23	150
ICMP Echo Request L3retriever Ping	23126	86	1
INFO MSN IM Chat data	7654	82	82
ICMP Echo Request Nmap or HPING2	3742	61	1
INFO Outbound GNUTella Connect request	2933	4	2180
High port 65535 udp - possible Red Worm – traffic	2242	76	118
INFO Inbound GNUTella Connect request	2190	1804	4
Watchlist 000220 IL-ISDNNET-990517	2134	30	12
ICMP Fragment Reassembly Time Exceeded	1735	27	1
MISC Large UDP Packet	1727	13	7
WEB-IIS view source via translate header	891	39	3
WEB-MISC Attempt to execute cmd	883	16	32
ICMP Router Selection	874	98	1
NMAP TCP ping!	865	23	297
Port 55850 tcp - Possible myserver activity - ref. 010313-1	861	9	9
FTP DoS ftpd globbing	548	8	3
Null scan!	382	69	12
Watchlist 000222 NET-NCFC	348	3	3
SCAN Proxy attempt	219	29	15
INFO FTP anonymous FTP	210	7	23
Possible trojan server activity	208	19	19
WEB-FRONTPAGE _vti_rpc access	188	73	2
WEB-IIS _vti_inf access	184	70	2
INFO napster login	140	1	25
WEB-CGI scriptalias access	131	6	1
suspicious host traffic	119	10	2
INFO Possible IRC Access	93	11	17
ICMP Destination Unreachable (Communication Administratively Prohibited)	90	1	1
INFO - Possible Squid Scan	87	16	14
INFO Napster Client Data	79	3	55
Queso fingerprint	60	6	5
Incomplete Packet Fragments Discarded	55	6	6
FTP CWD / - possible warez site	54	1	12
WEB-MISC 403 Forbidden	53	3	15
High port 65535 tcp - possible Red Worm - traffic	51	7	6
spp_http_decode: CGI Null Byte attack detected	46	4	6
SCAN Synscan Portscan ID 19104	42	42	10
ICMP Echo Request Windows	42	16	1
Russia Dynamo - SANS Flash 28-jul-00	24	3	3
EXPLOIT x86 setuid 0	24	23	8
EXPLOIT x86 NOOP	22	15	15
ICMP traceroute	19	9	1
WEB-MISC compaq nsight directory traversal	17	4	4

EXPLOIT x86 setgid 0	12	11	5
ICMP Echo Request BSDtype	10	3	1
Attempted Sun RPC high port access	10	4	7
Tiny Fragments - Possible Hostile Activity	9	1	1
TCP SRC and DST outside network	7	3	3
MISC traceroute	7	3	2
Back Orifice	7	4	5
WEB-MISC http directory traversal	6	1	1
WEB-IIS Unauthorized IP Access Attempt	5	2	2
EXPLOIT NTPDX buffer overflow	5	3	3
SCAN FIN	4	2	2
ICMP Destination Unreachable (Protocol Unreachable)	4	2	1
BACKDOOR NetMetro Incoming Traffic	4	1	1
x86 NOOP - unicode BUFFER OVERFLOW ATTACK	3	1	1
WEB-MISC ICQ Webfront HTTP DOS	3	2	1
INFO Inbound GNUTella Connect accept	3	3	3
RPC tcp traffic contains bin_sh	2	2	1
Port 55850 udp - Possible myserver activity - ref. 010313-1	2	2	2
ICMP Echo Request CyberKit 2.2 Windows	2	1	1
BACKDOOR NetMetro File List	2	1	1
X11 outgoing	1	1	1
WEB-MISC webdav search access	1	1	1
TFTP - Internal UDP connection to external tftp server	1	1	1
TFTP - External UDP connection to internal tftp server	1	1	1
SYN-FIN scan!	1	1	1
SMB CD...	1	1	1
ICMP Echo Request Sun Solaris	1	1	1
EXPLOIT x86 stealth noop	1	1	1
EXPLOIT x86 NOPS	1	1	1

4. Alert Summary Analysis

Analysis Criteria

The alert summary list identified in "Section 3: Alert Summary" detailed a summary overview of all alerts found in the *alert* data set sorted by frequency of occurrence. A total of 243,007 alerts are within the five days of alert logs. A detailed analysis follows for top ten most frequently occurring alerts. Analyzing the top 10 covers 229,386 or over 95% of the alert data generated over the five days.

The analysis will include the following analysis:

- Detect name and overview
- Triggering signature (if available)
- Top 10 sources generating alerts
- Top 10 targets of alerts
- Log Excerpt of a Specific Detect
- Analysis of a Specific Detect
- Correlations with outside information sources (if any)
- Defensive Recommendations

Detect #1: spp_http_decode: IIS Unicode attack detected

a. Detect Overview BugTraq ID: 1806 CVE-2000-0884

This detect was generated by the Snort http_decode preprocessor which is enabled in the snort.conf. A Unicode attack is a broad class of exploits on Microsoft IIS web servers that deal with input validation errors. Specially crafted input can be used to execute commands on vulnerable web servers. A broad discussion of the Unicode vulnerability can be found at http://rr.sans.org/threats/unicode.php.

The http_decode preprocessor is known to generate many false positives as evidenced by message board conversations between Snort administrators on the Internet[1] and analysis of this detect was performed with that in mind.

b. Top 10 Sources for Attack

Occurrences	Address
19354	MY.NET.153.197
3492	MY.NET.153.115
3305	MY.NET.152.19
2552	MY.NET.153.171
2547	MY.NET.153.124
2042	MY.NET.153.162
1746	MY.NET.153.137
1454	MY.NET.153.106
1424	MY.NET.153.190
1165	MY.NET.153.181

Clearly, the host MY.NET.153.197 generated an inordinate amount of these alerts. In fract, MY.NET.153.197 is identified as the "top talker" on the entire network as it generated 20730 log entries in the *alert* data set over the period.

In addition, it was noted that 9 out of the top 10 source addresses were sourced from the MY.NET.153.0/24 subnet.

c. Top 10 Destinations for Attack

Occurrences	Address	DNS Name / Site	Netblock Country
12636	211.115.212.150	cnts.godpeople.com/	Korea
2646	61.78.53.102	www.nartbox.com	Korea
2410	211.115.213.202	Not found	Korea
1884	211.115.213.207	www.iloveschool.co.kr	Korea
1690	211.115.212.175	Not found	Korea
1482	202.30.244.15	community0.shinbiro.com	Korea
1351	211.32.117.26	www6.hanmail.net	Korea
1317	211.32.117.206	www26.hanmail.net	Korea
1157	211.115.212.173	Not found	Korea
1045	211.32.117.27	www7.hanmail.net	Korea

[1] Berkers, John. "IIS Unicode attack detected". URL: http://www.geocrawler.com/mail/msg.php3?msg_id=6390557&list=4890 (May 1, 2002).

d. Detect Log Excerpt

```
<snip>

03/27-11:04:56.093954  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4052 -> 211.115.212.150:80

03/27-11:04:56.093954  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4052 -> 211.115.212.150:80

03/27-11:04:56.093954  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4052 -> 211.115.212.150:80

03/27-11:04:56.096097  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4053 -> 211.115.212.150:80

03/27-11:04:56.096097  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4053 -> 211.115.212.150:80

03/27-11:04:56.096097  [**] spp_http_decode: IIS Unicode attack detected [**]
MY.NET.153.197:4053 -> 211.115.212.150:80

</snip>
```

e. Detect Analysis Summary

The first observation is that no internal hosts were in the top 10 target list. In addition, performing whois lookups on the owners of each of these address blocks shows that every address belongs to a Korean organization. This fact proves extremely beneficial in analyzing the large quantities of "the IIS Unicode detected" alert. Because foreign language character sets are typically implemented with Unicode[2], we can likely attribute the high quantities of these alerts to foreign language character sets.

f. Defensive Recommendations

The top talkers lists for this signature does not indicate any internal web servers under massive attack. Even so, it is recommended that, as a best practice, the University ensure all Microsoft IIS web servers are operating with the latest patches installed. This will provide the most protection

The analysis sites false positives as the major reason for the high count for this alert. The latest version of Snort provides an updated preprocessor known as "unidecode". According to the snort.conf file included with Snort v1.8.6 (Build 105) the new preprocessor "works much the same as http_decode, but does a better job of categorizing and identifying Unicode attacks" and is "recommended as a potential replacement for http_decode.[3]"

Detect #2: SMB Name Wildcard

a. Detect Overview

This alert can be indicative of an information gathering probe by the source address against Microsoft Windows platforms or Linux Samba servers. This activity can reveal information about usernames and share names. This alert is commonly triggered by normal Server Message Block (SMB) protocol communication within a local area network. However, when this alert is associated

[2] "What is Unicode?". May 21, 2002. URL: http://www.unicode.org/unicode/standard/WhatIsUnicode.html (May 23, 2002).

[3] Roesch, Martin. snort.conf, Snort v1.77.2.9, March 18, 2002.

with external traffic, it can be indicative of reconnaissance and/or impending attack which can include file theft or placement. This activity may also be associated with the "network.vbs" worm[4].

A possible Snort signature that could have triggered these alerts is as follows:

```
alert udp any any -> $HOME_NET 137 (msg:"SMB Name Wildcard";
content:"CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|0000|";)
```

This signature will alert on any UDP packet sent to an internal address on port 137 with a SMB wildcard string "CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" and subsequent binary 0000.

b. Top Talkers

Top 10 Sources for Attack

Occurrences	Source Address
14293	MY.NET.11.6
7468	MY.NET.11.7
881	MY.NET.11.5
824	MY.NET.152.161
561	MY.NET.152.160
558	MY.NET.152.21
552	MY.NET.152.19
544	MY.NET.5.96
533	MY.NET.152.251
533	MY.NET.152.163

Because internal-to-internal traffic is likely associated with benign Windows/Samba networking traffic, an analysis was performed on the top external sources for this attack. Interestingly, out of 47283 alerts, only the external IP address 24.188.117.164 triggered the alert. This qualified it for further analysis. The first step is to gather as much information about who owns this host as possible.

```
IP: 24.188.117.164      Hostname: ool-18bc75a4.dyn.optonline.net

Cablevision Systems Corp (NETBLK-OOL-1NANTNY7-0110)
   111 New South Road
   Hicksville, NY 11801
   US
   Netname: OOL-1NANTNY7-0110
   Netblock: 24.188.117.128 - 24.188.117.191
   Coordinator:
      OOL Hostmaster  (OH4-ORG-ARIN)  hostmaster@CV.NET
      (516)393-3281
   Record last updated on 03-Nov-2001.
   Database last updated on  16-May-2002 19:59:02 EDT.
```

The hostname and whois record information would imply that this source IP address belongs to cable modem user on the Cablevision Systems Corp network.

[4] Alexander, Bryce. "Intrusion Detection FAQ Port 137 Scan". May 10, 2000. URL: http://www.sans.org/newlook/resources/IDFAQ/port_137.htm (May 1, 2002).

Top 10 Destinations for Attack

Occurrences	Address
14205	MY.NET.11.6
7404	MY.NET.11.7
875	MY.NET.11.5
826	MY.NET.152.161
566	MY.NET.152.21
558	MY.NET.152.160
557	MY.NET.152.19
545	MY.NET.5.96
542	MY.NET.152.163
534	MY.NET.152.251

c. Detect Log Excerpt

Because 24.188.117.164 was the only address generating external "SMB Name Wildcard" alerts, further analysis on this IP address was warranted. Each data set (*alerts, scans, oos*) was searched for the 24.188.117.164 address. No port scans or out-of-spec traffic was detected; however, there were several entries in the *alerts* file.

