Global Information Assurance Certification Paper

Intrusion Detection in Depth
SANS GCIA Practical Assignment

Heather M. Larrieu
GIAC GCIA Practical (version 3.3)
Submitted: November 2002

Table of Contents

Table of Contents 2
Assignment #1: Describe the State of Intrusion Detection 4
Grim'sPing: The tool of choice for warez scanners 4
Abstract 4
Introduction 4
Grim'sPing Details 5
Acquiring Grim'sPing 6
Grim'sPing in action 6
Impact and Countermeasures 8
Conclusion 9
References 9
Assignment #2: Three Network Detects 10
Detect #1: Whisker HEAD with large datagram 10
Log Trace 10
Source of Trace 11
Detect was Generated by 12
Probability the Source Address was Spoofed 13
Description of the Attack 13
Attack Mechanism 13
Correlations 15
Evidence of Active Targeting 15
Severity 16
Defensive Recommendation 16
Multiple Choice Test Question 16
Discussion of Detect #1 from the post to Intrusions@incidents.org 17
References 17
Detect #2: SNMP public access udp 18
Trace Log 18
Source of Trace 20
Detect was Generated by 21
Probability the Source Address was Spoofed 21
Probability the Source Address was Spoofed 22
Description of the Attack 22
Attack Mechanism 23
Correlations 24
Evidence of Active Targeting 24
Severity 24
Defensive Recommendation 25
Multiple Choice Test Question 25
References 25
Detect #3: WEB-CGI formmail attempt 26

Trace Log 26
Source of Trace 28
Detect was Generated by 28
Probability the Source Address was Spoofed 29
Description of the Attack 29
Attack Mechanism 29
Correlations 30
Evidence of Active Targeting 30
Severity 30
Defensive Recommendation 31
Multiple Choice Test Question 31
References 31
Assignment #3: Analyze This! 33
Executive Summary 33
Logs Analyzed 34
Most Frequent Events (Generated More than 10,000 Times) 34
Frequent Alert Details 35
Frequent Scan Details 41
TOP 5 External Scanners 44
Events of Interest: Alerts Concerning Trojan/Rootkit Activity 47
Trojan/Rootkit Details 47
Top 10 Hosts to investigate 50
Events of Interest: Out of Spec packets 50
User activity Policy issues 51
Conclusions and Defensive Recommendations 51
List of hosts to Investigate 53
References 55
Appendix A Methodologies 55
Tools and Methodology 55
Appendix B complete list of Detects 56

Assignment #1: Describe the State of Intrusion Detection

Grim'sPing: The tool of choice for warez scanners

Abstract

Warez pirates are actively scanning networks worldwide looking for open FTP servers where they can store their warez. The most commonly used tool for pub scanning is Grim'sPing. Grim'sPing leaves a signature that can be detected by most intrusion detection systems in use today. This paper provides some background into the warez pirate culture, discusses the features and usage of the tool, shows examples of Grim'sPing in action from different perspectives, and provides some countermeasures that may be used to protect machines.

Introduction

The rapid growth of the Internet with its complexity and distributed nature has engendered unique opportunities for the creation of niche social groups. These niche groups include individuals unified by real world hobbies like gardening, groups centered around thematic web-rings, where individually administered web sites are linked by that theme, and groups that would like to style themselves as a new "counter culture." This new "counter culture" includes cracker communities, like the Cult of the Dead Cow [1] and warez pirates, among others. Warez pirates, who often call themselves "warez d00dz [2]," specialize in getting copies, usually illegal, of software or digital media, breaking copy protection if it exists, and redistributing it worldwide via FTP servers. Empirical evidence suggests "warez d00dz"'s activities are a frequent source of alerts in intrusion detection systems.

Activities that an analyst sees which can be indicative of warez pirate activity may consist of pub scanning, "FXP"ing, and, of course uploading and downloading data on FTP servers. Pub scanning is the practice of scanning IP address ranges looking for FTP servers that allow anonymous users to read and write to directories [3]. "FXP"ing involves moving significant amounts of data directly between FTP servers using the File Exchange Protocol – FXP as an acronym. FXP allows files to be copied directly from one FTP server to another. FXP is used for data replication to protect the availability of the warez pirates' files, and to make the data as widely available as possible [4]. FTP servers that allow anonymous writes which are found during the pub scanning process will be used for storage of illegal software, videos, or music files. Usually the address of the vulnerable machine will be published to a warez list site or passed around via some form of IRC so that other warez pirates can share the site's resources.

There is a complex culture associated with warez pirates. They usually operate in groups

with some members assigned to scan and others to move or use the data [4]. In a fashion similar to street gangs, warez pirates might tag the directories they create on the FTP servers with special codes indicating which group "owns" the data contained therein. Tag lists are maintained on the Internet, and can usually be found at sites that may also host pub scanning tools or tutorials. The Grim'sPing site maintains a database of warez d00dz tags [5]. Tagging is supposedly respected by other warez groups, but there are some who actively delete rival groups' files. These people, along with legitimate system administrators, are often named, in a derogatory fashion, "deleters."

Warez pirates employ many techniques to try to protect their sites from deleters. These usually consist of some creative naming scheme, using unprintable characters, or exploiting system specifics to create hidden files or set permissions [5]. Techniques for thwarting deleters comprise a significant portion of web published tutorials and other warez pirate documents.

Warez pirates are often not interested in compromising the machines beyond their desire for storage space. They tend to be looking for places with high bandwidth and lots of disk space. Sometimes, however, they are employing cracker techniques to gain access to FTP servers. In addition, their basic philosophy of exploiting someone's configuration errors or open stance security policies makes them a general nuisance. Further, they may introduce liability, potential denial of service, or aggravation to legitimate site owners. Whatever their methods or motives, warez pirates, like other computer abusers, have a reconnaissance phase that can be detected. The tool most commonly used to seek out vulnerable systems seems to be Grim'sPing.

Grim'sPing Details

Grim'sPing is designed to take advantage of servers running an anonymous FTP service. FTP allows users to connect to a machine remotely to add and get data files from the file system hosted on the remote server. FTP can be configured to require varying levels of authentication to access the file system. Anonymous FTP allows unrestricted connection to the remote machine – no password or user account required. Usually, administrators who run anonymous FTP services are careful to configure it to allow user to read from the file system only. In some cases, however, the servers may be configured to allow both read and write access to anyone who wants to exchange files.

Grim'sPing[6] is a pub-scanning tool with a variety of features and complementary programs that make the pub finding process easy. The tool runs on Windows platforms from Windows95 through WindowsXP. One of the features of the tool is the ability to use a proxy to make it more difficult for security analysts to find the source of the scan. If the scanner does not already use proxy, Grim'sPing has a feature to log any Wingate proxies it finds during its scanning process that can then be used for future scanning efforts. Grim'sPing can record the speed, FXP capabilities, permissions, and operating

system of the remote machine. It can ping, scan, and pub find on any given IP address range. An FTP client is also a component of the program.

Some of the complementary programs available for Grim'sPing include: PingCompanion, TagCheck, Wingate Verification Utility, and Shutdown. PingCompanion provides a variety of capability measures of the FTP servers Grim'sPing encounters. These capability measures include download and upload speed, access time, and delete permissions, and available space. TagCheck will search the entire remote directory structure looking for tags that may have been left by other warez d00dz, comparing tags against a database kept on the Grim'sPing web site. The WinGate Verification Utility checks wingates' usability by executing an anonymous connection to ftp.microsoft.com. Finally, to make the most efficient use of a pub scanners time and dial up connection, Shutdown, allows the pub scan to run unmonitored, and will shutdown the program and machine at times specified. This helps keep costs down for the warez d00d by ensuring maximum scan time without exceeding available usage hours imposed by some ISPs, and will keep the phone available during waking hours for those using modem based network connections.

Acquiring Grim'sPing

Grim'sPing and its companion programs are available from http://grimsping.cjb.net/ and mirror sites. In addition to the program itself, there is an online tutorial. The site also contains links to sites with information relating to the warez d00dz scene such as protocol information, and pub scanning tips.

Grim'sPing in action

Grim'sPing walks the IP range given and attempts to get a successful connection to an FTP server on the default port number 21. If an FTP server is running on port 21, Grim'sPing attempts an anonymous login. Usually FTP servers that allow anonymous logins ask for an email address as the password. The password given is either Xgpuser@home.com where X will be some letter of the alphabet, or guest@here.com. Grim'sPing has a list of directories commonly found on FTP servers, such as /pub, /incoming, or /upload, and it tries to change to those directories. If a directory exists, Grim'sPing will attempt to write subdirectory with the name generated from a timestamp.

Here is a Grim'sPing scan that was detected by NID [8], an intrusion detection system created by the DOE.

[Begin NID Log]

```
#-ftp     1211   *6.285*  pD9030141.dip.t-dialin.net          AAA.BBB.org
============================================================
```

```
Source      = XXX.YYY.ZZZ.102 -- AAA.BBB.org
Destination =     217.3.1.65 -- pD9030141.dip.t-dialin.net
Start time  = Sat Aug 24 00:37:24 2002
Protocols   = [21 4512] (6)
Stream      = /n/nidwork/Connections/con02082322-8.1211.stream.dest
================================================================
<SNIP>

230 Guest login ok, access restrictions apply.
250 CWD command successful.
550 020824063837p: Permission denied on server. (Upload dirs)
550 /public/: No such file or directory.
250 CWD command successful.
550 020824063838p: Permission denied on server. (Upload dirs)
550 /incoming/: No such file or directory.
550 /_vti_pvt/: No such file or directory.
250 CWD command successful.
550 020824063839p: Permission denied on server. (Upload dirs)
550 /upload/: No such file or directory.

 [***** End of stream *****]

#-ftp     1211   *6.285*  pD9030141.dip.t-dialin.net            AAA.BBB.org
================================================================
Source      =     217.3.1.65 -- pD9030141.dip.t-dialin.net
Destination = XXX.YYY.ZZZ.102 -- AAA.BBB.org
Start time  = Sat Aug 24 00:37:24 2002
Protocols   = [4512 21] (6)
Stream      = /n/nidwork/Connections/con02082322-8.1211.stream.init
================================================================

USER anonymous
PASS Wgpuser@home.com
CWD /pub/
MKD 020824063837p
CWD /public/
CWD /pub/incoming/
MKD 020824063838p
CWD /incoming/
CWD /_vti_pvt/
CWD /
MKD 020824063839p
CWD /upload/
```

[End NID Log]

As can be seen from this NID log, the Grim'sPing user originates from a dial-up connection on the t-dialin.net, which is a German ISP known as a hot bed for pub scanner activity. The tool supplies "Wgpuser@home.com" as its password. The letters "gp" apparently stand for Grim'sPing. The first directory checked, /pub, exists on this server, so the tool attempts to create the file 020824063837p. Note that the file name given is effectively a time stamp for August 24, 2002 at 06:38:37, which corresponds to the time of the access plus the 6 hour time difference to Germany from the time zone in which this server resides. The next requested directory, /public, does not exist. The directory /pub/incoming is requested next, and since it exists, Grim'sPing again tries to create a directory with the access timestamp. The timestamps chosen for the files show that the entire session lasts less than two seconds, which is further evidence that this is tool-based activity.

Looking at the attack from another perspective, we can see that it is part of a scan of the

complete class C subnet. Below is an excerpt of the scan as seen by a SHADOW sensor, which resides outside the firewall [9]. The scan log here has been limited to only three machines. Two of the machines are not running an FTP server. The XXX.YYY.ZZZ.102 is the machine running the FTP server on which the activity shown in the NID alert takes place.

[Begin Shadow Log]

<Snip>

```
00:38:35.280429 pD9030141.dip.t-dialin.net.4503 > XXX.YYY.ZZZ.101.ftp: S 1324875463:1324875463(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
00:38:35.340429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: S 1325013762:1325013762(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
00:38:35.340429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: S 2648346965:2648346965(0) ack
1325013763 win 31740 <mss 1380,nop,nop,sackOK> (DF)
00:38:35.360429 pD9030141.dip.t-dialin.net.4526 > XXX.YYY.ZZZ.103.ftp: S 1325168382:1325168382(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
00:38:36.060429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 1:1381(1380) ack 1 win 31740 (DF)
00:38:36.630429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 1381:1648(267) ack 1 win 31740 (DF)
00:38:36.850429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 1:17(16) ack 1648 win 16293 (DF)
00:38:36.880429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 1648:1716(68) ack 17 win 31740 (DF)
00:38:37.070429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 17:40(23) ack 1716 win 16225 (DF)
00:38:37.340429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 1716:3096(1380) ack 40 win 31740
(DF)
00:38:37.950429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3096:3211(115) ack 40 win 31740
(DF)
00:38:38.310429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 40:51(11) ack 3211 win 16445 (DF)
00:38:38.350429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3211:3240(29) ack 51 win 31740 (DF)
00:38:38.370429 pD9030141.dip.t-dialin.net.4503 > XXX.YYY.ZZZ.101.ftp: S 1324875463:1324875463(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
00:38:38.440429 pD9030141.dip.t-dialin.net.4526 > XXX.YYY.ZZZ.103.ftp: S 1325168382:1325168382(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
00:38:38.750429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 51:70(19) ack 3240 win 16416 (DF)
00:38:38.780429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3240:3303(63) ack 70 win 31740 (DF)
00:38:39.100429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 70:84(14) ack 3303 win 16353 (DF)
00:38:39.120429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3303:3345(42) ack 84 win 31740 (DF)
00:38:39.360429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 84:104(20) ack 3345 win 16311 (DF)
00:38:39.410429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3345:3374(29) ack 104 win 31740
(DF)
00:38:39.640429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 104:123(19) ack 3374 win 16282 (DF)
00:38:39.660429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3374:3437(63) ack 123 win 31740
(DF)
00:38:39.850429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 123:139(16) ack 3437 win 16219 (DF)
00:38:39.880429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3437:3481(44) ack 139 win 31740
(DF)
00:38:40.070429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 139:155(16) ack 3481 win 16175 (DF)
00:38:40.100429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3481:3525(44) ack 155 win 31740
(DF)
00:38:40.290429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 155:162(7) ack 3525 win 16131 (DF)
00:38:40.310429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3525:3554(29) ack 162 win 31740
(DF)
00:38:40.490429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 162:181(19) ack 3554 win 16102 (DF)
00:38:40.520429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3554:3617(63) ack 181 win 31740
(DF)
00:38:40.810429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: P 181:195(14) ack 3617 win 16039 (DF)
00:38:40.830429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: P 3617:3659(42) ack 195 win 31740
(DF)
00:38:41.160429 pD9030141.dip.t-dialin.net.4512 > XXX.YYY.ZZZ.102.ftp: F 195:195(0) ack 3659 win 15997 (DF)
00:38:41.180429 XXX.YYY.ZZZ.102.ftp > pD9030141.dip.t-dialin.net.4512: F 3659:3659(0) ack 196 win 31740 (DF)
00:38:44.390429 pD9030141.dip.t-dialin.net.4526 > XXX.YYY.ZZZ.103.ftp: S 1325168382:1325168382(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
```

<Snip>

[End Shadow Log]

Impact and Countermeasures

The warez pirates can potentially fill up disk space or hog bandwidth that would better be allocated for legitimate system users, and they can potentially create legal trouble owing to the nature of the data being moved around. Based on the potential problem and the nuisance factor, warez d00dz should be regarded in the same vein as any malicious cracker.

Counter measures that might prove of value to protect FTP systems from warez pirates are effectively the same as with any host that provides service to the open Internet. The first requirement is to ensure that the service is actually needed. If it is, it should be on a hardened machine on a screened network that can limit the amount of contact available to the box. In addition, serious evaluation should be given as to the need for anonymous write access. There are very few cases where that should be allowed. Where anonymous writes are allowed, the machine's disk utilization should be monitored to show any sudden and inexplicable use of resources.

If an administrator wanted to protect or detect Grim'sPing using a network based intrusion detection system like Snort, there are a variety of rules that could be implemented [10]. A simple rule like the following would likely detect Grim'sPing access based on the string presented for the response to the password prompt.

```
(alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"Grims'sPing"; content:"gpuser@home.com";
flags:A+; classtype:attempted-recon;)
```

To stop Grim'sPing traffic at a site, there are flexible response options available in some network ID systems that can interrupt the connection possibly by sending TCP resets to both hosts in the session.

Conclusion

Warez pirate activity should be regarded as cracker activity. Tools like Grim'sPing make pub scanning easy for warez pirates, and seemingly, there is a large population of warez d00dz out there. Based on remarks in postings to various security specific mail lists, there are unusual concentrations of them in Germany and France, who are taking a crack at millions of IP addresses trying to find space and bandwidth. Fortunately for computer security analysts, the primary tool in use leaves distinct signatures that can be detected by most ID systems.

References

[1] cDc."CultofDeadCow" URL: www.cultdeadcow.com/. (Sept 5, 2002)

[2] esr. "Warez d00dz /weirz doodz/ n." URL: http://www.tuxedo.org/~esr/jargon/html/entry/warez-d00dz.html (Sept 5, 2002)

[3] fantasymike**.** **"**FXP - Finding Pubs." URL: http://core-knowledge.tripod.com/fxp_pubfind.htm (Sept 5, 2002)

[4] obscure. "When your server ends up a Warez site." 21.June.2001 URL: http://eyeonsecurity.net/papers/pubscanning.htm (Sept 5, 2002)

[5] grim. "Current Tag List" URL: http://Grim'sPing.cjb.net/downloads.htm (Sept 5, 2002)

[6] pirate. "HOW TO MANUAL - THE END OF DELETERS." Apr. 11, 2001 URL: http://www.xs4all.nl/~liew/startdivx/endofdeleters.txt (Sept 5, 2002)

[7] grim. "Grim'sPing: Making the everyday pub scanning faster and more reliable" July 12, 2002. URL: http://Grim'sPing.cjb.net/ (Aug 22, 2002)

[8] DOE-CIAC. " DOE-CIAC's Network Intrusion Detector (NID) Distribution Site" Dec 3, 2001. URL: http://ciac.llnl.gov/cstc/nid/nid.html (Aug 22, 2002)

[9] NSWC. "NSWC SHADOW INDEX" URL: http://www.nswc.navy.mil/ISSEC/CID/ (Aug 22,2002)

[10] Caswell and Roesch. "Snort: the Open Source Network Intrusion Detection System" 2002. URL: http://www.snort.org (Sept 14, 2002)

Assignment #2: Three Network Detects

For this assignment, I attempted to pick three detects which would form a representative set expressing the variety of detects an analyst should expect to encounter daily. Curiously, most of the detects I sifted through while working on this assignment were either the extremely popular attacks against IIS web servers (of which submission is discouraged), warez scans, and false positives resulting from badly configured machines.

Detect #1 was submitted on November 12, 2002 to intrusions@incidents.org as required.

Detect #1: Whisker HEAD with large datagram

Log Trace

Snort Alert:

[**] [1:1171:7] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/02-16:03:56.194488 208.187.37.97:1440 -> 46.5.180.133:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:987
AP Seq: 0x15150707 Ack: 0x105C801E Win: 0x7C70 TcpLen: 20

[Xref => http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html]

Full Packet Log:

```
[**] WEB-MISC whisker HEAD with large datagram [**]
07/02-16:03:56.194488 208.187.37.97:1440 -> 46.5.180.133:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:987
***AP*** Seq: 0x15150707  Ack: 0x105C801E  Win: 0x7C70  TcpLen: 20
0x0000: 00 00 0C 04 B2 33 00 03 E3 D9 26 C0 08 00 45 10  .....3....&...E.
0x0010: 03 DB 00 00 00 00 F0 06 00 00 D0 BB 25 61 2E 05  ............%a..
0x0020: B4 85 05 A0 00 50 15 15 07 07 10 5C 80 1E 50 18  .....P.....\..P.
0x0030: 7C 70 00 00 00 00 00 48 45 41 44 20 2F 6D 61 69 6E  |p....HEAD /main
0x0040: 2F 64 61 74 61 73 68 65 65 74 73 2F 33 32 30 30  /datasheets/3200
0x0050: 2E 70 64 66 20 48 54 54 50 2F 31 2E 31 0D 0A 48  .pdf HTTP/1.1..H
0x0060: 6F 73 74 3A 20 77 77 77 2E 58 58 58 58 2E 63 6F  ost: www.XXXX.co
0x0070: 6D 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D  m..User-Agent: M
0x0080: 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 58 31 31 3B  ozilla/5.0 (X11;
0x0090: 20 55 3B 20 4C 69 6E 75 78 20 69 36 38 36 3B 20   U; Linux i686;
0x00A0: 65 6E 2D 55 53 3B 20 72 76 3A 30 2E 39 2E 39 29  en-US; rv:0.9.9)
0x00B0: 20 47 65 63 6B 6F 2F 32 30 30 32 30 34 30 38 0D   Gecko/20020408.
0x00C0: 0A 41 63 63 65 70 74 3A 20 74 65 78 74 2F 78 6D  .Accept: text/xm
0x00D0: 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 6D  l,application/xm
0x00E0: 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78 68  l,application/xh
0x00F0: 74 6D 6C 2B 78 6D 6C 2C 74 65 78 74 2F 68 74 6D  tml+xml,text/htm
0x0100: 6C 3B 71 3D 30 2E 39 2C 74 65 78 74 2F 70 6C 61  l;q=0.9,text/pla
0x0110: 69 6E 3B 71 3D 30 2E 38 2C 76 69 64 65 6F 2F 78  in;q=0.8,video/x
0x0120: 2D 6D 6E 67 2C 69 6D 61 67 65 2F 70 6E 67 2C 69  -mng,image/png,i
0x0130: 6D 61 67 65 2F 6A 70 65 67 2C 69 6D 61 67 65 2F  mage/jpeg,image/
0x0140: 67 69 66 3B 71 3D 30 2E 32 2C 74 65 78 74 2F 63  gif;q=0.2,text/c
0x0150: 73 73 2C 2A 2F 2A 3B 71 3D 30 2E 31 0D 0A 41 63  ss,*/*;q=0.1..Ac
0x0160: 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 65  cept-Language: e
0x0170: 6E 2D 75 73 2C 20 65 6E 3B 71 3D 30 2E 35 30 0D  n-us, en;q=0.50.
0x0180: 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67  .Accept-Encoding
0x0190: 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 2C  : gzip, deflate,
0x01A0: 20 63 6F 6D 70 72 65 73 73 3B 71 3D 30 2E 39 0D   compress;q=0.9.
0x01B0: 0A 41 63 63 65 70 74 2D 43 68 61 72 73 65 74 3A  .Accept-Charset:
0x01C0: 20 49 53 4F 2D 38 38 35 39 2D 31 2C 20 75 74 66   ISO-8859-1, utf
0x01D0: 2D 38 3B 71 3D 30 2E 36 36 2C 20 2A 3B 71 3D 30  -8;q=0.66, *;q=0
0x01E0: 2E 36 36 0D 0A 4B 65 65 70 2D 41 6C 69 76 65 3A  .66..Keep-Alive:
0x01F0: 20 33 30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E   300..Connection
0x0200: 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A 0D 0A  : keep-alive....
0x0210: 47 45 54 20 2F 6D 61 69 6E 2F 64 61 74 61 73 68  GET /main/datash
0x0220: 65 65 74 73 2F 33 32 30 30 2E 70 64 66 20 48 54  eets/3200.pdf HT
0x0230: 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 77 77  TP/1.1..Host: ww
0x0240: 77 2E 58 58 58 58 2E 63 6F 6D 0D 0A 55 73 65 72  w.XXXX.com..User
0x0250: 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F  -Agent: Mozilla/
0x0260: 35 2E 30 20 28 58 31 31 3B 20 55 3B 20 4C 69 6E  5.0 (X11; U; Lin
0x0270: 75 78 20 69 36 38 36 3B 20 65 6E 2D 55 53 3B 20  ux i686; en-US;
0x0280: 72 76 3A 30 2E 39 2E 39 20 47 65 63 6B 6F 2F  rv:0.9.9) Gecko/
0x0290: 32 30 30 32 30 34 30 38 0D 0A 41 63 63 65 70 74  20020408..Accept
0x02A0: 3A 20 74 65 78 74 2F 78 6D 6C 2C 61 70 70 6C 69  : text/xml,appli
0x02B0: 63 61 74 69 6F 6E 2F 78 6D 6C 2C 61 70 70 6C 69  cation/xml,appli
0x02C0: 63 61 74 69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C  cation/xhtml+xml
0x02D0: 2C 74 65 78 74 2F 68 74 6D 6C 3B 71 3D 30 2E 39  ,text/html;q=0.9
0x02E0: 2C 74 65 78 74 2F 70 6C 61 69 6E 3B 71 3D 30 2E  ,text/plain;q=0.
0x02F0: 38 2C 76 69 64 65 6F 2F 78 2D 6D 6E 67 2C 69 6D  8,video/x-mng,im
0x0300: 61 67 65 2F 70 6E 67 2C 69 6D 61 67 65 2F 6A 70  age/png,image/jp
0x0310: 65 67 2C 69 6D 61 67 65 2F 67 69 66 3B 71 3D 30  eg,image/gif;q=0
0x0320: 2E 32 2C 74 65 78 74 2F 63 73 73 2C 2A 2F 2A 3B  .2,text/css,*/*;
0x0330: 71 3D 30 2E 31 0D 0A 41 63 63 65 70 74 2D 4C 61  q=0.1..Accept-La
0x0340: 6E 67 75 61 67 65 3A 20 65 6E 2D 75 73 2C 20 65  nguage: en-us, e
0x0350: 6E 3B 71 3D 30 2E 35 30 0D 0A 41 63 63 65 70 74  n;q=0.50..Accept
0x0360: 2D 45 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C  -Encoding: gzip,
0x0370: 20 64 65 66 6C 61 74 65 2C 20 63 6F 6D 70 72 65   deflate, compre
0x0380: 73 73 3B 71 3D 30 2E 39 0D 0A 41 63 63 65 70 74  ss;q=0.9..Accept
0x0390: 2D 43 68 61 72 73 65 74 3A 20 49 53 4F 2D 38 38  -Charset: ISO-88
0x03A0: 35 39 2D 31 2C 20 75 74 66 2D 38 3B 71 3D 30 2E  59-1, utf-8;q=0.
```

```
0x03B0: 36 36 2C 20 2A 3B 71 3D 30 2E 36 36 0D 0A 4B 65  66, *;q=0.66..Ke
0x03C0: 65 70 2D 41 6C 69 76 65 3A 20 33 30 30 0D 0A 43  ep-Alive: 300..C
0x03D0: 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D  onnection: keep-
0x03E0: 61 6C 69 76 65 0D 0A 0D 0A                       alive....
```