From alerts data set:

```
03/28-20:24:34.561650  [**] ICMP Echo Request L3retriever Ping [**]
24.188.117.164 -> MY.NET.5.44

03/28-20:24:36.563992  [**] SMB Name Wildcard [**] 24.188.117.164:1025 ->
MY.NET.5.44:137

03/28-20:24:36.569195  [**] ICMP Echo Request L3retriever Ping [**]
24.188.117.164 -> MY.NET.5.44

03/28-20:24:38.084710  [**] SMB Name Wildcard [**] 24.188.117.164:1025 ->
MY.NET.5.44:137

03/28-20:24:38.585474  [**] ICMP Echo Request L3retriever Ping [**]
24.188.117.164 -> MY.NET.5.44

03/28-20:24:39.579497  [**] SMB Name Wildcard [**] 24.188.117.164:1025 ->
MY.NET.5.44:137

03/28-20:24:40.591470  [**] SMB Name Wildcard [**] 24.188.117.164:137 ->
MY.NET.5.44:137

03/28-20:24:42.071370  [**] SMB Name Wildcard [**] 24.188.117.164:137 ->
MY.NET.5.44:137

03/28-20:24:43.586160  [**] SMB Name Wildcard [**] 24.188.117.164:137 ->
MY.NET.5.44:137

03/28-20:24:44.031638  [**] suspicious host traffic [**] 24.188.117.164:4520
-> MY.NET.5.44:135

<repeats snipped>

03/28-20:25:06.080747  [**] suspicious host traffic [**] 24.188.117.164:3571
-> MY.NET.5.44:9127

<repeats snipped>
```

This log excerpt is indicative of interleaved "L3retriever Pings" and "SMB Name Wildcard" alerts followed by "suspicious host traffic". A total of eight similar sets of log entries were generated between these address over a period of time ranging from 03/28-20:24:34 to 03/28-20:48:29. This excerpt appears to modeling a repeatable pattern of activity being generated by the 24.188.117.164 host. The pattern includes approximately 10 seconds of "L3retriever Pings" and "SMB Name Wildcard" activity followed up by approximately 30 seconds of "suspicious host traffic" being detected.

The "L3retriever Ping" signature is designed to alert on someone using the L3 "Retriever 1.5" security scanner. However, this signature, because it matches on `content: "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"`, generates false positives on "large" (ie. greater than 100 bytes) pings from Win2k/XP hosts because a similar pattern is used to pad the datagram. Whitehats.com also reports that "this type of ICMP ping seems to be also generated by (plain) Win2K host talking to Win2K domain controllers."[5]

The "suspicious host traffic" destined for port 135 could be indicative of communication to Microsoft applications including Windows NT 4.0 services such as DHCP Administration, DNS Administration, and WINS Manager along with Microsoft Exchange 5.0 client/server communications, administrator, and RPC communications.

Similar activity was also directed from this host towards MY.NET.5.45 after the MY.NET.5.44 activity had ceased with the exception of no "suspicious host traffic" alerts.

g. Detect Analysis Summary

It is the opinion of the analyst that the vast majority of the alerts associated with "SMB Name Wildcard" are false positives because of the clear presence of a Microsoft Windows Networking infrastructure. Traffic from internal hosts to other internal hosts on UDP 137 is commonly used for NetBIOS name service communication and is most likely benign. However, in analyzing the *alerts* data set, the top external talker list identified communications between 24.188.117.164 (ool-18bc75a4.dyn.optonline.net) and MY.NET.5.44 and MY.NET.5.45. This analysis identified potential communications from outside hosts to internal Microsoft applications such as Microsoft Exchange server. Because Microsoft networking traffic should be confined to the local area network, the ping activity followed by SMB wildcard activity and subsequent suspicious host activity indicates that unauthorized activity may have occurred associated with an outside source.

To be ensure MY.NET.5.44 was not compromised by this activity, the *alerts* data set was reviewed for other indications of Trojan or backdoor activity. In doing so, 13 "Possible Trojan server activity" alerts were associated with this ip address but were dismissed as false positives related to coincidental high tcp source port 27374 used for normal communications.

h. Defensive Recommendations

Immediate steps should be taken to restrict the flow of Windows networking traffic to the outside world. Best practices call for denying all network transmissions through network perimeters except that which is expressly permitted. However, if the University security policy does not allow this, access control lists and/or firewall rule sets should be established to deny all inbound and outbound traffic on ports tcp/udp ports 137, 138, and 139. Since this analysis identified potential application

[5] "IDS311/SCAN_PING-SCANNER-L3RETRIEVER". URL: http://www.whitehats.com/info/IDS311 (May 1, 2002).

communication to a Microsoft Exchange Server on tcp port 135, this service should be restricted from external access as well.

Detect #3: connect to 515 from inside

a. Detect Overview

This alert is indicative of attempts to print to a print server over the network using the lpr print spooler service. This service uses well-known TCP port 515 for communications.

A possible Snort signature that could have triggered these alerts is as follows:

```
alert TCP $HOME_NET any -> $EXTERNAL 515 (msg:" Connect to 515 from inside";
flags: S;)
```

b. Top Talkers

Top 10 Sources

Occurrences	Address
5994	MY.NET.153.203
4772	MY.NET.153.119
4351	MY.NET.153.118
2867	MY.NET.153.125
2560	MY.NET.153.109
2317	MY.NET.153.123
1466	MY.NET.153.121
1243	MY.NET.153.141
1152	MY.NET.153.137
1067	MY.NET.153.144

Top 10 Destinations

Occurrences	Address
44298	MY.NET.150.198
677	MY.NET.1.63
4	MY.NET.150.114

c. Detect Log Excerpt

```
03/27-08:19:26.070542  [**] connect to 515 from inside [**]
MY.NET.153.195:2422 -> MY.NET.150.198:515

03/27-08:19:26.071965  [**] connect to 515 from inside [**]
MY.NET.153.195:2422 -> MY.NET.150.198:515
```

d. Detect Analysis Summary

Analysis of the *alerts*, *scans,* and *oos* data sets produced no threatening findings. There were no *oos* entries. Analysis of the *scans* file shows only 2 entries for that all detected scans were sourced and destined to internal hosts with no persistent or broad scanning.

However, since the alerts were all associated with MY.NET.0.0/24 -> MY.NET.0.0/24 traffic, the activity was benign in nature.

e. Defensive Recommendations

Vulnerabilities do exist for the lpr service that can lead to root compromise. One such vulnerability is the LPRng buffer overflow detailed at http://www.whitehats.com/info/IDS457 and identified by CVE-2000-0917. Patches are generally available for this and any other known exploit for the lpr service. Because networking print services are in widespread use on the campus network, it is the recommendation of this analyst that the University adopt policies and procedures that ensure servers are running the latest patched versions of all software providing network services.

Detect #4: SNMP public access

a. Detect Overview

SNMP, or Simple Network Management Protocol, is a protocol used to manage and monitor devices with SNMP support. Community strings used as a crude authentication method (because they are transmitted in clear text and easily sniffed). "Public access" refers to the use of the word "public" as the community string. Many devices are configured with "public" as the default community string. Attackers can use this to gather information about networks where default community strings have been left in place. This alert is design to notify the intrusion analyst of the presence of this type of traffic.

A possible Snort signature that could have triggered these alerts is as follows:

```
alert udp any any - $HOME_NET 161 (msg: "SNMP public access";
content:"public";)
```

This alert will trigger when any udp traffic is detected destined to hosts on the internal network on udp 161 where the word "public" is in the datagram.

b. Top Talkers

Top 10 Sources for Attack

Occurrences	Address	Unique Src Ports	Unique Dest Addr
19460	MY.NET.70.177	2	33
4872	MY.NET.150.198	640	103
2441	MY.NET.153.220	5	1
1293	MY.NET.88.203	2	1
1284	MY.NET.88.159	3	1
1250	MY.NET.88.145	2	1
1239	MY.NET.88.207	1	1
1179	MY.NET.153.191	4	1
1169	MY.NET.88.181	2	1
717	MY.NET.88.136	1	1

Host MY.NET.70.177 demonstrates significantly more frequency of *alerts* log entries with respect to this signature. I decided to check the source ports used in the SNMP traffic using this command:

```
grep "SNMP public access" alerts.delimited | grep "ip_addr" | cut -d\; -f 4 |
sort | uniq -c | wc -l
```

The results show for MY.NET.70.177

Occurrences	Source Port
13363	1080
6097	1072

I ran the same command against MY.NET.150.198. There were interesting results. There were over 640 unique source ports. This led me to add an addition column to the Top 10 Sources for Attack table above to compare unique source ports for each source address. I also decided to add an additional column to show unique destinations for each address using a derivative of the above command (changing cut to extract field 5 instead of 4). This proved interesting as well.

It appears as though MY.NET.70.177 is acting as a network management station of the hosts on the MY.NET.5.0/24 subnet since the destination addresses of the alerts were confined to this network. This is substantiated by other previously completed GIAC Security Audits for the University[6].

In checking the unique destination addresses, it appears that six of the top ten source addresses are all talking to the same destination address: MY.NET.150.195. These six addresses are all in the MY.NET.88.0/24 subnet. Based on the table below, the 6952 alerts these six hosts are associated with accounted for over 96% of the alerts associated with the MY.NET.150.195 destination address.

Top 10 Destinations for Attack

Occurrences	Address
7225	MY.NET.150.195
3790	MY.NET.5.248
2959	MY.NET.152.109
2652	MY.NET.5.137
2638	MY.NET.5.143
1958	MY.NET.5.31
1949	MY.NET.5.97
1933	MY.NET.5.127
1760	MY.NET.150.147
1601	MY.NET.151.114

Intrigue and curiosity are sometimes the intrusion analyst's best friend so I attempted to correlate the activity identified in the *scans* data set with that of the MY.NET.150.195 address. I used this command:

```
grep "\-> MY.NET.150.195" scans | grep -v ":161 "
```

```
<data pruned>
Mar 27 05:25:57 211.94.66.9:4655 -> MY.NET.150.195:21 SYN ******S*
Mar 27 10:20:25 MY.NET.88.159:1071 -> MY.NET.150.195:9100 SYN ******S*
Mar 27 11:14:47 MY.NET.88.159:1217 -> MY.NET.150.195:9100 SYN ******S*
Mar 27 11:52:09 MY.NET.88.203:1521 -> MY.NET.150.195:9100 SYN ******S*
Mar 28 14:05:57 64.172.129.129:2964 -> MY.NET.150.195:21 SYN ******S*
Mar 28 20:43:54 64.172.129.129:2309 -> MY.NET.150.195:21 SYN ******S*
Mar 28 23:48:28 217.226.144.143:4286 -> MY.NET.150.195:80 SYN ******S*
Mar 29 04:40:25 129.93.47.215:3551 -> MY.NET.150.195:21 SYN ******S*
Mar 29 10:51:40 MY.NET.88.159:1580 -> MY.NET.150.195:9100 SYN ******S*
Mar 29 10:55:07 MY.NET.88.159:1621 -> MY.NET.150.195:9100 SYN ******S*
```

[6] Chapman, Todd. "SANS GCIA Practical Assignment". p43-44. URL: http://www.giac.org/practical/Todd_Chapman_GCIA.doc

```
Mar 29 13:05:38 MY.NET.88.203:2368 -> MY.NET.150.195:9100 SYN ******S*
Mar 29 15:44:35 172.147.15.96:3520 -> MY.NET.150.195:80 SYN ******S*
Mar 29 21:25:18 62.178.38.69:1865 -> MY.NET.150.195:80 SYN ******S*
Mar 29 21:26:00 62.178.38.69:2761 -> MY.NET.150.195:80 SYN ******S*
Mar 30 07:22:56 64.23.0.112:1465 -> MY.NET.150.195:21 SYN ******S*
Mar 30 23:30:29 64.45.60.38:1906 -> MY.NET.150.195:21 SYN ******S*
```

Connects to TCP port 9100, 161, and 80 are indicative of the presence of an HP JetDirect print server[7]. Port 9100 is used for printing, port 161 is used for checking the status of print jobs (hence the SNMP alerts), and 80 is used for a web gui configuration tool. These findings are validated by the many-to-one relationship for MY.NET.150.195 as identified by Top Talker analysis above. MY.NET.150.195 is a departmental HP JetDirect-based print server.

Documentation of all the ports used by the HP Jet Direct engine can be found at http://www.hp.com/cposupport/networking/support_doc/bpj01014.html.