Source of Trace

This trace comes from the log file 2002.6.2 available from http://www.incidents.org/logs/Raw.

Note that while the file name implies that the data is from 6/2/2002, it is really from 7/2/2002. It looks as if there may have been some editing in the packet payload, because the http host field in the packet data, which should be the name of the host to which the connection is directed, is " www.XXXX.com" which resolves to a very different address space than the domain at which the packet has been directed, i.e. 46.5.180.133. However, since the IP address has been preserved, I do not know what the motivation for the edit would have been.

Detect was Generated by

SNORT Version 1.8.4 (Build 99) was used to analyze the log file data.
The triggering signature for this detect is in figure 2.1.

Figure 2.1.Snort Whisker HEAD with large datagram

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-MISC whisker HEAD with large datagram";
content:"HEAD"; offset: 0; depth: 4; nocase; dsize:>512;
flags:A+; classtype:attempted-recon;
reference:url,www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html;
sid:1171; rev:7;)
```

This rule indicates that for any packet that enters the home network directed to any machine defined in the $HTTP_SERVERS list on any of the ports listed in the $HTTP_PORTS list which matches the following conditions, a "WEB-MISC whisker HEAD with large datagram" alert should be issued.

The triggering conditions in addition to the aforementioned source, destination, and ports are: The data payload contains the string "HEAD" either upper or lower case somewhere in the packet starting at the first byte with a four byte search depth. The data payload is larger than 512 Bytes. The packet has the acknowledgement flag set indicating that a TCP session has been established.

Log format explanation

When run in IDS mode with default logging, Snort creates a directory structure based on the source IP address in which to store the individual packets. The files stored this directory structure are named using protocol and port data gathered from the triggering packet. Each alert also has a summary entry in an alerts file located in the base directory that contains all of the alerts generated over the run period. The two entries generated by this particular event of interest are shown above labeled "Full Packet Log" and "Snort Alert."

The "Snort Alert" is a high level summary of the packet that triggered the alert that consists of data gleaned from the triggering rule and the incoming packet. The first line is an alert label. The first informative field specifies the rule's number and revision. The second field provides a descriptive label for the event, with the first string being a broad categorization of the type of event. This is usually consistent with the rule file in which the triggering rule is found. The second line provides a finer grained classification of the attack, and a priority level. The third line consists of the time stamp at which the IDS sensor saw the packet, and the source and destination IP address with associated source and destination ports. The fourth line indicates the packet's associated protocol, its Time to Live (TTL), type of service (TOS), identification (ID), IP header length (IpLen), and the datagram length (DgmLen). The fifth line consists of a summary of the flags set on the packet, the sequence number, the acknowledgement number, the window size and the TCP header length. The sixth line a pointer to further information about the alert.

The "Full Packet Log" is summary information followed by the packet contents in a hexadecimal dump with associated ASCII translation. As in the alert entry, the first line is a descriptive label. The second through fourth lines are equivalent to the third through fifth of the "Snort Alert" as described above. The next lines are the packet's data in hexadecimal and ASCII.

Probability the Source Address was Spoofed

The source address for this packet is probably not spoofed. The three-way handshake would have to have been established both before the HTTP HEAD was a legitimate request issued to the web server, and as a requirement for the triggering signature to generate the alert.

Description of the Attack

This detect is indicative of a potential Whisker CGI scan. Whisker is a tool that can be used for reconnaissance to find web servers that are badly configured and potentially exploitable. Basically, Whisker makes requests to web servers for files known to be exploitable, and reports the results to the user. Whisker has features that can help hide the reconnaissance scan from intrusion detection systems, including using the lesser

known HEAD directive instead of the GET request which is the basis for many common rules.

I believe that this is a false positive. This is the only packet directed at this web server from the source address over the course of the day, and the request is for a seemingly innocuous file. If the file is not innocuous, it certainly should not be accessible on a publicly accessible web server as that introduces the possibility of providing proprietary information to the general public. In addition, I examined Whisker version 2.0 and determined that it does not scan for any particular .pdf files by default. Further, although the payload size and the use of the directive HEAD are consistent with Whisker's ids evasion techniques, including a HEAD and a GET request in the same packet is not.

Attack Mechanism

Is it a stimulus or response: Stimulus – request for a web page
Affected Service: Web service on port 80/tcp
Known Vulnerabilities/Exposures: Unknown for this particular machine's installation, but, historically, web servers have many vulnerabilities, and are a frequent target.
Attack Intent: Reconnaissance if it was a real Whisker scan, but this is a false positive

Details: Whisker queries a web server looking for specific configuration information or the existence of files, directories, and scripts, to identify potentially exploitable vulnerabilities on the server. Whisker has a list of known vulnerabilities and weaknesses to check. Whisker tries to perform a scan without tripping intrusion detection systems by using the HEAD directive instead of GET, using encoding of the URI in he query, or padding a request using self referential paths among other techniques. The second two techniques are common IDS evasions. The directive selection is a web server specific evasion. According to the http protocol, the HEAD directive returns meta-data about the requested file, without returning the page proper. For Whisker, this provides all of the required information to use for reconnaissance while evading the IDS, as all Whisker is after is a confirmation that the file exists. A paper on Whisker's anti-IDS features is available from http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html. The large datagram component of this detect is probably based on the idea that the padding or encoding methods can potentially create very long URIs.

Attacker details:

Whois Info:

Server used for this query: [whois.arin.net]

OrgName: Electric Lightwave Inc
OrgID: ELIX

NetRange: 208.186.0.0 - 208.187.255.255
CIDR: 208.186.0.0/15

NetName: ELI-2-NETBLK99
NetHandle: NET-208-186-0-0-1
Parent: NET-208-0-0-0-0
NetType: Direct Allocation
NameServer: NS.ELI.NET
NameServer: NS2.ELI.NET
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 1999-08-24
Updated: 2001-09-26

TechHandle: DD179-ARIN
TechName: Data Eng, Dept
TechPhone: +1-360-892-1000
TechEmail: abuse@eli.net

OrgTechHandle: ENA-ARIN
OrgTechName: ELI Network Abuse
OrgTechPhone: +1-800-622-4354
OrgTechEmail: abuse@eli.net

ARIN Whois database, last updated 2002-09-13 19:05
Enter ? for additional hints on searching ARIN's Whois database

Host OS:

Judging by the TTL value, this is most likely from a Solaris box.

Correlations

I searched known scanners lists, the google search engine, my own site, and for five days around the triggered event in the log files available from http://www.incidents.org/logs/Raw, and this is the only packet I found from this source IP. I also queried dshield.org, and that was negative as well. Unfortunately, the request to dshield took three days to complete.

Michael Aylor's post to incidents.org on Saturday, August 03, 2002 6:43 PM, argues a similar case about the following packet being a false positive. Here as well, the requester was looking for a .pdf file, and not the type of file that would be expected in a Whisker scan (e.g. an .exe).

[**] [1:1171:6] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
07/18-07:16:36.714488 202.214.44.44:1677 -> 46.5.180.133:80 TCP TTL:46
TOS:0x0 ID:60402 IpLen:20 DgmLen:570 DF
AP Seq: 0x8A1E6C65 Ack: 0xDCAE637 Win: 0x4470 TcpLen: 20 [Xref
=> http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html]

Sebastien Pratte posted a similar Whisker detect to incidents.org, and indicated that there were several in rapid succession which he suggested could be the basis for a denial of service attempt on the web server.

[**] [1:1171:3] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/29-11:30:20.844488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x35E
195.132.0.30:14937 -> 46.5.180.133:80 TCP TTL:240 TOS:0x10 ID:0 IpLen:20

```
DgmLen:848
***AP*** Seq: 0x5241DADC Ack: 0xE824E61C Win: 0x7C70 TcpLen: 20

[**] [1:1171:3] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/29-11:30:27.014488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x35F
195.132.0.30:14937 -> 46.5.180.133:80 TCP TTL:240 TOS:0x10 ID:0 IpLen:20
DgmLen:849
***AP*** Seq: 0x5241DDFE Ack: 0xE824E945 Win: 0x7C70 TcpLen: 20

[**] [1:1171:3] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/29-11:30:28.454488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x351
195.132.0.30:14937 -> 46.5.180.133:80 TCP TTL:240 TOS:0x10 ID:0 IpLen:20
DgmLen:835
***AP*** Seq: 0x5241E100 Ack: 0xE824EC60 Win: 0x7C70 TcpLen: 20