With this newfound knowledge, it leaves MY.NET.150.198 as having statistically interesting traffic patterns. Again, we turn to the *scans* data set and it reveals that MY.NET.150.198 conducted a broad scan of the network for SNMP each night of the five days in the logs.

```
Mar 27 00:56:33 MY.NET.150.198:1576 -> MY.NET.71.24:161 UDP
Mar 27 00:56:38 MY.NET.150.198:1578 -> MY.NET.138.228:161 UDP
Mar 27 00:56:39 MY.NET.150.198:1579 -> MY.NET.86.8:161 UDP
.

.     <data pruned>
.
Mar 28 00:22:06 MY.NET.150.198:1691 -> MY.NET.163.56:161 UDP
Mar 28 00:22:08 MY.NET.150.198:1696 -> MY.NET.106.202:161 UDP
Mar 28 00:22:09 MY.NET.150.198:1702 -> MY.NET.53.228:161 UDP
.
.     <data pruned>
.
Mar 29 00:42:44 MY.NET.150.198:1879 -> MY.NET.163.56:161 UDP
Mar 29 00:42:45 MY.NET.150.198:1883 -> MY.NET.106.202:161 UDP
Mar 29 00:42:46 MY.NET.150.198:1889 -> MY.NET.53.228:161 UDP
.
.     <data pruned>
.
Mar 30 01:08:49 MY.NET.150.198:1779 -> MY.NET.163.56:161 UDP
Mar 30 01:08:50 MY.NET.150.198:1784 -> MY.NET.106.202:161 UDP
Mar 30 01:08:51 MY.NET.150.198:1790 -> MY.NET.53.228:161 UDP
.
.     <data pruned>
.
Mar 31 00:35:27 MY.NET.150.198:1509 -> MY.NET.163.56:161 UDP
Mar 31 00:35:28 MY.NET.150.198:1513 -> MY.NET.106.202:161 UDP
Mar 31 00:35:30 MY.NET.150.198:1519 -> MY.NET.53.228:161 UDP
<data pruned>
```

[7] "HP Jetdirect Print Servers - HP Jetdirect Port Numbers for TCP and/or UDP Connections". URL: http://www.hp.com/cposupport/networking/support_doc/bpj01014.html (May 22, 2002).

Each night between 00:00:00 and 01:30:00, MY.NET.150.198 generated between 100 and 114 scan log entries each night on port 161. As we know from our Top Sources table, there are 103 unique destinations for these scans. More analysis was completed with the following set of commands.

```
egrep -e "MY\.NET\.150\.198:[0-9]* \->" scans | grep "Mar 27" | cut -d" " -f
6 | sort | uniq > tmp27

egrep -e "MY\.NET\.150\.198:[0-9]* \->" scans | grep "Mar 28" | cut -d" " -f
6 | sort | uniq > tmp28

egrep -e "MY\.NET\.150\.198:[0-9]* \->" scans | grep "Mar 29" | cut -d" " -f
6 | sort | uniq > tmp29

egrep -e "MY\.NET\.150\.198:[0-9]* \->" scans | grep "Mar 30" | cut -d" " -f
6 | sort | uniq > tmp30

egrep -e "MY\.NET\.150\.198:[0-9]* \->" scans | grep "Mar 31" | cut -d" " -f
6 | sort | uniq > tmp31

#check number of entries in each tmp file
wc -l tmp*

#compare differences
diff tmp27 tmp28
diff tmp28 tmp29
diff tmp29 tmp30
diff tmp30 tmp31
```

The output from these commands showed that there were between 94 and 99 unique addresses scanned each night and there was very little variance in the set of addresses checked. All of this information suggests that there is a process running on MY.NET.150.198 that runs each night to check a set of hosts for its status using SNMP with a "public" community string.

c. Detect Analysis Summary
It has been determined from the above analysis of the top sources of the "SNMP public access" alerts that none of the top sources are generating malicious traffic.

MY.NET.70.177 was identified as a likely network management station for hosts on the MY.NET.5.0/24 network. MY.NET.150.198 was identified as likely running a script to poll the status of a set of hosts each night. The remaining sources were identified as having a many-to-one relationship with printers that use HP JetDirect for printing over the network.

d. Defensive Recommendations
The analysis above for MY.NET.70.177 and MY.NET.150.198 should be confirmed to verify no malicious or unauthorized activity is occurring from these addresses using SNMP. It is also recommended that the community strings for all SNMP managed devices, regardless if it is SNMP read only access, be changed to a significantly more obscure community string. In addition, where feasible, it is strongly recommended that SNMP v3 be adopted as its primary goal is to offer a more secure version of the SNMP protocol[8].

Detect #5: ICMP Echo Request L3retriever Ping

[8] "FAQs – SNMPv3 related". http://www.adventnet.com/products/snmp/help/faqs/faq_snmpv3.html (May 22, 2002).

a. Detect Overview
This alert could be indicative of a host scanning a network using the L3 "Retriever" security scanning tool.

A possible Snort signature that could have triggered these alerts is as follows:

```
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS311/scan_ping-scanner-
L3retriever"; itype: 8; icode: 0; content:
"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; depth: 32;)
```

The "L3retriever Ping" signature is designed to alert on someone using the L3 "Retriever 1.5" security scanner. However, this signature, because it matches on `content: "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"`, generates false positives on "large" (ie. greater than 100 bytes) pings from Win2k/XP hosts because a similar pattern is used to pad the datagram. Whitehats.com also reports that "this type of ICMP ping seems to be also generated by (plain) Win2K host talking to Win2K domain controllers[9]."

b. Top Talkers

Top 10 Sources for Attack

Occurrences	Address
834	MY.NET.152.161
570	MY.NET.152.21
565	MY.NET.152.160
555	MY.NET.152.19
535	MY.NET.152.163
533	MY.NET.152.251
532	MY.NET.152.171
526	MY.NET.152.173
515	MY.NET.152.15
514	MY.NET.152.178

Top 10 Destinations for Attack

Occurrences	Address
14280	MY.NET.11.6
7453	MY.NET.11.7
883	MY.NET.11.5
291	MY.NET.5.4
141	MY.NET.10.49
29	MY.NET.5.44
28	MY.NET.5.35
12	MY.NET.5.45
9	MY.NET.5.96

c. Detect Analysis Summary
Because the University network has a significant deployment of Microsoft Windows networking, these alerts generated are likely false positives related to Windows 2000 hosts talking to Windows 2000 domain controllers. It would be unlikely that all of these hosts would be using the L3 tool to

[9] "IDS311/PING-SCANNER-L3RETRIEVER" URL: http://www.whitehats.com/info/IDS311 (May 22, 2002).

scan the network. According to whitehats.com "these probes should be rare, since the software is usually restricted to limited IP address ranges.[10]"

d. Defensive Recommendations
These alerts are VERY likely to be false positives across the board and no recommended action needs to be taken with respect to the L3 Retriever scanner from an internal perspective. However, it is considered a best practice to limit ICMP traffic ingress and egress as much as possible. This can be easily achieved by router access control lists and firewall rules at the perimeter.

Detect #6: INFO MSN IM Chat data

a. Detect Overview
IM is Internet vernacular for "Instant Messenger", and in its original form allows for individuals to transmit chat messages "instantly" to each other without the use of email. The Microsoft Network offers its own software for instant messaging that now allows voice,and video conversations along with file sharing among other features. More information can be found at http://messenger.msn.com/.

b. Top Talkers

Top 10 Sources for Attack

Occurrences	Address
795	MY.NET.150.165
493	64.4.12.178
457	MY.NET.153.108
399	MY.NET.153.146
357	64.4.12.158
321	64.4.12.190
263	MY.NET.153.113
227	MY.NET.88.151
199	MY.NET.153.177
198	64.4.12.171

Top 10 Destinations for Attack

Occurrences	Address
1077	MY.NET.150.165
478	MY.NET.153.146
415	MY.NET.153.108
345	64.4.12.190
329	64.4.12.158
300	MY.NET.153.113
293	64.4.12.178
288	MY.NET.150.246
264	MY.NET.88.151
204	64.4.12.191

[10] "IDS311/PING-SCANNER-L3RETRIEVER"
URL:http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids311&view=research (May 22,2002).

c. Detect Analysis Summary
This traffic within itself is generally benign in nature and is common among students. However, because of its voice, video, and file transmission capabilities, MSN Messenger can become a prolific consumer of network bandwidth. It also provides a potential entry point for **new** viruses and Trojans into the campus LAN.

There is significant MSN IM traffic occurring on the University network that could be contributing to network performance and virus/Trojan issues.

d. Defensive Recommendations
If possible, restrict the use of MSN IM by blocking inbound and outbound port 1863 with access control lists and/or firewall rules. Maintain antivirus software with current virus patterns on all university computing resources, especially those that must have MSN IM access.

Detect #7: ICMP Echo Request Nmap or HPING2

a. Detect Overview
Nmap is a utility for network mapping and/or security auditing[11]. HPING2 is a tool used to send arbitrary TCP/UDP/ICMP packets to network hosts[12]. Either of these tools can be used by potential attacks in information gathering efforts.

A possible Snort signature that could have triggered these alerts is as follows:

```
alert icmp any any -> any any (msg:"ICMP Echo Request Nmap or
HPING2";itype:8; dsize:0; reference:arachnids,162;)
```

The key distinguishing feature of this type of ICMP echo request is that the data size is zero. In tcpdump, this is recorded as "len 28".

For example, the command "nmap -sP 192.168.1.1" will decode as the following in tcpdump.

```
23:39:51.076414 192.168.1.50 > 192.168.1.1: icmp: echo request (ttl 41, id
54105, len 28)
```

Pings with len=28 is most likely related to nmap as it uses a payload size of zero by default. Standard pings will report with len 60 from Windows platforms or len 84 from Linux systems unless the ping size has been set to another value by command line. Hping2 can generate this signature as well.

Generally speaking, alerts of these types originating from any external host or unauthorized internal host is not a good thing. They are indicative of mapping efforts underway via nmap or hping2 and could be indicative of an impending attack.

b. Top Talkers

[11] What is nmap?". URL: http://www.nmap.org/nmap/index.html#intro (May 22, 2002).

[12] HPING2. URL: http://www.hping.org/ (May 22, 2002).

Top 10 Sources for Attack

Occurrences	Address
311	MY.NET.253.10
84	MY.NET.152.19
75	MY.NET.152.174
75	MY.NET.152.164
74	MY.NET.152.171
74	MY.NET.152.165
73	MY.NET.152.170
71	MY.NET.152.21
71	MY.NET.152.157
70	MY.NET.152.251

Top 10 Destinations for Attack

Occurrences	Address
2119	MY.NET.11.6
1301	MY.NET.11.7
5	207.46.131.30
4	MY.NET.1.3
2	209.53.113.23
2	MY.NET.88.234
2	MY.NET.88.225
2	MY.NET.88.202
2	MY.NET.88.196
2	MY.NET.88.186

c. Detect Log Excerpt

In searching the alerts file for other activity from MY.NET.253.10, the following log data was found using this command:

```
grep -i "Nmap" alerts | grep -v "ICMP Echo Request Nmap or HPING2"
```

Log excerpt:

```
.
.     <data pruned>
.
03/28-15:08:40.026411  [**] NMAP TCP ping! [**] MY.NET.253.10:48277 ->
MY.NET.5.108:6112

03/28-15:08:40.375746  [**] NMAP TCP ping! [**] MY.NET.253.10:48277 ->
MY.NET.5.109:6112
.
.     <data pruned>
.
```

This data confirms that MY.NET.253.10 very likely used the nmap tool to gather information on the internal network. No other MY.NET address was found to have been correlated with a source of a "NMAP TCP ping! alert".

d. Detect Analysis Summary

Only the alerts from MY.NET.253.10 could be correlated against a "NMAP TCP ping!" alert. This correlation makes it extremely likely that this host did use the NMAP tool to map the network. The remaining internal addresses could not be correlated against other log data to confirm the use of NMAP and/or HPING2.

e. Defensive Recommendations
Immediately confront the user who initiated the NMAP activity from MY.NET.253.10. Ensure that the use of network reconnaissance tools is against University acceptable use policies.