[**] [1:1171:3] WEB-MISC whisker HEAD with large datagram [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/29-11:30:30.014488 0:3:E3:D9:26:C0 -> 0:0:C:4:B2:33 type:0x800 len:0x34E
195.132.0.30:14937 -> 46.5.180.133:80 TCP TTL:240 TOS:0x10 ID:0 IpLen:20
DgmLen:832
***AP*** Seq: 0x5241E41A Ack: 0xE824EF78 Win: 0x7C70 TcpLen: 20
```


Evidence of Active Targeting

Active targeting is evident with the information available. The request for a very specific (not common or default page) is made to a specific web server, and there is no other activity to other ports on the same machine, nor for any other machine on the network at any port. It is not, however, any compromise attempt, unless the document has been erroneously published to the web server and the searcher is taking advantage of the situation to gain access to proprietary data.

Severity

Severity is calculated using the formula:

(Target's Criticality + Attack Lethality) - (System defense + Network defense)

Each element is worth 1 (lowest) to 5 (highest) points

Criticality	It's a web server which is critical if this is an information portal or an ecommerce site	**5**
Lethality	This is a reconnaissance attempt in and of itself it does not harm the server	**1**
System	This page and port look to be purposefully available, and I have no information about the system other than that it is a web server, so err on the conservative side.	**1**
Network	It is monitored by a network based IDS, so I will give the benefit of the doubt for perimeter defenses (e.g. a firewall)	**4**

According to the formula, the severity of this detect is 1.

Because this is a false positive, we end up with a very low severity value. Had it been an actual Whisker scan that was attempting to evade the IDS, I would have increased the lethality a little bit because of the presumably malicious intent.

Defensive Recommendation

While this particular detect was not a problem, it would be prudent to run a vulnerability assessment tool, perhaps even Whisker, against the web server. Other than that, keep the server patched and monitored. Make sure development and production environments are separate, and limit the access to this machine at the firewall to only those ports, which are required.

Multiple Choice Test Question

Which of the following would trigger the given Snort Rule?

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-MISC Anti-IDS" content:"/cgi-bin/my.cgi"; nocase;
offset : 0; flags:A+; classtype:attempted-recon;
reference:url,www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html;
sid:1171; rev:7;)
```

a. HEAD /./Cgi-bin/./my.cgi HTTP/1.0
b. GET /Cgi-Bin/my.cgi HTTP/1.0
c. GET /Cgi-bin\My.cgi HTTP/1.0
d. HEAD /cgi-bin/../cgi-bin/ HTTP/1.0

Answer: (b) Only b will trigger this rule, because we specify that the packet must contain the string "/cgi-bin/my.cgi" regardless of the case.

a. This tries to evade detection using mixed case, self referential paths, and HEAD instead of Get
c. This takes advantage of the Windows file system presenting what would be a valid request to an IIS server, but it does not match the string we are looking for
d. This tries to take advantage of reverse directory transversal, and does not actually request our "my.cgi" file

Discussion of Detect #1 from the post to Intrusions@incidents.org

The discussion generated by my post on November 12, 2002 centered primarily on Snort usage issues, and the possible causes for the HEAD and Get request being contained in the single packet.

Julian Radoff and David Hoelzer were concerned that the “padding” at the beginning of the HEX dump was some indication that the packet was crafted, but it turns out that the way I was running Snort (-X) it both interprets the packet header data and displays the

HEX encoding of the data.

Robert Wagner asked if it would be prudent to check the referring page to see if the link was intentionally constructed that way, and whether it was possible that this was normal behavior for the user-agent making the request. Laura Nuñez also asked whether is was normal to have the HEAD and GET request in the same packet.

I determined that this is not usual behavior, but it is still not evidence of malicious intent because it neither compromises the server in any way, nor does it gain the user any further information. A check of the referring page, maybe possibly turn up a specifically crafted user request, but even then this would probably just be an error and not malice. After a lot of thrashing around and attempting to recreate the packet itself, I have determined that this is most likely an artifact of a buggy implementation of the new html pipelining capability available in HTTP 1.1. Specifically it looks as if the pipelining did not take into account the point of the caching scheme. The caching scheme requires only a short exchange to determine if the page needs to be redelivered from the server, then based on the return data the update request could be made if necessary. If you pipeline both of the requests, you effectively negate the benefits of the cache as you still receive a new copy of the requested page.

References

Rain Forest Puppy. "A look at whisker's anti-IDS tactics" 12/24/99 URL: http://www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html(Sept 5, 2002)

Rain Forest Puppy. "Whisker information, scripts, and updates" May 5, 2002 URL: http://www.wiretrip.net/rfp/p/doc.asp/i7/d21.htm (Sept 5, 2002)

CenterGate Research Group. "Whois Proxy" URL: http://www.geektools.com/cgi-bin/proxy.cgi (Sept 14, 2002)

MAP Data Centre. "Default TTL Values in TCP/IP" Apr 2001 URL: http://www.map.ethz.ch/ftp-probleme.htm - overview (Sept 5, 2002)

Caswell and Roesch. "Snort: the Open Source Network Intrusion Detection System" 2002. URL: http://www.snort.org (Sept 14, 2002)

Detect #2: SNMP public access udp

Trace Log

[Snort Alert]

```
[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]

[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]

[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]

[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]

[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]

[**] [1:1411:2] SNMP public access udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0013]
```

[End Snort Alert]

[Snort Full Packet Log]

```
[**] SNMP public access udp [**]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E8 00 00 70 11 A8 2F 44 0A 7E C9 00 00  .i4...p../D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
```

```
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

[**] SNMP public access udp [**]
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E9 00 00 70 11 A8 2E 44 0A 7E C9 00 00  .i4...p...D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

[**] SNMP public access udp [**]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E8 00 00 70 11 A8 2F 44 0A 7E C9 00 00  .i4...p../D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

[**] SNMP public access udp [**]
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E9 00 00 70 11 A8 2E 44 0A 7E C9 00 00  .i4...p...D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

[**] SNMP public access udp [**]
09/06-14:56:26.706112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13544 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E8 00 00 70 11 A8 2F 44 0A 7E C9 00 00  .i4...p../D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

[**] SNMP public access udp [**]
```

```
09/06-14:56:32.726112 68.10.126.201:1027 -> XXX.YYY.ZZZ.96:161
UDP TTL:112 TOS:0x0 ID:13545 IpLen:20 DgmLen:105
Len: 85
0x0000: 00 02 17 C3 78 1C 00 60 83 65 BF 20 08 00 45 00  ....x..`.e. ..E.
0x0010: 00 69 34 E9 00 00 70 11 A8 2E 44 0A 7E C9 00 00  .i4...p...D.~..9
0x0020: 00 00 04 03 00 A1 00 55 85 BC 30 4B 02 01 00 04  )`.....U..0K....
0x0030: 06 70 75 62 6C 69 63 A0 3E 02 01 1B 02 01 00 02  .public.>.......
0x0040: 01 00 30 33 30 0F 06 0B 2B 06 01 02 01 19 03 02  ..030...+.......
0x0050: 01 05 01 05 00 30 0F 06 0B 2B 06 01 02 01 19 03  .....0...+......
0x0060: 05 01 01 01 05 00 30 0F 06 0B 2B 06 01 02 01 19  ......0...+.....
0x0070: 03 05 01 02 01 05 00                             .......

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

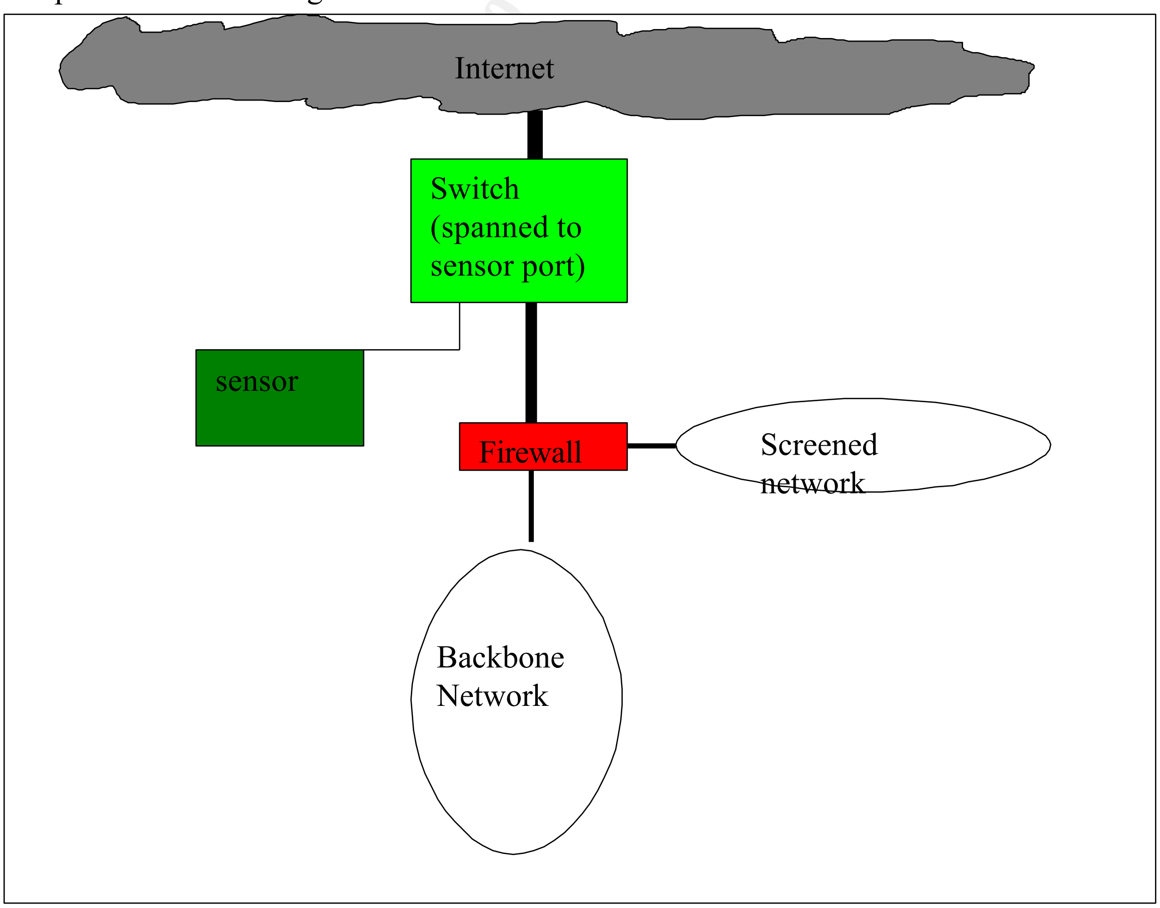
[End Snort Full Packet Log]

Source of Trace

This trace comes from a tcpdump-based tap on my network's DMZ. Data from the tap is analyzed internally using Snort. All of the traffic that enters the site network from the Internet is recorded on this external tap. The data collected by this tap is also the basis for the Shadow IDS which provides an overall picture of the perimeter assault directed at the site networks.

A simplified diagram which shows the placement of the sensor follows.

Simplified Network Diagram



Detect was Generated by

SNORT Version 1.8.4 (Build 99) was used to analyze the log file data.
The triggering signature for this detect is in figure 2.2

Figure 2.2 Snort SNMP public access udp

```
alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP public
access udp"; content:"public"; reference:cve,CAN-2002-0012;
reference:cve,CAN-2002-0013; sid:1411; rev:2;
classtype:attempted-recon;)
```

This rule flags any packet that enters the site network directed at port 161 via the UDP protocol that has the string "public" any where in the data packet. Port 161 is the well-known SNMP server port.

Log format explanation

When run in IDS mode with default logging, Snort creates a directory structure based on the source IP address in which to store the individual packets. The files stored this directory structure are named using protocol and port data gathered from the triggering packet. Each alert also has a summary entry in an alerts file located in the base directory that contains all of the alerts generated over the run period. The two entries generated by this particular event of interest are shown above labeled "Full Packet Log" and "Snort Alert."

The "Snort Alert" is a high level summary of the packet that triggered the alert that consists of data gleaned from the triggering rule and the incoming packet. The first line is an alert label. The first informative field specifies the rule's number and revision. The second field provides a descriptive label for the event, with the first string being a broad categorization of the type of event. This is usually consistent with the rule file in which the triggering rule is found. The second line provides a finer grained classification of the attack, and a priority level. The third line consists of the time stamp at which the IDS sensor saw the packet, and the source and destination IP address with associated source and destination ports. The fourth line indicates the packet's associated protocol, its Time to Live (TTL), type of service (TOS), identification (ID), IP header length (IpLen), and the datagram length (DgmLen). The next lines provide a pointer to further information about the alert.

The "Full Packet Log" is summary information followed by the packet contents in a hexadecimal dump with associated ASCII translation. As in the alert entry, the first line is a descriptive label. The rest is the same following the classification line up through to the data dump.

Probability the Source Address was Spoofed

I suspect that this packet was probably not spoofed. If this were a reconnaissance attempt, the attacker would want to know the results generated by the querying MIB so that they could appropriately direct further attacks.

Also, it turns out that this address resolves to the local address space of the major cable modem access provider. So this packet is beginning to look like a user configuration issue and not an attack, which makes it even less likely that the address was spoofed.

Description of the Attack

SNMP (Simple Network Management Protocol) is a common device management protocol that is often implemented on printers, network devices, and computers to provide remote management and monitoring capabilities. SNMP can allow users access to descriptive information, capabilities, and control points. By default, SNMP uses the strings "public" and "private" to allow read and read/write access respectively to SNMP enabled services. These strings are not encrypted and are well known, and yet they are used like passwords to enable access to the remote device.

At first glance, this seems to be a reconnaissance scan for SNMP device capabilities perhaps to determine if they are susceptible to the wide variety of SNMP vulnerabilities published earlier this year. The attacker is sending some request for information using the default SNMP community string "public" which when enable can allow access to any readable parameter on the remote system.

This is likely a false positive. As mentioned earlier, the source address is from the local broadband provider, and the user directs this query to specific single printer on site. I suspect that this is coming from a laptop computer that the user is moving to and from home, and that there is some lingering printer configuration issue that caused the request to be made. It fails because SNMP services are not passed across the firewall, nor are any printers available from the open internet.

CAN numbers CAN-2002-0012, CAN-2002-0013

Attack Mechanism

Is it a stimulus or response: Stimulus
Affected Service: SNMP
Known Vulnerabilities/Exposures: This packet is directed at an HP printer, which is potentially susceptible to the malformed SNMP packet exploit, which can result in a denial of service. Further, there is a but that can allow a user to send a READ request to a vulnerable printer, and it will return the telnet and administrator password for the embedded web server in HEX format.
Attack Intent: Reconnaissance, this particular packet doe not look to be malformed.

Details: The attacker requests information from the default UDP SNMP port 161 using a known default community string. I cannot find a description of MIBS available for HP printers, so I cannot determine exactly what the user is looking for.

Attacker details:

Whois Info:

```
Server used for this query: [ whois.arin.net ]

Cox Communications Inc. COX-ATLANTA (NET-68-0-0-0-1)
                  68.0.0.0 - 68.15.255.255
Cox Communications, Inc HRRDC-68-10-0-0 (NET-68-10-0-0-1)
                  68.10.0.0 - 68.10.255.255

# ARIN Whois database, last updated 2002-09-13 19:05
# Enter ? for additional hints on searching ARIN's Whois database.
```

Host OS:

The TTL value seems to indicate that this most likely came from a Windows NT 4.0 machine

Correlations

I could not find correlations for either the IP address or the specific data payload in a Google search, nor was there any indications of further activity from this host for the previous fifteen days on my external tap. Also a search on dshield.org revealed nothing. However, there are many indications of attackers using SNMP with default public community strings for network mapping and other detailed reconnaissance.

D. MacLeod saw the following SNMP based probe, which he determined to be a SNMP based scan in his November 2000 analysis.

```
Packet Capture from Network Ice and viewed in ethereal
User Datagram Protocol
   Source port: 2437 (2437)
   Destination port: snmp (161)
   Length: 50
```

Checksum: 0x6e33
Simple Network Management Protocol
Version: 1
Community: **public**
PDU type: GET
Request Id: 0x2539c
Error Status: NO ERROR
Error Index: 0
Object identifier 1: 1.3.6.1.2.1.1.2.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0)
Value: NULL

Evidence of Active Targeting

This collection of packets represents the only connections made to my network from the attacker. All the packets are specifically directed at an internal host, which happens to be an HP printer, so this is definitely active targeting.

Severity

Severity is calculated using the formula:

(Target's Criticality + Attack Lethality) - (System defense + Network defense)

Each element is worth 1 (lowest) to 5 (highest) points

Criticality	In my experience, people get very upset when they can not print, but there are many more printers on site the loss of one is not a show stopper.	**2**
Lethality	This looks like reconnaissance, so it does not harm the printer, but I cannot interpret what the data content is exactly.	**2**
System	This printer could potentially be using the public strings, and it is likely vulnerable to the SNMP denial of service	**1**
Network	Whew! no SNMP traffic allowed through the firewall	**5**

According to the formula, the severity of this detect is -2.

Defensive Recommendation

The first and foremost thing to do is to verify that the site is not permitting SNMP traffic to cross the perimeter, and ensure that default community strings are not being used.

Second, verify whether the printer is vulnerable to the SNMP attacks, and if so apply any applicable patches from the vendor.

Finally, maybe some user support for how to properly configure laptops might be useful to reduce false positives that may stem from computer settings.

Multiple Choice Test Question

Which packet header could provide clues as to the operating system of the attacking machine?

a. Datagram Length
b. Sequence Number
c. Time To Live
d. Destination Port

Answer: (c) Default TTL values vary somewhat, so they can potentially indicate the source operating system.

References

X-Force. "PROTOS Remote SNMP attack tool" Mar 2002. URL: http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise110 (Sept 14 2002)

Caswell and Roesch. "Snort: the Open Source Network Intrusion Detection System" 2002. URL: http://www.snort.org (Sept 14, 2002)

JWS. "TCPDUMP/LIBPCAP" May 2002. URL: http://www.tcpdump.org (Sept 14, 2002)

CenterGate Research Group. "Whois Proxy" URL: http://www.geektools.com/cgi-bin/proxy.cgi (Sept 14, 2002)

MAP Data Centre. "Default TTL Values in TCP/IP" Apr 2001 URL: http://www.map.ethz.ch/ftp-probleme.htm - overview (Sept 5, 2002)

MITRE Corporation. "Common Vulnerabilities and Exposures: The Key to Information Sharing" Sept 2002. URL: http://cve.mitre.org/

Detect #3: WEB-CGI formmail attempt

Trace Log

[ACID Alert Screenshot]

Meta				
	ID #	Time	Triggered Signature	
	1 - 830533	2002-08-30 02:35:39	[bugtraq] [CVE] [arachNIDS] WEB-CGI formmail attempt	
	Sensor	name	interface	filter
		inmon3	any	*none*
	Alert Group	*none*		

IP										
	source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
	172.146.158.142	XXX.YYY.ZZZ.117	4	5	0	1420	10807	0	0	47	11622
	FQDN	Source Name	Dest. Name								
		AC929E8E.ipt.aol.com	AAA.BBB.org								
	Options	*none*									

TCP																
	source port	dest port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
	1564	80				X					903802265	2113999517	5	0	63888	0	33182
	Options	*none*															

[END ACID Alert Screenshot]

[ACID payload]

```
000 : 47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 66 6F 72   GET /cgi-bin/for
010 : 6D 6D 61 69 6C 2E 70 6C 3F 26 65 6D 61 69 6C 3D   mmail.pl?&amp;email=
020 : 54 25 37 32 69 63 25 36 42 73 74 25 36 35 72 25   T%72ic%6Bst%65r%
030 : 34 30 70 69 25 36 44 25 37 30 2E 25 36 33 25 36   40pi%6D%70.%63%6
040 : 46 25 36 44 26 73 75 62 6A 65 63 74 3D 25 32 30   F%6D&amp;subject=%20
050 : 31 35 36 2E 25 32 30 31 32 39 25 32 45 35 37 2E   156.%20129%2E57.
060 : 33 34 2E 25 33 31 31 37 25 32 46 63 67 25 36 39   34.%3117%2Fcg%69
070 : 2D 62 25 36 39 25 36 45 2F 66 6F 72 6D 25 36 44   -b%69%6E/form%6D
080 : 61 69 25 36 43 2E 70 6C 26 72 65 63 69 70 69 65   ai%6C.pl&amp;recipie
090 : 6E 74 3D 6C 73 64 74 72 69 63 6B 73 74 65 72 40   nt=lsdtrickster@
0a0 : 61 6F 6C 2E 63 6F 6D 26 3D 25 34 38 65 79 25 32   aol.com&amp;=%48ey%2
0b0 : 30 25 37 32 65 25 36 44 65 25 36 32 25 36 35 25   0%72e%6De%62%65%
0c0 : 37 32 25 32 30 6D 25 36 35 25 32 30 25 36 39 74   72%20m%65%20%69t
0d0 : 73 25 32 30 25 36 41 65 73 25 37 33 25 32 30 77   s%20%6Aes%73%20w
0e0 : 65 25 36 43 6C 25 32 30 69 25 36 44 25 32 30 62   e%6Cl%20i%6D%20b
0f0 : 25 36 31 25 36 33 6B 25 32 30 25 36 31 6E 64 25   %61%63k%20%61nd%
100 : 32 30 25 36 39 25 32 30 77 61 25 36 45 74 25 36   20%69%20wa%6Et%6
110 : 35 25 36 34 25 32 30 25 37 34 6F 25 32 30 25 36   5%64%20%74o%20%6
120 : 42 6E 6F 25 37 37 25 32 30 69 25 36 36 25 32 30   Bno%77%20i%66%20
130 : 25 37 35 25 32 30 25 37 33 25 37 34 25 36 39 6C   %75%20%73%74%69l
140 : 6C 25 32 30 25 37 37 61 25 36 45 74 65 64 25 32   l%20%77a%6Eted%2
150 : 30 25 37 34 25 36 46 25 32 30 73 65 25 36 35 25   0%74%6F%20se%65%
160 : 32 30 73 6F 25 36 44 65 25 32 30 6E 65 77 25 36   20so%6De%20new%6
170 : 35 25 37 32 25 32 30 70 25 36 39 63 25 37 33 25   5%72%20p%69c%73%
180 : 32 30 25 36 46 66 25 32 30 25 36 44 25 36 39 25   20%6Ff%20%6D%69%
190 : 36 45 65 25 32 30 69 66 25 32 30 25 37 33 6F 25   6Ee%20if%20%73o%
1a0 : 32 30 25 37 34 68 65 6E 25 32 30 25 36 33 6C 69   20%74hen%20%63li
1b0 : 63 25 36 42 25 32 30 6D 25 37 39 25 32 30 25 36   c%6B%20m%79%20%6
1c0 : 43 69 6E 25 36 42 25 32 30 74 6F 25 32 30 6D 79   Cin%6B%20to%20my
1d0 : 25 32 30 73 25 36 39 25 37 34 65 25 32 30 61 25   %20s%69%74e%20a%
1e0 : 36 45 25 36 34 25 32 30 63 25 36 46 6D 65 25 32   6E%64%20c%6Fme%2
1f0 : 30 25 37 33 65 65 25 32 30 6D 6F 72 65 25 32 30   0%73ee%20more%20
```

```
200 : 6F 66 25 32 30 25 36 44 65 25 32 30 62 61 62 25   of%20%6De%20bab%
210 : 37 39 25 32 30 6C 6F 76 65 25 32 30 79 61 25 32   79%20love%20ya%2
220 : 30 4A 65 73 25 37 33 25 32 30 25 32 30 25 32 30   0Jes%73%20%20%20
230 : 3C 25 36 31 25 32 30 25 36 38 72 65 66 25 33 44   &lt;%61%20%68ref%3D
240 : 22 61 6F 6C 25 33 41 2F 25 32 46 31 32 25 33 32   &quot;aol%3A/%2F12%32
250 : 33 3A 25 33 32 36 25 33 32 36 30 25 32 46 25 36   3:%326%3260%2F%6
260 : 38 74 25 37 34 25 37 30 25 33 41 25 35 43 5C 72   8t%74%70%3A%5C\r
270 : 2E 61 6F 6C 2E 63 25 36 46 6D 5C 63 67 69 5C 25   .aol.c%6Fm\cgi\%
280 : 37 32 65 64 25 36 39 72 2D 25 36 33 6F 6D 25 37   72ed%69r-%63om%7
290 : 30 25 36 43 65 78 3F 75 72 25 36 43 25 33 44 68   0%6Cex?ur%6C%3Dh
2a0 : 74 25 37 34 70 3A 2F 25 32 46 77 77 77 25 32 45   t%74p:/%2Fwww%2E
2b0 : 25 25 33 37 34 25 32 35 25 33 34 25 33 35 25 36   %%374%25%34%35%6
2c0 : 25 33 35 25 36 45 25 32 35 35 34 25 25 33 34 35   %35%6E%2554%%345
2d0 : 65 25 36 45 25 37 34 25 36 35 25 34 35 25 32 35   e%6E%74%65%45%25
2e0 : 34 65 25 32 45 25 36 33 6F 6D 25 32 46 2E 73 62   4e%2E%63om%2F.sb
2f0 : 25 36 35 61 6E 3F 25 36 32 65 25 36 31 25 36 45   %65an?%62e%61%6E
300 : 25 33 44 31 25 32 44 30 25 32 44 25 33 33 2D 31   %3D1%2D0%2D%33-1
310 : 25 33 34 39 35 25 33 36 2D 25 33 31 2D 25 33 31   %3495%36-%31-%31
320 : 25 32 44 25 33 31 30 22 25 33 45 25 34 44 79 25   %2D%310&quot;%3E%4Dy%
330 : 32 30 73 69 74 65 25 32 30 25 33 43 2F 61 3E 25   20site%20%3C/a&gt;%
340 : 33 43 25 36 32 25 37 32 25 33 45 25 30 41 25 33   3C%62%72%3E%0A%3
350 : 43 25 36 32 25 37 32 25 33 45 25 33 43 25 36 32   C%62%72%3E%3C%62
360 : 25 37 32 25 33 45 25 33 43 25 36 32 25 37 32 25   %72%3E%3C%62%72%
370 : 33 45 25 35 34 68 69 73 25 32 30 45 25 32 44 25   3E%54his%20E%2D%
380 : 34 44 25 36 31 69 25 36 43 25 32 30 25 36 39 73   4D%61i%6C%20%69s
390 : 25 32 30 6E 25 36 46 25 37 34 25 32 30 25 35 33   %20n%6F%74%20%53
3a0 : 70 25 36 31 6D 2E 25 32 30 25 35 39 6F 75 25 32   p%61m.%20%59ou%2
3b0 : 30 61 72 65 25 32 30 25 36 31 6E 25 32 30 41 25   0are%20%61n%20A%
3c0 : 37 32 25 36 33 68 25 36 39 25 37 36 25 36 35 64   72%63h%69%76%65d
3d0 : 25 32 30 25 34 46 25 37 30 74 2D 69 6E 25 32 30   %20%4F%70t-in%20
3e0 : 53 75 25 36 32 25 37 33 63 72 69 25 37 30 25 36   Su%62%73cri%70%6
3f0 : 35 25 37 32 25 32 30 25 36 36 6F 72 25 32 30 25   5%72%20%66or%20%
400 : 36 46 75 72 25 32 30 44 61 69 6C 25 37 39 25 32   6Fur%20Dail%79%2
410 : 30 4E 25 36 35 25 37 37 73 6C 65 74 74 25 36 35   0N%65%77slett%65
420 : 25 37 32 25 32 30 2A 53 69 6D 70 6C 79 25 32 30   %72%20*Simply%20
430 : 46 72 25 36 35 65 25 32 30 25 35 30 69 25 36 33   Fr%65e%20%50i%63
440 : 74 25 37 35 72 65 73 2A 2E 25 32 30 49 25 36 36   t%75res*.%20I%66
450 : 25 32 30 25 37 39 6F 75 25 32 30 77 69 25 37 33   %20%79ou%20wi%73
460 : 68 25 32 30 74 6F 25 32 30 25 36 32 65 25 32 30   h%20to%20%62e%20
470 : 25 37 32 25 36 35 25 36 44 6F 76 65 64 25 32 30   %72%65%6Doved%20
480 : 66 72 6F 25 36 44 25 32 30 66 75 72 74 68 25 36   fro%6D%20furth%6
490 : 35 72 25 32 30 25 34 35 2D 6D 25 36 31 69 6C 25   5r%20%45-m%61il%
4a0 : 37 33 25 32 43 25 32 30 70 6C 65 61 25 37 33 65   73%2C%20plea%73e
4b0 : 25 32 30 25 37 32 65 70 6C 25 37 39 25 32 30 77   %20%72epl%79%20w
4c0 : 69 25 37 34 68 25 32 30 74 25 36 38 25 36 35 25   i%74h%20t%68%65%
4d0 : 32 30 77 6F 25 37 32 25 36 34 25 32 30 2A 52 45   20wo%72%64%20*RE
4e0 : 25 34 44 4F 56 25 34 35 2A 2E 25 33 43 25 36 32   %4DOV%45*.%3C%62
4f0 : 25 37 32 25 33 45 25 33 43 25 36 32 25 37 32 25   %72%3E%3C%62%72%
500 : 33 45 25 30 41 25 33 43 25 36 32 25 37 32 25 33   3E%0A%3C%62%72%3
510 : 45 25 33 43 25 36 32 25 37 32 25 33 45 20 48 54   E%3C%62%72%3E HT
520 : 54 50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20   TP/1.1..Accept:
530 : 69 6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65   image/gif, image
540 : 2F 78 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67   /x-xbitmap, imag
550 : 65 2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A   e/jpeg, image/pj
560 : 70 65 67 2C                                       peg,
```

[END ACID payload]
[Translated ACID payload]

GET/cgi-bin/formmail.pl?&email=Trickster@pimp.com&subject= 156. XXX.YYY.ZZZ.117/cgi-bin/formmail.pl&recipient=lsdtrickster@aol.com&=Hey remeber me its jess well im back and i wanted to

know if u still wanted to see some newer pics of mine if so then click my link to my site and come see more of me baby love ya Jess My site

This E-Mail is not Spam. You are an Archived Opt-in Subscriper for our Daily Newsletter *Simply Free Pictures*. If you wish to be removed from further E-mails, please reply with the word *REMOVE*.

HTTP/1.1..Accept:image/gif,image/x-xbitmap,image/jpeg,image/pjpeg,

[END Translated ACID payload]

Source of Trace

This trace comes from an ACID console on my local network that is monitoring the site network via a passive sensor just inside the site firewall. If you reference the simplified network diagram above, this sensor would be on the link between the firewall and the backbone network.

Detect was Generated by

ACID version 0.9.6b21

Figure 2.3 WEB-CGI formmail attempt

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-CGI formmail attempt"; flags:A+;
uricontent:"/formmail"; nocase; content:"%0a"; nocase;
reference:bugtraq,1187; reference:cve,CVE-1999-0172;
reference:arachnids,226; classtype:web-application-attack;
sid:1610;  rev:3;)
```

The rule triggered is pretty simple, if an access to the formmail CGI is made during an established session to a web server that contains the string "%0a," trigger this alert. "%0A" is the line feed character.

Log format explanation

ACID provides a web based interface to alert data. The screen shot taken shows the packet header data, packet data contents, and meta-data about the detect. The meta-data includes which sensor saw the alert, the timestamp associated with the detect, and a link to the rule that generated the detect. After the meta-data, the packet headers are displayed in user friendly format. Finally, the packet data associated is displayed in HEX and ASCII format.

Probability the Source Address was Spoofed

The source address associated with this attack was probably not spoofed. The user would need to establish a full session in order to get the response desired from the web server. Likely, the source email address is fake because the spammer probably does not want

email back especially not the vitriolic responses that might be generated based on some of this stuff.

Description of the Attack

This is an exploit of the formmail CGI to bounce SPAM for a pornographic site off our server. Formmail is a public domain PERL script which parses the results of any form, and emails then to a specified user.

The hacker used encoding tricks to hide the exact content of the message, so I had to translate the request from the Unicode encoding scheme to readable text. I presented the translated text with the detect log above.

CVE number CVE-1999-0172

Attack Mechanism

Is it a stimulus or response: Stimulus
Affected Service: CGI
Known Vulnerabilities/Exposures: Formmail 1.6 or less can allow users an anonymous mail message
Attack Intent: SPAM Relay, Social Irritation
Details: The attacker relays a mail message that would seem to originate from my site. To execute this attack the hacker has only to send form data to formmail.pl. Formmail would use the address of the web server as the senders address, and would fill in other mail fields based on data submitted by the hacker. The mail is sent out to the address indicated in the recipient parameter. With this mechanism, the spammer can send out any message anonymously.

Attacker details:

Whois Info:

OrgName: America Online
OrgID: AOL

NetRange: 172.128.0.0 - 172.191.255.255
CIDR: 172.128.0.0/10
NetName: AOL-172BLK
NetHandle: NET-172-128-0-0-1
Parent: NET-172-0-0-0-0
NetType: Direct Allocation
NameServer: DAHA-01.NS.AOL.COM
NameServer: DAHA-02.NS.AOL.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 2000-03-24
Updated: 2002-08-09

TechHandle: AOL-NOC-ARIN
TechName: America Online, Inc.
TechPhone: +1-703-265-4670
TechEmail: domains@aol.net

ARIN Whois database, last updated 2002-09-14 19:05
Enter ? for additional hints on searching ARIN's Whois database.

Host OS:

The TTL value seems to indicate that this most likely came from Linux or SunOS 4.0 box.

Correlations

I could not find correlations for either the IP address or the specific data payload in a Google search. However there are several references to Formmail being used in such a fashion that helps provide anonymity to vile spammers. In addition, the ACID console shows other reconnaissance related alerts for this source IP address.

Here is another example of the exploit from Raj Bhatt's GCIA practical submission. This seems to be more like the reconnaissance, than the spam relay usage in my detect.

172.138.24.237 [08/Dec/2001:21:39:16 +0900] "GET
/cgi-bin/formmail.pl?email=f2%40aol%2Ecom&subject=www%2Eskwea%2Eco%2Ejp%2Fcg
i%2Dbin%2Fformmail%2Epl&recipient=ciphernotcyphr%40aol%2Ecom&msg=w00t

Evidence of Active Targeting

The perpetrator apparently knew the web server address, but not the vulnerabilities on the web server proper. Before the formmail attack was make, the user ran a reconnaissance probe to check the machine for known vulnerable CGI scripts. After the reconnaissance indicated the vulnerability, the attack was actively targeted to the vulnerable script, and that was the end of the activity.

Severity

Severity is calculated using the formula:

(Target's Criticality + Attack Lethality) - (System defense + Network defense)

Each element is worth 1 (lowest) to 5 (highest) points

Criticality	This machine is our primary web server, but we are not an ecommerce or portal, so we could live without the server for a short time.	**4**
Lethality	This attack does not really harm the server, but it can harm our site's reputation, and cause someone some grief. This attack also serves to indicate configuration issues on the primary web server. Finally, I hate spam, especially that which is exploitative of women or young girls.	**4**
System	This server has apparently had no defense against this kind of attack.	**1**
Network	This server is available through the firewall for all web traffic	**1**

According to the formula, the severity of this detect is 6.

Defensive Recommendation

The server configuration for this machine needs to be audited. I suspect that there is no programmatic need for the formmail access, so that script should be removed. If there is a need for the script, there is an upgrade available (version 1.91) that addresses these type of issues associated with formmail.

Multiple Choice Test Question

Attackers can obfuscate data payload using encoding strategies. What does the following string say?

%48a%63%6Be%64%21

a. Help me
b. Hax0r!
c. Sans GCIA
d. Hacked!