There appears to be a significant amount of anomalous ICMP echo request traffic generating this alerts. Rather than dismissing them as false positives related to some accepted type of network traffic, it is recommended that a network sniffer be deployed to capture these types of packets for decoding and analysis so that a definitive answer be provided as to why these alerts are occurring.

Detects #8,10: INFO Inbound/Outbound GNUTella Connect request

a. Detect Overview
These two alerts indicate that a host is attempting to connect to another host on the GNUTella network, a peer-to-peer file sharing network. More information on the GNUTella network can be found at http://www.gnutellanews.com/information/what_is_gnutella.shtml

Possible Snort signatures that could have triggered these alerts are as follows:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Inbound GNUTella Connect
request"; content: "GNUTELLA CONNECT"; nocase; depth: 40;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Outbound GNUTella Connect
request"; content: "GNUTELLA CONNECT"; nocase; depth: 40;)
```

b. Top Talkers

Top 10 Sources for Outbound

Occurrences	Address
2616	MY.NET.88.223
201	MY.NET.152.21
92	MY.NET.88.194
24	MY.NET.150.209

Top 10 Destinations for Inbound

Occurrences	Address
1757	MY.NET.88.223
179	MY.NET.152.21
129	MY.NET.150.209
125	MY.NET.88.194

c. Detect Analysis Summary
This traffic within itself is generally benign in nature and is common among students. However, as with MSN IM, GNUTella traffic can become a prolific consumer of network bandwidth if left unchecked because of its file transmission capabilities. It also provides a potential entry point for **new** viruses and Trojans into the campus LAN.

There is a strong correlation between the top 10 sources for outbound connects with top 10 sources for inbound connections indicating that the activity of the hosts sharing files is fairly symmetrical.

d. Defensive Recommendations
If possible, restrict the use of GNUTella by blocking inbound and outbound connections with access control lists and/or firewall rules. Common TCP ports used are 1214 and 6346. Maintain antivirus software with current virus patterns on all university computing resources, especially those that must have GNUTella access.

Detect #9: High port 65535 udp - possible Red Worm – traffic

a. Detect Overview
This alert is intended to indicate possible activity of the Unix worm known as Red Worm a.k.a. Adore. Red Worm is a self propagating entity that upon infecting a host results in root compromise. When infected, a ping of size 77 to the host will cause a process to be forked to listen for connection on tcp port 65535. Telnetting to this host on port 65535 will allow unauthenticated root access. More information on this worm can be found at http://www.europe.f-secure.com/v-descs/adore.shtml and http://www.sans.org/y2k/adore.htm.

b. Top Talkers

Top 10 Sources for Attack

Occurrences	Address
447	MY.NET.6.48
426	MY.NET.6.49
418	MY.NET.6.52
397	MY.NET.6.50
175	64.124.157.32
62	MY.NET.6.51
53	MY.NET.6.60
53	MY.NET.6.53
23	MY.NET.6.45
17	203.231.232.136

Top 10 Destinations for Attack

Occurrences	Address
186	MY.NET.152.165
175	MY.NET.153.46
140	MY.NET.152.158
84	MY.NET.153.163
78	MY.NET.152.171
77	MY.NET.152.19
59	MY.NET.153.216
54	MY.NET.152.21
42	MY.NET.153.162
42	MY.NET.152.170

The *alerts* and *scans* log files confirm extensive traffic occurring on UDP 65535 on internal hosts.

c. Detect Analysis Summary

The *alerts* and *scans* log files confirm extensive traffic occurring on UDP 65535 on internal hosts. However, the association of UDP 65535 traffic with the Red Worm by the Snort signature rule set is indeterminate. In fact, this rule was not included with the Snort rules in Version 1.8.6 (Build 105).

d. Defensive Recommendations
Extensive traffic on UDP port 65535 is anomalous in that there is no commonly known software available that communicates with this port. It is recommended that all of the hosts on the top talker lists be checked for Trojan investation.

5. Top Talker Analysis

Top Talkers: *alert* Data Tables

Alerts	Source Addr
20730	MY.NET.153.197
19500	MY.NET.70.177
14293	MY.NET.11.6
7468	MY.NET.11.7
7108	MY.NET.153.203
5100	MY.NET.153.119
4872	MY.NET.150.198
4502	MY.NET.152.19
4351	MY.NET.153.118
3726	MY.NET.153.115

Alerts	Destination Addr
44300	MY.NET.150.198
14205	MY.NET.11.6
7404	MY.NET.11.7
7363	MY.NET.150.195
3795	MY.NET.5.248
2959	MY.NET.152.109
2653	MY.NET.5.137
2638	MY.NET.5.143
2344	MY.NET.5.96
1958	MY.NET.5.31

Top Talkers: *alert* Data Analysis

Hosts: MY.NET.153.197 **Threat Level:** **Low**

Alert Summary (w/ host as source address):

Occurrences	Signature
19354	spp_http_decode: IIS Unicode attack detected
518	connect to 515 from inside

a. Host Analysis:
This host would not have made the top talkers list were it not for the "IIS Unicode detected" alerts. A substantial discussion of this alert is found under Section 5: Alert Summary Analysis under Detect 1. In summary, these Unicode alerts are being generated by www access sourced from this address to foreign (namely Korean) web sites where Unicode is used to generate the foreign language character sets. The "connect to 515 from inside" alerts were all destined toward MY.NET.150.198 which as been identified as a print server on the network in Section 3: Host Profile.

b. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.70.177 **Threat Level:** **CRITICAL**

a. Alert Summary (w/ host as source address)

Occurrences	Signature
19460	SNMP public access
24	SMB Name Wildcard
16	Possible trojan server activity

b. Host Analysis:
It appears as though MY.NET.70.177 is acting as a network management station of the hosts on the MY.NET.5.0/24 subnet since the destination addresses of the alerts were confined to this network. This is substantiated by other previously completed GIAC Security Audits for the University[13].

As a network management stations, this server should be considered a critical host. With this in mind, the Trojan server activity alerts must be treated with the highest level of concern. The log entries for this possible Trojan traffic is below.

```
03/31-01:07:44.431198  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-01:07:44.444553  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-01:07:44.444755  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-01:07:44.444886  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-01:07:44.448410  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-01:07:44.448545  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903

03/31-18:55:16.754618  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.754753  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.754900  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.755539  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.780593  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.780960  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.781321  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.782640  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.802006  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.803372  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.813717  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.845513  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903
03/31-18:55:16.845648  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.857060  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.70.177:27374
03/31-18:55:16.857194  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:8903

03/31-18:55:58.275697  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:7938
03/31-18:55:58.275766  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.70.177:27374
03/31-18:55:58.275921  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:7938
03/31-18:55:58.276187  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:7938
03/31-18:55:58.277563  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.70.177:27374
```

[13] Chapman, Todd. "SANS GCIA Practical Assignment". p43-44. URL:http://www.giac.org/practical/Todd_Chapman_GCIA.doc

```
03/31-18:55:58.278615  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:7938
03/31-18:55:58.278684  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.70.177:27374
03/31-18:55:58.278750  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.70.177:27374
03/31-18:55:58.278888  [**] Possible trojan server activity [**] MY.NET.70.177:27374 ->
MY.NET.5.83:7938
```

It appears as though three distinct sessions (based on time elapsed) occurred between MY.NET.70.177 and MY.NET.5.83. SubSeven Trojan activity is associated with destination port 27374 and is indicative of a potential root/administrator rights compromise. While it appears that the above logs indicate a source port of 27374, we cannot be sure without reviewing the Snort rule. The Snort rule could be set to trigger on the return traffic as it is with the following rule:

```
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR subseven 22"; flags: A+;
content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;
reference:url,www.hackfix.org/subseven/; sid:103; classtype:misc-activity; rev:4;)
```

We must assume the worst. Trojan alerts for MY.NET.5.83 were subsequently reviewed for other activity. There were numerous other hosts that appear to be compromised and under the control of MY.NET.5.83

```
03/27-06:09:49.858162  [**] Possible trojan server activity [**] MY.NET.5.44:27374 ->
MY.NET.5.83:9162
03/27-06:09:49.858231  [**] Possible trojan server activity [**] MY.NET.5.83:9162 ->
MY.NET.5.44:27374
.
.
03/28-13:33:07.790586  [**] Possible trojan server activity [**] MY.NET.191.20:27374 ->
MY.NET.5.83:7938
03/28-13:33:07.790656  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.191.20:27374
.
.
03/28-19:12:10.156200  [**] Possible trojan server activity [**] MY.NET.5.29:27374 ->
MY.NET.5.83:7938
03/28-19:12:10.157499  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.5.29:27374
.
.
03/29-00:37:54.858961  [**] Possible trojan server activity [**] MY.NET.5.50:27374 ->
MY.NET.5.83:7938
03/29-00:37:54.859034  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.5.50:27374
.
.
03/31-06:31:56.848866  [**] Possible trojan server activity [**] MY.NET.5.45:27374 ->
MY.NET.5.83:7938
03/31-06:31:56.848936  [**] Possible trojan server activity [**] MY.NET.5.83:7938 ->
MY.NET.5.45:27374
.
.
03/31-10:04:29.968896  [**] Possible trojan server activity [**] MY.NET.5.77:27374 ->
MY.NET.5.83:8903
03/31-10:04:29.969092  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.5.77:27374
.
.
03/31-13:47:55.222608  [**] Possible trojan server activity [**] MY.NET.5.55:27374 ->
MY.NET.5.83:8903
03/31-13:47:55.222687  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.5.55:27374
.
.
03/31-14:26:11.426168  [**] Possible trojan server activity [**] MY.NET.5.77:27374 ->
MY.NET.5.83:8903
```