Answer: (d) This is standard ASCII/UNICODE encoding

References

CenterGate Research Group. "Whois Proxy" URL: http://www.geektools.com/cgi-bin/proxy.cgi (Sept 14, 2002)

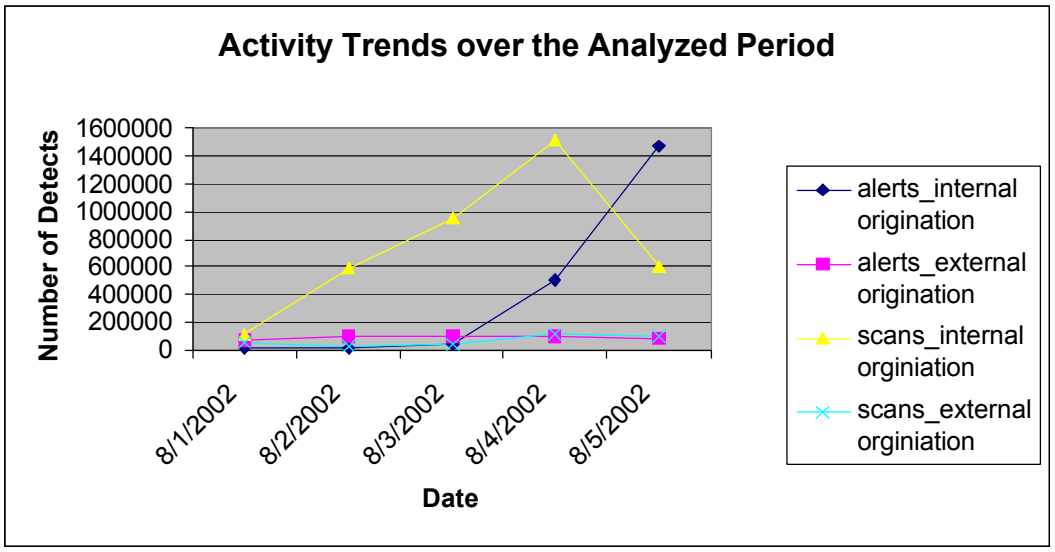
MAP Data Centre. "Default TTL Values in TCP/IP" Apr 2001 URL: http://www.map.ethz.ch/ftp-probleme.htm - overview (Sept 5, 2002)

MITRE Corporation. "Common Vulnerabilities and Exposures: The Key to Information Sharing" Sept 2002. URL: http://cve.mitre.org/

Guilmette and Mason. "Anonymous Mail Forwarding Vulnerabilities in FormMail 1.9" Jan 23, 2002 URL: http://www.monkeys.com/anti-spam/formmail-advisory.pdf (Sept 14, 2002)

Assignment #3: Analyze This!

Executive Summary



The graph above shows a significant number of IDS alerts and scans issued over the course of the period analyzed. Attention is immediately drawn to the dramatic upswing in scans detected over the last two days. With such a large number of base detects, peaks as shown should immediately lead to the suspicion of some mass mailing worm or virus. Other possible factors include the announcement of a new vulnerability or a new exploit. Spikes like that should be investigated immediately. In this case, a significant NIMDA infection and some undetermined infector have been found on two primary site web servers.

In addition to discovering several significant machine compromises, the analysis of the University's network illustrated the need for several items of note. First, the patches for the most frequently detected alerts have been available for some time, but the University machines can still be infected. This argues for a need for better configuration management, especially of web servers. Secondly, the perimeter does not comply with industry best practices in ingress and egress filtering. This includes filters on non-routable IP addresses as well as protocol traffic related to Microsoft networking and RPC. Finally, there is some evidence that the University should evaluate its acceptable use policy, and educate the users as necessary.

Logs Analyzed

This report is based on three sets of log files containing header data for alerts, scans, and out of specification packets. These files covered the period of August 1, through August 5, 2002.

The log files provided for analysis are listed in figure 3.1.

Figure 3.1: Files Used for Analysis

Filename
alert.020801
alert.020802
alert.020803
alert.020804
alert.020805
scans.010801
scans.010802
scans.010803
scans.010804
scans.010805
oos_Aug.1.2002
oos_Aug.2.2002
oos_Aug.3.2002
oos_Aug.4.2002
oos_Aug.5.2002

The data files for each time period were combined into one file covering each type of event. This was done so that trends over the course of the five days could be determined.

Most Frequent Events (Generated More than 10,000 Times)

There were 2,236,823 events detected by the University's intrusion detection system over the course of the five days in the sample period analyzed. That indicates an average of approximately 5.2 events of interest flagged every second of the evaluated period. This is clearly too much information for an analyst to deal with effectively.

The overall goal of this analysis is to help determine what can be improved in terms of intrusion detection system's rule set configuration, or the perimeter defenses of the University's network. This will help significant events of interest be identified and corrected in a timely fashion. The analysis should also highlight the most significant of those events of interest detected over the analyzed period.

The alerts in the below were reported more than 10,000 times over the investigated period. These could indicate a massive attack on the University's network, some configuration issue with the site networking hardware or user machines, or a too general triggering rule. These are the best place to start whittling down the information bombarding the analysts.

Table 3.1: Alerts Reported More Than 20,000 Times

Reported Occurrences	Alert Message
877,538	NIMDA – Attempt to execute cmd from campus host
494,119	spp_http_decode: IIS Unicode attack detected
482,402	IDS552/web-iis_IIS ISAPI Overflow ida INTERNAL nosize
123,305	NIMDA – Attempt to execute root from campus host
106,883	UDP SRC and DST outside network
53,562	spp_http_decode: CGI Null Byte attack detected
30,083	SMB Name Wildcard
24,220	TFTP – External UDP connection to internal tftp server

Table 3.2: Scans Reported More Than 20,000 Times

Reported Occurrences	Alert Message
3,088,442	UDP scan (Internal Origination)
673,848	SYN scan (Internal Origination)
322,537	SYN scan (External Origination)
24,021	UDP scan (External Origination)

Frequent Alert Details

NIMDA – Attempt to execute cmd from campus host Reported: 877,538 times

```
08/05-23:58:58.637510 [**] NIMDA - Attempt to execute cmd from campus host [**] 130.85.100.208:3855 ->
130.220.31.85:80
```

Summary: NIMDA is a well-known worm that has multiple propagation techniques including the exploitation Microsoft's IIS web server using the Unicode Web Traversal exploit, in addition to taking advantage of any host previously compromised with the CodeRed worm.

Here it looks like the University has created a Snort rule to specifically monitor for internal NIMDA infestations.

There are ten campus hosts which have been flagged by this detect, they are listed in figure 3.2. One of the hosts, 130.85.100.208, is responsible for 110,298 of the alerts.

Figure 3.2 NIMDA HOSTS

Host
130.85.82.87
130.85.70.16
130.85.83.176

130.85.111.30
130.85.165.19
130.85.70.169
130.85.70.144
130.85.105.10
130.85.130.20
130.85.100.208

Recommendations: Because NIMDA leaves the machine open for a remote administrative login, these hosts should be removed from the network and rebuilt completely. That rebuild should include patching the machines with the appropriate security bundle to ensure that they cannot become infected again. In addition, the University should remind the users about the propagation of such mass mailing worms so that they do not help to spread them.

spp_http_decode: IIS Unicode attack detected Reported: 494,119 times

08/05-23:58:58.637510 [**] spp_http_decode: IIS Unicode attack detected [**] 130.85.100.208:3855

Summary: A variety of the most common worms (e.g. NIMDA, CodeRed, etc.) use tricks involving Unicode character encoding to move around the file system of a remote machine. There is no legitimate reason for these encoding techniques, so all of these are exploit attempts of some kind.

These alerts stem from 566 unique source addresses. Of those source addresses, 230 are internal to the University's network space. This implies that the University is hosting some of these worms, or there are hackers present on the site attempting to take advantage of un-patched web servers. The attacks detected are directed at the University's network and by hosts on the University's network. These detects need to be addressed immediately as the University is attacking other systems, which is not generally good for the site's reputation.

Figure 3.3 Internal Hosts triggering the IIS Unicode Attack Rule

HOST IP Address

130.85.10.31	130.85.88.78	130.85.153.71
130.85.10.86	130.85.88.137	130.85.153.105
130.85.10.175	130.85.88.143	130.85.153.109
130.85.15.179	130.85.88.151	130.85.153.110
130.85.15.212	130.85.88.220	130.85.153.111
130.85.15.222	130.85.90.43	130.85.153.114
130.85.17.54	130.85.90.59	130.85.153.116
130.85.18.30	130.85.91.16	130.85.153.117
130.85.18.36	130.85.91.26	130.85.153.118
130.85.53.35	130.85.91.53	130.85.153.119
130.85.53.36	130.85.91.62	130.85.153.120
130.85.53.37	130.85.91.91	130.85.153.121
130.85.53.42	130.85.91.95	130.85.153.122
130.85.53.45	130.85.91.97	130.85.153.123
130.85.53.46	130.85.91.100	130.85.153.124
130.85.53.47	130.85.91.101	130.85.153.141
130.85.53.51	130.85.91.103	130.85.153.142
130.85.53.54	130.85.91.104	130.85.153.143
130.85.53.55	130.85.91.105	130.85.153.145
130.85.53.59	130.85.91.106	130.85.153.146
130.85.53.60	130.85.91.160	130.85.153.150
130.85.53.67	130.85.99.165	130.85.153.152
130.85.53.120	130.85.100.208	130.85.153.153
130.85.53.146	130.85.104.49	130.85.153.154
130.85.53.147	130.85.104.141	130.85.153.159
130.85.53.160	130.85.105.19	130.85.153.160
130.85.53.175	130.85.105.22	130.85.153.162
130.85.53.177	130.85.106.176	130.85.153.163
130.85.53.189	130.85.107.141	130.85.153.165
130.85.55.93	130.85.108.46	130.85.153.167
130.85.70.42	130.85.109.11	130.85.153.168
130.85.70.50	130.85.109.13	130.85.153.176
130.85.70.101	130.85.109.26	130.85.153.177
130.85.70.232	130.85.109.77	130.85.153.180
130.85.80.96	130.85.109.83	130.85.153.184
130.85.80.134	130.85.110.52	130.85.153.185
130.85.80.143	130.85.110.139	130.85.153.186
130.85.80.159	130.85.110.224	130.85.153.188
130.85.81.37	130.85.110.227	130.85.153.189
130.85.83.95	130.85.111.30	130.85.153.190
130.85.83.131	130.85.111.145	130.85.153.191
130.85.83.146	130.85.111.173	130.85.153.193
130.85.83.189	130.85.111.196	130.85.153.194
130.85.83.247	130.85.111.204	130.85.153.195
130.85.84.5	130.85.111.213	130.85.153.196
130.85.84.141	130.85.111.221	130.85.153.197
130.85.84.142	130.85.111.222	130.85.153.205
130.85.84.145	130.85.111.225	130.85.153.206
130.85.84.147	130.85.113.4	130.85.153.211
130.85.84.167	130.85.115.66	130.85.157.105
130.85.84.180	130.85.115.132	130.85.157.108
130.85.84.185	130.85.115.186	130.85.158.75
130.85.84.188	130.85.116.37	130.85.162.22
130.85.84.190	130.85.116.52	130.85.162.68
130.85.84.194	130.85.116.84	130.85.162.91
130.85.84.195	130.85.130.73	130.85.162.156
130.85.84.202	130.85.130.132	130.85.168.167
130.85.84.203	130.85.140.79	130.85.168.177
130.85.84.213	130.85.140.143	130.85.168.231
130.85.84.216	130.85.140.196	130.85.178.57
130.85.84.233	130.85.143.107	130.85.178.78
130.85.84.239	130.85.145.27	130.85.178.119
130.85.84.245	130.85.145.215	130.85.178.137
130.85.84.249	130.85.146.94	130.85.178.181
130.85.84.250	130.85.150.97	130.85.180.10

Correlations: Brian Coyle reports similar activity on the University's network in his analysis of April 2001 traffic. Even then, 32 addresses originated inside the University's network.

From Brian's Report:

> 04/01-01:54:56.247338 [**] spp_http_decode: IIS Unicode attack detected [**] 130.87.17.168:1718 -> MY.NET.150.195:80

Recommendations: For the detects originating internally, those machines need to be completely rebuilt, as there is no way to easily determine the degree of compromise. The rebuild should include an evaluation of the site's configuration management to ensure that the patches required to protect the web servers from known malware are applied consistently, and to evaluate other protection issues. Those other issues include possibly switching to a less insecure server, like Apache, and ensuring that development and operational server installations are separate, and possibly installing the base operating system on a different volume than the web server. In addition, this type of traffic should be restricted internally and externally at the perimeter.

IDS552/ISAPI Overflow ida INTERNAL nosize Reported 482,402

> 08/04-19:29:34.123055 [**] IDS552/web-iis_IIS ISAPI Overflow ida INTERNAL nosize [**] 130.85.84.234:3287 -> 200.42.134.111:80

Summary: This is another example of a common and frequent attempt to compromise an IIS web server again probably one of the common worms. In this case, the attacker is attempting to exploit an unchecked buffer in the Index Server ISAPI Extension that can allow them to attain privileged access to the server. Each of these detects represents an attack on some system. In this case, it looks as if the University has created a rule to specifically detect these attacks originating on the University's network.

All of these reported attacks came from one machine on site, 130.85.84.234.

Correlations: This is a very common attack. Here is a partial packet dump snipped from a detect submitted by David Leadston to the intrusions@incidents.org mail list. It shows the signature overflow attempt.