```
03/31-14:26:11.426234  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.5.77:27374
.
.
03/31-20:24:14.578987  [**] Possible trojan server activity [**] MY.NET.191.20:27374 ->
MY.NET.5.83:8903
03/31-20:24:14.579056  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.191.20:27374
.
.
03/31-20:55:37.343580  [**] Possible trojan server activity [**] MY.NET.5.45:27374 ->
MY.NET.5.83:8903
03/31-20:55:37.343649  [**] Possible trojan server activity [**] MY.NET.5.83:8903 ->
MY.NET.5.45:27374
```

We see that there is activity to the following hosts:

MY.NET.191.20	MY.NET.5.29	MY.NET.5.44	MY.NET.5.45
MY.NET.5.50	MY.NET.5.55	MY.NET.5.77	MY.NET.5.88

Perhaps as interesting, suspected source ports were confined to three distinct numbers: 7938, 8903, 9162. This level of port predictability is not consistent with normal TCP/IP communications and further justifies action.

It appears as though MY.NET.5.83 has several hosts under remote control including a key network management station.

c. Recommendations:
Immediately quarantine hosts MY.NET.70.177 and MY.NET.5.83 from the network until the source of this suspected Trojan traffic can be determined. Investigate hosts MY.NET.191.20, MY.NET.5.29, MY.NET.5.44, MY.NET.5.45, MY.NET.5.50, MY.NET.5.55, MY.NET.5.77, and MY.NET.5.88 for possible infection/compromise as well. Sanitize all suspected hosts. Ensure all University systems have functional antivirus software with virus signatures that are automatically updated at least daily.

SubSeven is a remote control Trojan that allows its commander to remotely capture keystrokes, screen images, etc. If the University determines the SubSeven Trojan was indeed installed, all activity on the above hosts should be considered to have been remotely logged to unauthorized third parties. Any confidential data, such as passwords, passing through the compromised hosts should be considered compromised and appropriate action taken.

Host: MY.NET.11.6 **Threat Level: Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
14293	SMB Name Wildcard

b. Host Analysis:
The sole alert generated for this host as the source address is "SMB Name Wildcard". This is a false positive consistent with normal traffic patterns for a Windows NetBIOS/SMB fileserver.

c. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.11.7 **Threat Level:** **Low**

Alert Summary (w/ host as source address):

Occurrences	Signature
7469	SMB Name Wildcard

a. Host Analysis:
The sole alert generated for this host as the source address is "SMB Name Wildcard". This is a false positive consistent with normal traffic patterns for a Windows NetBIOS/SMB fileserver.

b. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.153.203 **Threat Level:** **Low**

Alert Summary (w/ host as source address):

Occurrences	Signature
5994	connect to 515 from inside
1081	spp_http_decode: IIS Unicode attack detected

a. Host Analysis:
The "connect to 515 from inside" alerts were all destined toward MY.NET.150.198 which as been identified as a print server on the network in Section 3: Host Profile. The "IIS Unicode attack" alerts are most likely false positive. A substantial discussion of this alert is found under Section 5: Alert Summary Analysis under Detect 1. In summary, these Unicode alerts are being generated by www access sourced from this address to foreign (namely Korean) web sites where Unicode is used to generate the foreign language character sets.

b. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.153.119 **Threat Level:** **Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
4773	connect to 515 from inside
328	spp_http_decode: IIS Unicode attack detected

b. Host Analysis:
The "connect to 515 from inside" alerts were all destined toward MY.NET.150.198 which as been identified as a print server on the network in Section 3: Host Profile. The "IIS Unicode attack" alerts are most likely false positive. A substantial discussion of this alert is found under Section 5: Alert Summary Analysis under Detect 1. In summary, these Unicode alerts are being generated by www access sourced from this address to foreign (namely Korean) web sites where Unicode is used to generate the foreign language character sets.

c. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.150.198 **Threat Level:** **Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
4872	SNMP public access

b. Host Analysis:

This host has been identified as a network print server. Section 5: Alert Summary Analysis under Detect 4 has an extensive analysis that confirms this as a host with both print server and network management station characteristics. In summary of that analysis, it seems as though this server, in addition to being a print server, polls a set of approximately 100 hosts each night using SNMP.

c. Recommendations:
Verify this host is authorized to be conducting SNMP activity.

Host: MY.NET.152.19 **Threat Level:** **Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
3305	spp_http_decode: IIS Unicode attack detected
552	SMB Name Wildcard

b. Host Analysis:
The "IIS Unicode attack" alerts are most likely false positive. A substantial discussion of this alert is found under Section 5: Alert Summary Analysis under Detect 1. In summary, these Unicode alerts are being generated by www access sourced from this address to foreign (namely Korean) web sites where Unicode is used to generate the foreign language character sets. The "SMB Name Wildcard" alerts are also likely false positives. These alerts were exclusively related to traffic with MY.NET.11.5, MY.NET.11.6, and MY.NET.11.7. These hosts have repeatedly demonstrated a high count of SMB/NetBIOS related alerts.

c. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.153.118 **Threat Level:** **Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
4351	connect to 515 from inside

b. Host Analysis:
The "connect to 515 from inside" alerts were all destined toward MY.NET.150.198 which as been identified as a print server on the network in Section 3: Host Profile.

c. Recommendations:
Confirm the above services in operation are authorized.

Host: MY.NET.153.115 **Threat Level:** **Low**

a. Alert Summary (w/ host as source address):

Occurrences	Signature
3492	spp_http_decode: IIS Unicode attack detected
234	connect to 515 from inside

b. Host Analysis:
The "IIS Unicode attack" alerts are most likely false positive. A substantial discussion of this alert is found under Section 5: Alert Summary Analysis under Detect 1. In summary, these Unicode alerts are being generated by www access sourced from this address to foreign (namely Korean) web sites where Unicode is used to generate the foreign language character sets. The

"connect to 515 from inside" alerts were all destined toward MY.NET.150.198 which as been identified as a print server on the network in Section 3: Host Profile.

c. Recommendations:
Confirm the above services in operation are authorized.

Top Talkers: *scans* Data Tables

Scans	Source Addr
363399	MY.NET.60.43
334259	MY.NET.11.8
198475	MY.NET.150.143
125524	MY.NET.150.113
27087	MY.NET.6.45
26352	MY.NET.6.50
25242	MY.NET.6.49
24013	MY.NET.6.48
22449	MY.NET.152.21
22096	MY.NET.6.52

Scans	Destination Addr
38681	MY.NET.1.3
28787	MY.NET.11.6
20196	MY.NET.1.4
18234	MY.NET.153.46
16502	MY.NET.152.20
16327	MY.NET.152.12
16065	MY.NET.152.249
16022	MY.NET.152.162
16000	MY.NET.152.16
15992	MY.NET.152.18

Top Talkers: *scans* Data Analysis

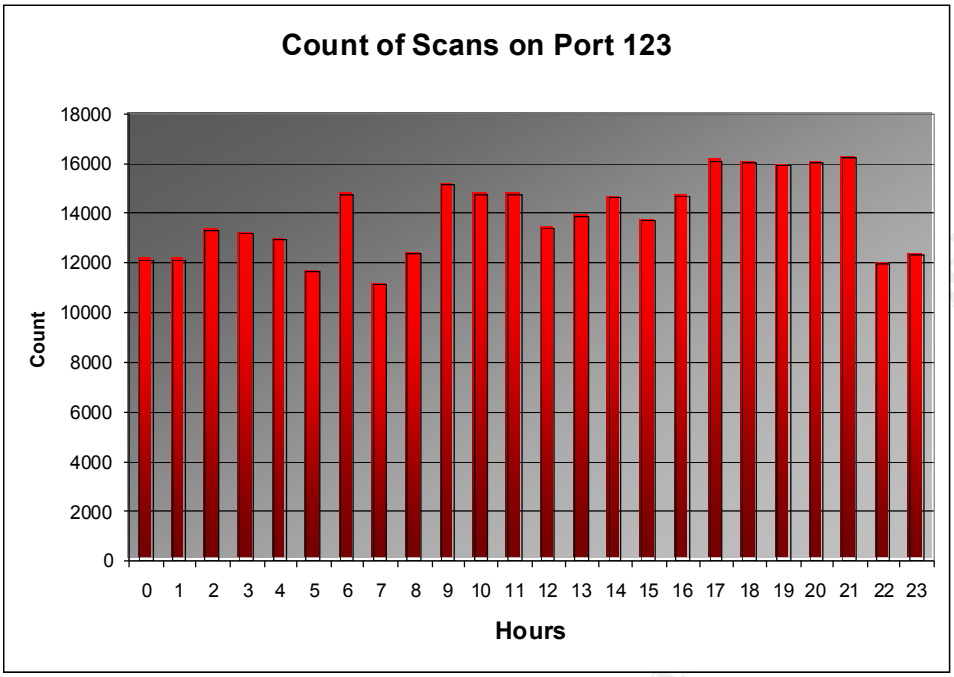
Host: MY.NET.60.43 **Threat Level: Medium**

a. Scans Summary (w/ host as source address):

Occurrences	Port
333222	123/udp
27647	7000/udp
1958	0/udp

b. Host Analysis:
A massive quantity of port scans on UDP port 123 are reported in the *scans* logs. UDP port 123 traffic is typically indicative of network time protocol traffic. Initial inspection seems to indicate a fairly continuous, yet uniform dispersion of traffic throughout the day across five days. To confirm this observation, the following command was used to generate the data for the graph below.

```
egrep –e ":[0-9]*;MY\.NET\.60\.43;123" scans.delimited | cut -d\; -f 1 | cut
--b="7,8" | sort -n | uniq -c
```



The port 123 scans are restricted across a host range MY.NET.153.140-MY.NET.153.216 with only one exception to host MY.NET.88.148.

This information makes a compelling case that this is an ntp (network time protocol) server for this set of hosts. However, other correlations with other similar hosts (see analysis for **MY.NET.6.45** in this same section) show that UDP port 123 traffic frequently occurs in association with AFS traffic.

The *scans* file was reviewed for an explanation regarding the port 7000 traffic on MY.NET.60.43. All ports for the corresponding hosts were confined to 7000/udp and 7001/udp. This is indicative of AFS, a distributed file system[14].

Finally, the UDP port 0 traffic is especially disconcerting. While I have a suspicion it is related to the AFS traffic, I cannot confirm this. My research has revealed no concrete correlation, however, other GIAC audits[15] have reported similar traffic in conjunction with AFS.

c. Recommendations:
Confirm the above services in operation are authorized. Investigate UDP port zero traffic using sniffer or other network analysis tool in order to verify activity is benign.

Host: MY.NET.11.8 **Threat Level:** **Low**

a. Scans Summary (w/ host as source address):

Occurrences	Port
334237	1347/udp
12	1345/udp
10	137/udp

[14] "UDP Ports Used by AFS." URL: http://www.transarc.ibm.com/Support/afs/admin/UDP.html (May 22, 2002).
[15] Larratt, Glenn. "Analysis of the Various Top-Ten Nodes". GCIA Practical v3.0. URL: http://www.giac.org/practical/Glenn_Larratt_GCIA.zip

b. Host Analysis:
UDP port 1347 reports to be used by multimedia conferencing applications[16], however, the traffic patterns derived from log entry times suggest a fairly uniform distribution of traffic over the day. The traffic is largely occurring between this host and many hosts on the MY.NET.152.0 network. This suggests this host is acting as some type of server. This is very likely authorized traffic related to legitimate network services.

c. Recommendations
Confirm the above services in operation are authorized.

Host: MY.NET.150.143, MY.NET.150.113 **Threat Level:** **Low**

a. Scans Summary:
Diverse high port numbers associated with these host as the source address. For MY.NET.150.143, a destination port count shows over 127573 entries for destination UDP port 4665 across 240 unique EXTERNAL hosts.

b. Host Analysis:
Research shows eDonkey2000 as the likely perpetrator of this traffic. eDonkey2000[17] is yet another file sharing application that talks on UDP 4665 and TCP 4661 and 4662. There are connects to these ports confirmed in both the *scans* and *alerts* data files. This traffic within itself is generally benign in nature and is common among students. However, as with GNUTella, this traffic can become a prolific consumer of network bandwidth if left unchecked because of its file transmission capabilities. It also provides a potential entry point for **new** viruses and Trojans into the campus LAN.

c. Recommendations
If possible, restrict the use of eDonkey2000 by blocking inbound and outbound connections to UDP 4665 and TCP 4661,4662 with access control lists and/or firewall rules. Maintain antivirus software with current virus patterns on all university computing resources, especially those that are allowed to use eDonkey2000.

Hosts: MY.NET.6.45, MY.NET.6.50, MY.NET.6.49, MY.NET.6.52 **Threat Level:** **Low**

a. Scans Summary (w/ host as source address):

For Host MY.NET.6.45 (MY.NET.6.50 exhibited similar counts):

Occurrences	Port
20422	7000/udp
3348	123/udp
2359	0/dp

b. Host Analysis:
Scans reported on these hosts meet a similar pattern to that of MY.NET.60.43. Again, we find UDP 7000,123, and 0 occurring. This previously justifies the previous observation that the observed UDP port 0 traffic may be related to the AFS traffic. It is also interesting to note that all of these hosts demonstrate an extraordinarily high number of UDP port 65535 traffic. I

[16] "The Giant Port List". URL: http://keir.net/portlist.html (May 22, 2002).
[17] "eDonkey FAQ" URL: http://www.edonkey2000.com/faq.html#port (May 22, 2002).

believe this also somehow to be related to AFS. The communications appear to be largely confined to MY.NET.152.0 and MY.NET.153.0.

c. Recommendations
Confirm the services in operation are authorized. Investigate UDP port 0 and 65535 traffic using sniffer or other network analysis tool in order to verify if activity is indeed correlated to AFS.

Host: MY.NET.152.21 **Threat Level: Low**

a. Scans Summary (w/ host as source address):
The majority of the *scans* log entries for this host are for TCP port 6346. This is GNUTella traffic. Corresponding log entries from the *alerts* data set confirm this traffic.

b. Host Analysis:
This traffic within itself is generally benign in nature and is common among students. However, as with MSN IM, GNUTella traffic can become a prolific consumer of network bandwidth if left unchecked because of its file transmission capabilities. It also provides a potential entry point for **new** viruses and Trojans into the campus LAN.

c. Recommendations
If possible, restrict the use of GNUTella by blocking inbound and outbound connections with access control lists and/or firewall rules. A common tcp port used is 1214. Maintain antivirus software with current virus patterns on all university computing resources, especially those that must have GNUTella access.

Top Talkers: *oos* Data Tables

Oos	Source Addr
29	80.133.124.114
4	213.169.245.41
2	128.97.84.53
1	80.144.189.160
1	61.216.83.124
1	217.82.123.75
1	213.132.137.149
1	212.242.58.14
1	140.110.30.59
1	0.192.5.106

Oos	Destination Addr
30	MY.NET.150.113
5	MY.NET.152.21
2	MY.NET.153.210
2	MY.NET.150.220
1	MY.NET.153.196
1	MY.NET.153.191
1	MY.NET.150.226

Top Talkers: *oos* Data Analysis

OOS log entries document out-of-spec packets. These packets have invalid flag combinations that are not allowed under normal RFC specifications for TCP/IP. However, there are no standards for response to irregular packets and various operating systems respond differently to invalid flag combinations. The deliberate crafting of these types of packets is used in fingerprinting. Potential attackers use applications such as *nmap* or *queso* to generate stimulus traffic towards hosts of interest. These same applications understand the subtleties in response from varying platforms and provide this information to the attacker[18].

[18] Fyodor. "Remote OS detection via TCP/IP Stack FingerPrinting". April 10, 1999. URL:http://www.insecure.org/nmap/nmap-fingerprinting-article.html

Over the five days analyzed, there were 42 out-of-spec packets detected. Flag combinations are summarized by occurrence below:

Occurrences	Flags Set
34	21S*****
2	2*SF*P*U
1	**SFR*AU
1	2*SF***U
1	2*SFRPAU
1	2*SF*PA*
1	21S*R*A*
1	21SF*P**

Hosts: 80.133.124.114, 80.144.189.160, 217.82.123.75 **Threat Level: Medium**

a. OOS Summary (w/ host as source address):
On March 28th, 80.133.124.114 generated these 29 oos packets over a period of time from 06:44 through 07:31. Source ports incremented without pattern up from 3621 to 4666. Destination port was always 1214. Destination port 1214 corresponds to Kazaa peer-to-peer file sharing activity. Over the exact same period of time, the *alerts* data set reported 29 "Queso fingerprint" alerts were attributed to this address.

Log Excerpt

```
03/28-06:44:33.753660 80.133.124.114:3621 -> MY.NET.150.113:1214
TCP TTL:39 TOS:0x0 ID:56429  DF
21S***** Seq: 0x95B4CF26   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 4939 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/28-06:44:37.146162 80.133.124.114:3687 -> MY.NET.150.113:1214
TCP TTL:39 TOS:0x0 ID:19815  DF
21S***** Seq: 0x96BB59AE   Ack: 0x0   Win: 0x16B0
TCP Options => MSS: 1412 SackOK TS: 5321 0 EOL EOL EOL EOL
```

Similar activity was detected from 80.144.189.160 and 217.82.123.75 but on a reduced scale.

b. Host Analysis:

Reverse IP lookup:

Host	Reverse Lookup
80.133.124.114	p50857C72.dip.t-dialin.net
80.144.189.160	p5090BDA0.dip.t-dialin.net
217.82.123.75	pD9527B4B.dip.t-dialin.net

IP Address Registration Information

```
inetnum:      80.128.0.0 - 80.146.159.255
netname:      DTAG-DIAL16
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP-RIPE
tech-c:       ST5359-RIPE
status:       ASSIGNED PA
remarks:      ****************************************************************
remarks:      * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS,      *
remarks:      * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC.        *
remarks:      ****************************************************************
notify:       auftrag@nic.telekom.de
notify:       dbd@nic.dtag.de
```

```
mnt-by:        DTAG-NIC
changed:       auftrag@nic.telekom.de 20020108
source:        RIPE

route:         80.128.0.0/11
descr:         Deutsche Telekom AG, Internet service provider
origin:        AS3320
mnt-by:        DTAG-RR
changed:       bp@nic.dtag.de 20010807
source:        RIPE

person:        Security Team
address:       Deutsche Telekom AG
address:       Technikniederlassung Schwaebisch Hall
address:       D-89070 Ulm
address:       Germany
phone:         +49 731 100 84055
fax-no:        +49 731 100 84150
e-mail:        abuse@t-ipnet.de
nic-hdl:       ST5359-RIPE
notify:        auftrag@nic.telekom.de
notify:        dbd@nic.dtag.de
mnt-by:        DTAG-NIC
changed:       auftrag@nic.telekom.de 20010321
source:        RIPE
```

A total of 29 out-of-spec packets and 29 "Queso fingerprint" alerts occurring over identical time spans suggests the fingerprinting activity was the stimulus for the oos log entries for this host. Single fingerprinting incidents with associated oos and Queso alerts were detected from 80.144.189.160 and 217.82.123.75. Both of these addresses belong to Deutsche Telekom AG.

c. Recommendations
If supported, configure the University's perimeter firewalls to deny packets with anomalous flags set in the headers.

Continued probing from this address block could indicate impending attack. Report any future probing from this provider's network by emailing abuse@t-ipnet.de or calling the Deutsche Telekom Security Team. Be aware that this host IP address belongs to an Internet Service Provider providing dial-up services, and future probes from the same person are not likely to be sourced from the same address.

Host: 213.169.245.41 **Threat Level: Medium**

a. OOS Summary (w/ host as source address):

Log Excerpt

```
03/27-15:24:28.649944 213.169.245.41:3800 -> MY.NET.152.21:6346
TCP TTL:110 TOS:0x0 ID:408  DF
2*SF*P*U Seq: 0x3F7473   Ack: 0x20736D61   Win: 0x6564
68 65 61 64 20 77 69 74 68 20                    head with

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/27-15:24:29.845479 213.169.245.41:3800 -> MY.NET.152.21:6346
TCP TTL:110 TOS:0x0 ID:5784  DF
2*SF*P*U Seq: 0x3F7473   Ack: 0x20736D61   Win: 0x6564
68 65 61 64 20 77 69 74 68 20                    head with

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/27-15:28:06.137307 213.169.245.41:3800 -> MY.NET.152.21:6346
TCP TTL:110 TOS:0x0 ID:8618  DF
2*SF*PA* Seq: 0x4143B2   Ack: 0xF3660ABC   Win: 0x970A
TCP Options => Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17
Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17
Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17 Opt 17
Opt 17 Opt 17 Opt 17
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/27-15:29:17.651596 213.169.245.41:3800 -> MY.NET.152.21:6346
TCP TTL:110 TOS:0x0 ID:23472  DF
21SF*P** Seq: 0x410005   Ack: 0x2549DEE5   Win: 0x4A9D
34 CB 4A 9D 1C 41 A5 88 BA 8F 76 80 01 06 1D 00  4.J..A....v.....
00 00 00 00 6E 37                                ....n7
```

Alerts related to this host:

```
03/27-15:28:43.272800  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:43.272800  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:57.235603  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
03/27-15:28:57.235603  [**] Null scan! [**] 213.169.245.41:3800 -> MY.NET.152.21:6346
```

Portscans related to this host:

```
Mar 27 15:24:21 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2UA*R** RESERVEDBITS
Mar 27 15:24:24 213.169.245.41:3800 -> MY.NET.152.21:6346 NMAPID *2U*P*SF RESERVEDBITS
Mar 27 15:27:42 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK 1**APRS* RESERVEDBITS
Mar 27 15:28:00 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK *2U*PR*F RESERVEDBITS
Mar 27 15:28:01 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2*AP*SF RESERVEDBITS
Mar 27 15:28:43 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL ********
Mar 27 15:28:57 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL ********
Mar 27 15:29:12 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK 12**P*SF RESERVEDBITS
Mar 27 15:32:15 213.169.245.41:3800 -> MY.NET.152.21:6346 NULL 1******* RESERVEDBITS
Mar 27 15:32:26 213.169.245.41:3800 -> MY.NET.152.21:6346 NOACK *2U*PR*F RESERVEDBITS
Mar 27 15:33:47 213.169.245.41:3800 -> MY.NET.152.21:6346 INVALIDACK *2UA**S* RESERVEDBITS
```

b. Host Analysis:

Reverse IP lookup:

Host	Reverse Lookup
213.169.245.41	245.169.213-41-dial-in-dynamic.ision.nl

IP Address Registration Information

```
inetnum:      213.169.244.0 - 213.169.245.255
netname:      KNOWARE
descr:        Dial-in Pool VPOP-IP
country:      NL
admin-c:      AS3556-RIPE
tech-c:       NR97-RIPE
tech-c:       ED460-RIPE
tech-c:       HO849-RIPE
tech-c:       JT5851-RIPE
status:       ASSIGNED PA
mnt-by:       KNOWARE-MNT
notify:       beheer@ision.nl
changed:      oudheusden@ision.nl 20011210
source:       RIPE
```

The data correlated from the three log files show that there was likely a fingerprinting attempt by this host. It should be noted that MY.NET.152.21 is a frequent user of GNUTella. GNUTella uses TCP port 6346 connections for communications. It is likely that the involvement of host MY.NET.152.21 on this file sharing network prompted the activity since the individual at 213.169.245.41 was aware that TCP 6346 traffic was allowed to this host.

The above activity is all the activity logged for 213.169.245.41 so no subsequent attack was detected where the fingerprinting information was used. However, if future activity from this or any other host in the 213.169.245.0 netblock is detected, it may be the same person engaged in follow up activity.

The above netblock information can be used for contacting the address block owner if future activity is detected from this host.

c. Recommendations
If supported, configure the University's perimeter firewalls to deny packets with anomalous flags set in the headers.

Continued probing from this address block could indicate impending attack. Report any future probing from this provider's network by emailing oudheusden@ision.nl . Be aware that this host IP address belongs to an Internet Service Provider providing dial-up services, and future probes from the same person are not likely to be sourced from the same address. If possible, restrict the use of GNUTella by blocking inbound and outbound connections with access control lists and/or firewall rules. Common TCP ports used are 1214 and 6346.

Host: 128.97.84.53 **Threat Level: Medium**

a. OOS Summary (w/ host as source address):

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/28-14:03:11.738685 128.97.84.53:20 -> MY.NET.153.210:1320
TCP TTL:50 TOS:0x0 ID:42649  DF
21S***** Seq: 0xF15214E3   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110473850 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/28-14:03:11.864168 128.97.84.53:2075 -> MY.NET.153.210:113
TCP TTL:50 TOS:0x0 ID:58086  DF
21S***** Seq: 0xF0B15061   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110473863 0 EOL EOL EOL EOL
```

Alerts related to this host:

```
03/28-14:03:07.181525  [**] Queso fingerprint [**] 128.97.84.53:20 -> MY.NET.153.210:1320
03/28-14:03:07.307006  [**] Queso fingerprint [**] 128.97.84.53:2075 -> MY.NET.153.210:113
```

Portscans related to this host:

```
Mar 28 14:03:07 128.97.84.53:20 -> MY.NET.153.210:1320 SYN 12****S* RESERVEDBITS
Mar 28 14:03:07 128.97.84.53:2075 -> MY.NET.153.210:113 SYN 12****S* RESERVEDBITS
```

b. Host Analysis:
Reverse IP lookup:

Host	Reverse Lookup
128.97.84.53	ndep.seas.ucla.edu

IP Address Registration Information

```
University of California, Los Angeles (NET-UCLANET)
   741 Circle Dr South
   Los Angeles, CA 90095-1363
   US

   Netname: UCLANET
   Netblock: 128.97.0.0 - 128.97.255.255

   Coordinator:
      University of California, Los Angeles  (NO102-ORG-ARIN)  noc@NOC.UCLA.EDU
      +1 310 206 5345
```

The data correlated from the three log files show that there was likely a fingerprinting attempt by this host using the *queso* program.

The above activity is all the activity logged for 128.97.84.53 so no subsequent attack was detected where the fingerprinting information was used. However, if future activity from this or any other host in the 128.97.84.0 netblock is detected, it may be the same person engaged in follow up activity.

c. Recommendations
If supported, configure the University's perimeter firewalls to deny packets with anomalous flags set in the headers. Continued probing from this address block could indicate impending attack. Report any future probing from this provider's network by emailing noc@noc.ucla.edu or calling the University of California, Los Angeles at (310) 206-5345.

Remaining Hosts in *OOS* logs

Possible malicious activity:

61.216.83.124 61-216-83-124.HINET-IP.hinet.net

```
Mar 28 23:09:44 61.216.83.124:64835 -> MY.NET.150.220:4662 FULLXMAS *2UAPRSF RESERVEDBITS
```

Log excerpt from the *scans* data set shows a xmas tree packet (all bits in the flags field set).

140.110.30.59 hpcs009.nchc.gov.tw

```
03/27-21:22:29.672469  [**] Queso fingerprint [**] 140.110.30.59:32862 -> MY.NET.150.220:4662
```

Queso fingerprint alert was generated that corresponded to the *oos* log entry.

Probable errors in transmission:

213.132.137.149 cable-213-132-137-149.upc.chello.be

```
Mar 27 18:09:56 213.132.137.149:3504 -> MY.NET.150.113:1214 INVALIDACK **UA*RSF
```

This is an isolated event related to likely legitimate activity on TCP port 1214 (GNUTella/Kazaa file sharing) and therefore likely a transmission error.

212.242.58.14 port75.ds1-vbr.adsl.cybercity.dk

```
Mar 27 17:05:48 212.242.58.14:12730 -> MY.NET.150.226:80 INVALIDACK 12*A*RS* RESERVEDBITS
```

This is an isolated event related to likely legitimate activity on TCP port 80 (www) and therefore likely a transmission error.

0.192.5.106 <invalid ip address!>

```
Mar 28 15:48:23 0.192.5.106:19169 -> MY.NET.153.191:33376 NOACK *2U***SF RESERVEDBITS
```

Highly suspicious because the IP address is invalid. This is unlikely to be a fingerprinting technique since successful fingerprinting requires a response from the stimulated host unless source routing is used in conjunction with a sniffer. It is possible that this either a transmission error or Snort error since there is only one packet of interest with this source address. Further corroborating this suspicion is the fact that TCP ports 19169 and 33376 are not referenced again in any of the log files.

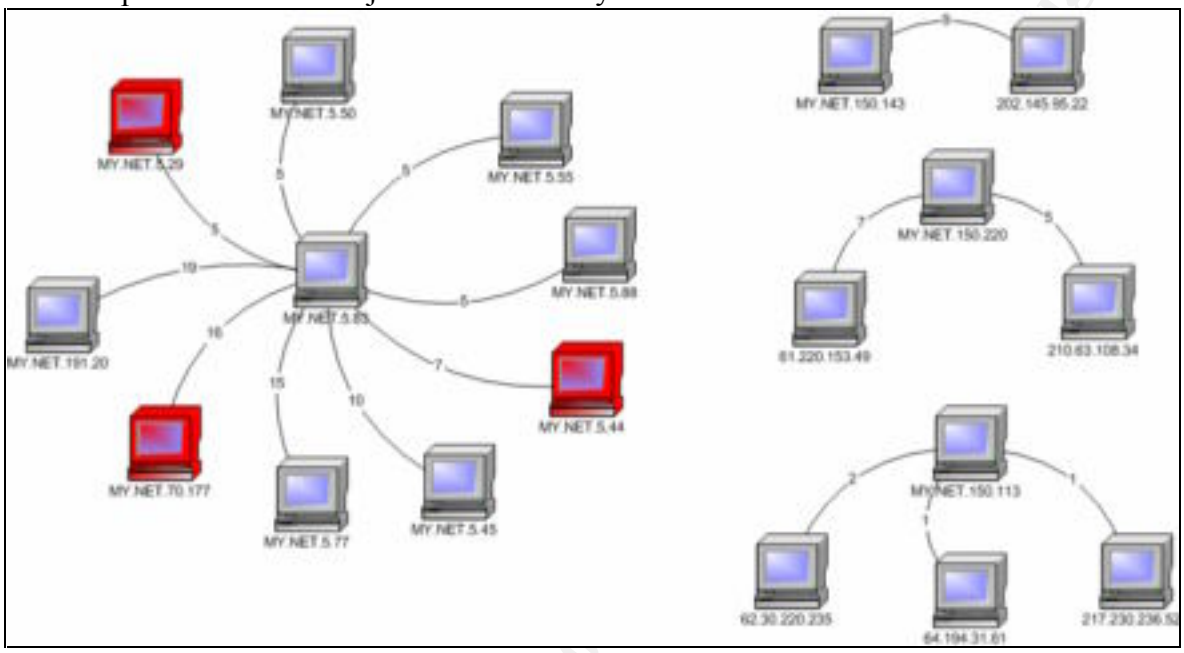
6. Suspicious Internal Host Activity

Hosts: Numerous Possible Compromises Possible trojan server activity

Many hosts exhibited traffic to destination TCP port 27374 which is commonly associated with the SubSeven Trojan. This Trojan offers its controller remote control to the infected host[19]. The "Top Talker Alert Data Analysis" section of this audit addresses a portion of this traffic in depth.

In order to assess the extent of potential Trojan server activity on the network, the following link graph was created to illustrate communication patterns among the 19 unique hosts associated with these alerts. The numeric value on the line indicates the quantity of log entries associated between these two hosts.

Link Graph for Possible Trojan Server Activity



All of the above internal hosts are should IMMEDIATELY be investigated for compromise. Hosts in red were sited as high traffic servers for the internal network. Investigative priority should be placed on these hosts.

There are six external hosts found to be associated with this suspicious Trojan server traffic. This could be the controlling host or a host under the control of a University system. Regardless, all of the owners of these hosts should be contacted pending the results of the University's investigation into the activity. The contact information for these six hosts is as follows:

```
Host: 61.220.153.49

inetnum:     61.220.0.0 - 61.227.255.255
netname:     HINET
descr:       Data Communication Business Group, Chunghwa Telecom Co., Ltd.
descr:       Commerical ISP
descr:       21, Section 1, Hsin-Yi Road, Taipei,
descr:       Taipei 100, Taiwan, R.O.C.
country:     TW
admin-c:     HN27-AP
tech-c:      HN28-AP
mnt-by:      TWNIC-AP
changed:     hostmaster@apnic.net 20010515
source:      APNIC

person:      HINET Network-Adm
address:     CHTD, Chunghwa Telecom Co., Ltd.
address:     Data-Bldg. 6F,  No. 21, Sec. 21, Hsin-Yi Rd.,
```

[19] "About SubSeven." URL: http://www.hackfix.org/subseven/about.shtml (May 25, 2002).

```
address:     Taipei Taiwan 100
country:     TW
phone:       +886 2 2322 3495
phone:       +886 2 2322 3442
phone:       +886 2 2344 3007
fax-no:      +886 2 2344 2513
fax-no:      +886 2 2395 5671
e-mail:      network-adm@hinet.net
nic-hdl:     HN27-AP
remarks:     same as TWNIC nic-handle HN184-TW
mnt-by:      TWNIC-AP
changed:     hostmaster@twnic.net 20000721
source:      APNIC
```

Host: 62.30.220.235

```
inetnum:      62.30.0.0 - 62.31.255.255
netname:      UK-CABLEINET-20000211
descr:        Cable Internet Ltd
descr:        PROVIDER
country:      GB
admin-c:      IH249-RIPE
admin-c:      CS82-RIPE
admin-c:      SL3595-RIPE
admin-c:      DR1307-RIPE
tech-c:       MG645-RIPE
tech-c:       SB5110-RIPE
status:       ALLOCATED PA
mnt-by:       RIPE-NCC-HM-MNT
mnt-lower:    AS5462-MNT
mnt-routes:   AS5462-MNT
changed:      hostmaster@ripe.net 20000211
changed:      hostmaster@ripe.net 20000322
changed:      hostmaster@ripe.net 20010112
changed:      hostmaster@ripe.net 20020220
changed:      hostmaster@ripe.net 20020422
changed:      hostmaster@ripe.net 20020423
source:       RIPE

route:        62.30.0.0/15
descr:        Cable Internet
descr:        UK ISP
origin:       AS5462
notify:       netmail@cableinet.net
mnt-by:       AS5462-MNT
changed:      mike@cableinet.net 20001012
source:       RIPE
```

Host: 64.194.31.61

```
Telocity (NETBLK-TELOCITY-2)
   10355 N. De Anza Blvd
   Cupertino, CA 95014
   US

   Netname: TELOCITY-2
   Netblock: 64.192.0.0 - 64.195.255.255
   Maintainer: TELO

   Coordinator:
      Telocity  (ZT26-ARIN)  ip-admin@telocity.net
      408-863-6600
```

Host: 202.145.95.22

```
inetnum:     202.145.32.0 - 202.145.127.255
netname:     FICNET
descr:       FIC Network Service, INC.
descr:       110 , 8F , No 89 , Sung Jen RD , Taipei
country:     TW
admin-c:     IP11-AP
tech-c:      IP11-AP
mnt-by:      APNIC-HM
mnt-lower:   MAINT-TTN-AP
changed:     jengjr@ttn.com.tw 20010911
```

```
changed:     hostmater@apnic.net 20020227
source:      APNIC

role:        TTN IP-Team
address:     Taiwan Telecommunication Network Services Co. Ltd.
address:     IP Network Dept.
address:     8F , No 89, Songren RD
address:     Shinyi Chiu, Taipei,  Taiwan  110
phone:       +886-2-8788-3728
fax-no:      +886-2-8789-0500
e-mail:      whois@ttn.com.tw
admin-c:     IP11-AP
tech-c:      IP11-AP
nic-hdl:     IP11-AP
remarks:     ### Abuse , Spam , Security ###
remarks:     abuse@ttn.com.tw
remarks:     spam@ttn.com.tw
remarks:     ### Abuse , Spam , Security ###
mnt-by:      MAINT-TTN-AP
changed:     jengjr@ttn.com.tw 20020222
source:      APNIC
```

```
Host: 210.63.108.34
inetnum:     210.60.0.0 - 210.63.255.255
netname:     TWNIC-TW
descr:       Taiwan Network Information Center
descr:       4F-2, No. 9 Sec. 2, Roosevelt Rd.,
descr:       Taipei, Taiwan, 100
country:     TW
admin-c:     SO12-AP
tech-c:      NS10-AP
mnt-by:      APNIC-HM
mnt-lower:   MAINT-TW-TWNIC
changed:     hostmaster@twnic.net 20000811
source:      APNIC

person:      Shih-Chiung Ouyang
address:     Taiwan Network Information Center
address:     4F-2, No. 9 Sec. 2, Roosevelt Rd.,
address:     Taipei, Taiwan, 100
country:     TW
phone:       +886 2 2341 1313 ext. 301
fax-no:      +886 2 2396 8832
e-mail:      oyang@twnic.net
nic-hdl:     SO12-AP
notify:      hostmaster@twnic.net
mnt-by:      MAINT-TW-TWNIC
changed:     hostmaster@twnic.net 20000808
source:      APNIC
```

```
Host: 217.230.236.52
inetnum:      217.224.0.0 - 217.237.161.47
netname:      DTAG-DIAL15
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP-RIPE
tech-c:       ST5359-RIPE
status:       ASSIGNED PA
remarks:      ************************************************************
remarks:      * ABUSE CONTACT: abuse@t-ipnet.de IN CASE OF HACK ATTACKS, *
remarks:      * ILLEGAL ACTIVITY, VIOLATION, SCANS, PROBES, SPAM, ETC.   *
remarks:      ************************************************************
notify:       auftrag@nic.telekom.de
notify:       dbd@nic.dtag.de
mnt-by:       DTAG-NIC
changed:      auftrag@nic.telekom.de 20020108
source:       RIPE
```


Host MY.NET.253.10 NMAP TCP ping!, ICMP Echo Request Nmap or HPING2

On 03/28/2002-15:06:55 and continuing until 03/29/2002-00:25:55, suspicious activity was detected from host MY.NET.253.10. NMAP activity was directed across multiple internal class C networks by

host MY.NET.253.10 including: MY.NET.149.0, MY.NET.150.0, MY.NET.151.0, MY.NET.152.0, MY.NET.153.0, MY.NET.5.0, MY.NET.88.0.

There is no reason this activity should be detected from anyone other than authorized personnel. The user of the host during this period of time should be questioned as this his/her motives. All data collected by the user as a result of this activity should be confiscated and destroyed. If this host is a system under University control and the activity was unauthorized, the *nmap* program should be removed along with any other network reconnaissance tools that may be found installed.

Host MY.NET.186.16 Null Scan!

On 03/27, 03/28, 03/29, and 03/31, packets with no TCP flags set were sent to MY.NET.150.44 and MY.NET.150.137. This is known as null scanning and qualifies this host as suspicious.

In all cases, the source ports were set to TCP port 23, well known for telnet services. However, there is no other activity in all of the logs suggesting MY.NET.186.16 is offering telnet services.

Destination ports were limited to 1081, 1639, 1058, and 1231 for host MY.NET.150.137. Destination ports were limited to 1061, 1053, 1089, and 1050 for MY.NET.150.44.

Null scanning is considered malicious activity because it provides a potential attacker reconnaissance information for follow up attacks. Based on the destination ports for this activity, it is unlikely to be hostile host activity.

7. Analysis Process

Five days of data was downloaded for the alert, scans, and oos data sets. These were downloaded to a Mandrake Linux 8.2 platform. The data was combined within each individual data set using the following sequence of commands.

```
zcat alert.020327.gz > alerts
zcat alert.020328.gz >> alerts
zcat alert.020329.gz >> alerts
zcat alert.020330.gz >> alerts
zcat alert.020331.gz >> alerts

zcat scans.020327.gz > scans
zcat scans.020328.gz >> scans
zcat scans.020329.gz >> scans
zcat scans.020330.gz >> scans
zcat scans.020331.gz >> scans

zcat oos_Mar.27.2002.gz > oos
zcat oos_Mar.28.2002.gz >> oos
zcat oos_Mar.29.2002.gz >> oos
zcat oos_Mar.30.2002.gz >> oos
zcat oos_Mar.31.2002.gz >> oos
```

I made initial attempts at processing the data with SnortSnarf but the script ran out of memory before it could complete. It seems as though a couple of hundred megabytes of Snort alert data is just too much for it to swallow at one time! Rather than fight SnortSnarf, I decided it was probably worth the extra effort in honing my command line skills since these skills will prove valuable on a daily basis for general log intrusion analysis.

The data sets were then processed with custom shell scripts that incorporated heavy use of grep, awk, sed, cut, uniq, and sort to process the data as needed.

Primary custom scripts utilized to process the data:

proc-alerts.sh:	Processes *alerts* data set by parsing it into ";" delimited fields to facilitate analysis with awk and cut. Generates top talker statistics for *alerts* data set. Generates data presented in Section 6: Top Talkers. Generates alert summary data found in Section 4: Alert Summary.
proc-scans.sh	Processes *scans* data set by parsing it into ";" delimited fields to facilitate analysis with awk and cut. Generates top talker statistics for *scans* data set. Used to generate data presented in Section 6: Top Talkers.
proc-oss.ssh	Processes *oos* data set by parsing it into ";" delimited fields to facilitate analysis with awk and cut. Generates top talker statistics for *oos* data set. Used to generate data presented in Section 6: Top Talkers.
attack-profiler.sh	Identifies top source and destination addresses for a given non-ICMP related signature. Used to generate top talker data found throughout Section 5: Alert Summary Analysis.
attack-profiler-icmp.sh	Identifies top source and destination addresses for a given ICMP related signature. Used to generate top talker data found throughout Section 5: Alert Summary Analysis.
host-profiler.sh	Profiles hosts providing well known services on the network. Used to generate data presented in Section 3: Host Profile.

In general, scripts were only used to process the data when repetitive tasks could be facilitated using 'for' loops and the like. When general queries of the data was needed, combinations of grep, cut, and sort commands were issued to the command line.

proc-alerts.sh

```
# Strip out report header rows for each day
grep -v "Snort Alert Report" alerts | grep -v "^\*\*\*\*\*\*\*" > alerts.clean

# Strip out portscan alerts to be counted in scans file
grep -v spp_portscan: alerts.clean > alerts.clean2
rm alerts.clean

# Delimit alerts file for parsing
sed -f sed-script-alerts alerts.clean2 > alerts.delimited
 rm alerts.clean2

# Find top destination ips
awk -F";" '{ print $3 }' alerts.delimited | sort -n | uniq -c | sort -rn > alerts.sourcecount
awk -F";" '{ print $5 }' alerts.delimited | sort -n | uniq -c | sort -rn > alerts.destcount

# Find top signatures
#awk -F";" '{ print $2 }' alerts.delimited | sort -n | uniq -c | sort -rn > alerts.sigcount

rm -f alerts.sigsrcdestcount.*

# Find number of unique sources and destinations for each signature

signatures=`cut -f 2 alerts.sigcount | grep -v ICMP | sed -e 's/ /\.\*/g' `

for i in $signatures ; do
       echo $i `egrep $i alerts.delimited | awk -F";" '{ print $3 }' | sort | uniq -c | wc -l` `egrep
$i alerts.delimited | awk -F";" '{ print $5 }' | sort | uniq -c | wc -l` |
sed -e 's/\.\*/ /g' >> alerts.sigsrcdestcount.nonicmp
       done

signatures=`cut -f 2 alerts.sigcount | grep ICMP | sed -e 's/ /\.\*/g' `

for i in $signatures ; do
```

```
        echo $i `egrep $i alerts.delimited | awk -F";" '{ print $3 }' | sort | uniq -c | wc -l` `egrep
$i alerts.delimited | awk -F";" '{ print $4 }' | sort | uniq -c | wc -l` |
sed -e 's/\.\*/ /g' >> alerts.sigsrcdestcount.icmp
        done
```

proc-scans.sh

```
# Strip out report header rows for each day
grep -v "Snort Scan Report" scans | grep -v "^\*\*\*\*\*\*\*" > scans.clean
# Delimit scans file for parsing
sed -f sed-script-scans scans.clean > scans.delimited
rm scans.clean

# Find top source ips
awk -F";" '{ print $2 }' scans.delimited | sort -n | uniq -c | sort -rn > scans.sourcecount

# Find top destination ips
awk -F";" '{ print $4 }' scans.delimited | sort -n | uniq -c | sort -rn > scans.destcount
```

proc-oos.sh

```
# Strip out all but first line of record for address analysis
grep " -> " oos > oos.1

# Delimit alerts file for parsing
sed -f sed-script-oos oos.1 > oos.delimited
rm oos.1

# Find top sources ips
awk -F";" '{ print $2 }' oos.delimited | sort -n | uniq -c | sort -r -n > oos.sourcecount

# Find top destination ips
awk -F";" '{ print $4 }' oos.delimited | sort -n | uniq -c | sort -r -n > oos.destcount
```

attack-profiler.sh

```
# Accept attack name as $1 from cmd line.  Accept $2 from command line as number of top sources and
destinations to display.

echo $1 > /tmp/tmp.src

echo "Top X Sources for attack \`" $i "\`"
grep -f /tmp/tmp.src alerts.delimited | cut -d";" -f 3 | sort | uniq -c | sort -rn | head -$2

echo "Top X Destinations for attack \`" $i "\`"
grep -f /tmp/tmp.src alerts.delimited | cut -d";" -f 5 | sort | uniq -c | sort -rn | head -$2
```

attack-profiler-icmp.sh

```
# Accept attack name as $1 from cmd line.  Accept $2 from command line as number of top sources and
destinations to display.

echo $1 > /tmp/tmp.src

echo "Top X Sources for attack \`" $i "\`"
grep -f /tmp/tmp.src alerts.delimited | cut -d";" -f 3 | sort | uniq -c | sort -rn | head -$2

echo "Top X Destinations for attack \`" $i "\`"
grep -f /tmp/tmp.src alerts.delimited | cut -d";" -f 4 | sort | uniq -c | sort -rn | head -$2
```

host-profiler.sh

```
# Populate services variable with list of search parameters.
services=`cat host-profiling-service-list.alerts`

# Search delimited alerts for most frequently occurring destination ports.
for i in $services ; do
                echo "For service " $i ":"
                grep $i alerts.delimited | awk -F";" '{ print $5 ":" $6 }' | grep "MY\.NET" | sort |
uniq -c | sort -rn | head -20
```

```
                done
# Populate services variable with list of search parameters.
services=`cat host-profiling-service-list.scans`

# Search delimited scan for most frequently occurring destination ports.
for i in $services ; do
                echo "For service " $i ":"
                grep $i scans.delimited | grep -v ICMP | awk -F";" '{ print $4 ":" $5 ":" $6 }' | grep
"MY\.NET" | sort | uniq -c | sort -rn | head -20
                done
```

8. References

"About SubSeven." URL: http://www.hackfix.org/subseven/about.shtml (May 25, 2002).

Alexander, Bryce. "Intrusion Detection FAQ Port 137 Scan". May 10, 2000. URL: http://www.sans.org/newlook/resources/IDFAQ/port_137.htm (May 1, 2002).

Berkers, John. "IIS Unicode attack detected". URL: http://www.geocrawler.com/mail/msg.php3?msg_id=6390557&list=4890 (May 1, 2002).

Chapman, Todd. "GCIA Practical Assignment v3.0." Oct 2001. URL: http://www.giac.org/practical/Todd_Chapman_GCIA.doc (May 20, 2002).

"eDonkey FAQ". URL: http://www.edonkey2000.com/faq.html#port (May 22, 2002).

"FAQs – SNMPv3 related". http://www.adventnet.com/products/snmp/help/faqs/faq_snmpv3.html (May 22, 2002).

Fyodor. "Remote OS detection via TCP/IP Stack FingerPrinting". April 10, 1999. URL:http://www.insecure.org/nmap/nmap-fingerprinting-article.html (May 22, 2002).

"Giant Port List". URL: http://keir.net/portlist.html (May 22, 2002).

Haugness, Kyle. "GCIA Practical Assignment v3.0." Dec 2001. URL: http://www.giac.org/practical/Kyle_Haugsness_GCIA.zip (May 20, 2002).

"HP Jetdirect Print Servers - HP Jetdirect Port Numbers for TCP and/or UDP Connections". URL: http://www.hp.com/cposupport/networking/support_doc/bpj01014.html (May 22, 2002).

HPING2. URL: http://www.hping.org/ (May 22, 2002).

"IDS311/PING-SCANNER-L3RETRIEVER" URL: http://www.whitehats.com/info/IDS311 (May 22, 2002).

Larratt, Glenn. "Analysis of the Various Top-Ten Nodes". GCIA Practical v3.0. URL: http://www.giac.org/practical/Glenn_Larratt_GCIA.zip (May 22, 2002).

"Microsoft SQL Spida Worm Propagation." Internet Security Systems Security Alert: May 21, 2002. URL:http://www.iss.net/security_center/alerts/advise118.php (May 27, 2002).

Neohapsis Ports List. URL: http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html (May 26, 2002).

Roesch, Martin. snort.conf, Snort v1.77.2.9, March 18, 2002.

SQL Security. URL: http://www.sqlsecurity.com/ (May 27, 2002).

"Strange scan on 1433." URL: http://archives.neohapsis.com/archives/incidents/2002-05/0103.html (May 29, 2002).

Weaver, Lorraine. "GCIA Practical Assignment v2.9". Aug 2001.
URL: http://www.giac.org/practical/Lorraine_Weaver_GCIA.zip (May 21, 2002).

"What is nmap?". URL: http://www.nmap.org/nmap/index.html#intro (May 22, 2002).

"What is Unicode?". May 21, 2002. URL: http://www.unicode.org/unicode/standard/WhatIsUnicode.html (May 23, 2002).

"UDP Ports Used by AFS." URL: http://www.transarc.ibm.com/Support/afs/admin/UDP.html (May 22, 2002).