> [**] [1:1243:6] WEB-IIS ISAPI .ida attempt [**]
> [Classification: Web Application Attack] [Priority: 1]
> 06/18-02:30:02.434488 213.81.216.58:3979 -> 46.5.180.133:80
> TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:1504
> ***AP*** Seq: 0xB1ADC0B0 Ack: 0xFA21A80D Win: 0x7D78 TcpLen: 20
> [Xref => http://www.whitehats.com/info/IDS553]

```
02:30:02.434488 213.81.216.58.3979 > 46.5.180.133.80: P
2980954288:2980955752(1464) ack 4196509709 win 32120 [tos 0x
0x0000   4510 05e0 0000 0000 f006 0000 d551 d83a      E.............Q.:
0x0010   2e05 b485 0f8b 0050 b1ad c0b0 fa21 a80d      .......P.....!..
0x0020   5018 7d78 0000 0000 4745 5420 2f64 6566      P.}x....GET./def
0x0030   6175 6c74 2e69 6461 3f4e 4e4e 4e4e 4e4e      ault.ida?NNNNNNN
0x0040   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0050   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0060   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0070   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0080   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0090   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00a0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00b0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00c0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00d0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00e0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x00f0   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0100   4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e 4e4e      NNNNNNNNNNNNNNNN
0x0110   4e4e 4e4e 4e4e 4e4e 4e00 0000 0000 0000      NNNNNNNNN.......
0x0120   0000 0000 0000 0000 c303 0000 0078 00fa      .............x..
```

<Snip>

Gregory Lajon also saw this type of traffic to the University's network in his analysis of the August 14-18 2001. In his analysis, this detect accounted for over 34% out of 780,000 detects, all of these were from external hosts at that time.

Recommendations: Clean the worm from this host! Again, this host should be treated as thoroughly compromised, and have the operating system completely installed. This type of traffic should be including in the ingress and egress restrictions at the perimeter.

NIMDA- Attempt to execute root from campus host Reported 123,305

```
08/05-23:58:56.130269 [**] NIMDA - Attempt to execute root from campus host [**] 130.85.100.208:3517 ->
130.71.236.111:80
```

Summary: This is an example of the NIMDA worm attempting to take advantage of a vulnerability that was left as a result of a machine's compromise by the CodeRed worm variants. Again, this is a very common attack on an IIS based web server.

All of these reported attacks came from one machine on site, 130.85.100.208 which is also a primary generator of the "NIMDA-Attempt to execute cmd from campus host" as well as the "spp_http_decode: IIS Unicode attack detected" alerts, as well as a source for the most significant scan detects as indicated below.

Recommendations: The recommendations are the same as above.

UDP SRC and DST outside network Reported: 106,883 times

```
08/04-16:46:51.741193 [**] UDP SRC and DST outside network [**] 192.168.1.101:1085 -> 68.34.76.5:53
08/05-23:58:38.405380 [**] UDP SRC and DST outside network [**] 3.0.0.99:137 -> 10.0.0.1:137
08/02-11:01:16.843590 [**] UDP SRC and DST outside network [**] 169.254.145.84:123 -> 207.46.226.34:123
```

08/01-02:59:15.489792 [**] UDP SRC and DST outside network [**] 128.223.147.216:1346 -> 229.55.150.208:1345

Summary: The majority of the traffic being picked up by this rule is just noise. Specifically, if the site allows the use of Multicast traffic, then nearly 55% of this traffic is related to Multicast. The rest seems to be the results of bad user machine configuration. Either the users are using reserved (supposedly) non-routed IP space (192.168.0.0/16, etc.), or they have the address assigned by default when an attempt to connect via DHCP fails (address 169.x.x.x).

Correlations: James Hoover saw similar traffic patterns, with 13,345 detects, in his analysis, December 23, 2001.

11/02-08:01:51.280055 [**] UDP **SRC and DST outside network** [**] **3.0.0.99**:137 -> 10.0.0.1:137

Recommendations: Tune the rule to ignore the Multicast network space (224.0.0.0 – 239.255.255.255), if Multicast is permitted on the network.

For the rest, have the network team chase down the ports associated with the users who have mis-configured their networking and straighten them out. Furthermore, you should consider evaluating your network equipment to not route such traffic.

In addition, you might give some emphasis on user education about DHCP, private addressing, and the perils of just punching in numbers.

spp_http_decode: CGI Null Byte attack detected Reported: 53,526 times

08/01-09:11:18.346129 [**] spp_http_decode: CGI Null Byte attack detected [**] 130.85.70.48:2572 -> 216.241.219.28:80

Summary: This alert is triggered when the encoded NULL character (%00) is found in a packet's contents. This character is commonly used for padding in overflow attacks, but is also shows up frequently in binary data and data encoded via SSL. There is no way to determine the intent of these packets without looking at the packet contents, which are not available for this analysis.

Recommendations: Examine the packets to determine is there is any condition under which you can limit the triggering of this alert. You should be able to ignore any connection going to an SSL enable web server.

SMB Name Wildcard Reported: 30,083 times

08/05-23:58:17.330053 [**] SMB Name Wildcard [**] 66.156.162.106:137 -> 130.85.145.247:137

Summary: Port 137 is used for NetBIOS name resolution and is traffic that is normal on corporate networks running Microsoft operating system products. This rule has only

tagged connections to port 137 that originate outside the University's address space.

Correlations: Tod Beardsley saw similar traffic in March 2001; only then, it was mainly internal traffic generating the alerts. He suggested it should only trigger on external sources.

Recommendations: The rule is fine, but it is generally considered good practice not to let this sort of traffic cross a site's perimeter. I suggest blocking it if possible.

TFTP External UDP connection to internal tftp server Reported: 24220 times

> 08/01-00:07:11.963426 [**] TFTP - External UDP connection to internal tftp server [**] 130.85.109.105:69 -> 192.168.0.216:9695

Summary: This rule seems to trigger on the source host communication originating from port 69. Port 69 is associated with the Trivial File Transfer Protocol (tftp). Tftp is often used to transfer configuration files to network devices or devices that boot remotely. Tftp is an insecure protocol.

In this case, all of the detects are for one host 192.168.0.216. This is a false positive. The IP address being flagged as an external host is most likely a mis-configured host on the University's network. It is configured to use a private non-routable address.

Recommendations: The machine using the "192.168" address needs to be configured with the correct assigned IP address.

Frequent Scan Details

UDP Scan (Internal Origination) **Reported: 3,088,442 times**

Top 3 Scanners

130.85.70.200 2,437,164 events

Aug 5 11:07:31 130.85.70.200:4946 -> 18.241.0.138:41170 UDP
Aug 5 11:07:31 130.85.70.200:4946 -> 68.34.227.112:41170 UDP

130.85.70.207 137,226 events

Aug 1 00:33:33 130.85.70.207:12203 -> 216.195.9.63:24148 UDP
Aug 1 00:33:32 130.85.70.207:12300 -> 4.41.76.87:2070 UDP
Aug 1 00:33:32 130.85.70.207:12300 -> 4.41.76.87:2156 UDP

130.85.82.2 127,725 events

Aug 3 08:20:22 130.85.82.2:12203 -> 172.179.228.126:1285 UDP
Aug 3 08:20:22 130.85.82.2:12203 -> 213.114.52.204:3065 UDP

Summary: These are the top three scans UDP scans originating on the University's network.

The first set appears to be a user participating on the Blubster peer-to-peer music-sharing network. This type is identified by UDP connections to port 41170. This scan represents 78% of the internally originating UDP scans!

The second two sets of scans have very similar source ports, but no specific destinations. It looks as if they may be hosting the in.amdq Trojan. The in.amdq has been documented as being delivered with a rootkit known to take advantage of Bind vulnerabilities. It starts a listening service on port 12300, and from that service, a hacker may be directing network scans. A look at the traffic (and the machines) should prove enlightening.

Recommendation: If the University's usage policy prohibits peer-to-peer file sharing applications, then an administrator should visit the owner of 130.85.70.200, and help uninstall Blubster. If the University allows such activity, this is just noise.

The second two scans are a problem. Either the machines hosting them have been rooted, are hosting a virus, or there are malicious users on site. Those machines should be removed from the network for complete analysis. There is no legitimate reason for machines to display that kind of behavior.

SYN Scan (Internal Origination) Reported: 673,848 times

Top 3 Scanners

130.85.84.234 478,419 events

Aug 4 17:30:00 130.85.84.234:4724 -> 156.89.231.106:80 SYN ******S*
Aug 4 17:30:00 130.85.84.234:4737 -> 160.193.184.87:80 SYN ******S*
Aug 4 17:30:00 130.85.84.234:4740 -> 188.146.27.103:80 SYN ******S*

130.85.100.208 170,142 events

Aug 5 21:21:55 130.85.100.208:2021 -> 130.95.40.191:80 SYN ******S*
Aug 5 21:21:55 130.85.100.208:2026 -> 130.7.64.55:80 SYN ******S*
Aug 5 21:21:55 130.85.100.208:2029 -> 130.178.180.123:80 SYN ******S*

130.85.137.7 4,217 events

Aug 1 00:26:58 130.85.137.7:3497 -> 208.45.133.107:25 SYN ******S*
Aug 1 00:27:00 130.85.137.7:3505 -> 64.4.49.7:25 SYN ******S*
Aug 1 00:27:00 130.85.137.7:3513 -> 204.183.84.130:80 SYN ******S*

Summary: The first two scans represent 98% of this category of scan. Unfortunately, both scans are indicative of some sort of machine compromise. In addition, both of these hosts are flagged as significant alert generators, corroborating the notion that they have been compromised in some fashion.

The third scan also indicates similar problems on 130.85.137.7, which appears to be a significant site web server.

Recommendation: These machines need to be thoroughly investigated.

SYN Scan (External Origination) Reported: 322,537 times

Top 3 Scanners

216.228.171.81 25,015 events

Aug 1 06:00:05 216.228.171.81:3089 -> 130.85.10.220:139 SYN ******S*
Aug 1 06:00:05 216.228.171.81:3107 -> 130.85.10.229:139 SYN ******S*
Aug 1 06:00:05 216.228.171.81:3106 -> 130.85.10.229:445 SYN ******S*

24.138.61.171 21,020 events

Aug 4 17:30:48 24.138.61.171:2050 -> 130.85.10.0:80 SYN ******S*
Aug 4 17:30:46 24.138.61.171:2020 -> 130.85.10.5:80 SYN ******S*
Aug 4 17:30:46 24.138.61.171:2021 -> 130.85.10.6:80 SYN ******S*

161.132.205.100 20,329 events

Aug 5 02:24:31 161.132.205.100:4645 -> 130.85.5.83:80 SYN ******S*
Aug 5 02:24:31 161.132.205.100:4649 -> 130.85.5.87:80 SYN ******S*
Aug 5 02:24:31 161.132.205.100:4661 -> 130.85.5.99:80 SYN ******S*

Summary: These represent common scan patterns. The first is scanning for Microsoft Window's based services, and the second two are searching for vulnerable web services of some kind.

Recommendation: The University might consider keeping a scanners list and contacting responsible parties where possible. It might also be prudent to

explicitly block scanners at the perimeter.

UDP Scan (External Origination) Reported: 24,021 times

Top 3 Scanners

205.188.228.17 6,605 events

Aug 1 10:45:02 205.188.228.17:20226 -> 130.85.182.15:6970 UDP
Aug 1 10:45:02 205.188.228.17:13074 -> 130.85.145.166:6970 UDP
Aug 1 10:45:02 205.188.228.17:28720 -> 130.85.151.85:6970 UDP

205.188.288.129 4,238 events

Aug 1 11:00:31 205.188.228.129:24642 -> 130.85.182.56:6970 UDP
Aug 1 11:00:32 205.188.228.129:20932 -> 130.85.90.130:6970 UDP
Aug 1 11:00:32 205.188.228.129:25002 -> 130.85.146.15:6970 UDP

63.241.203.98 2,313 events

Aug 5 07:05:58 63.241.203.98:32168 -> 130.85.117.25:8699 UDP
Aug 5 07:05:58 63.241.203.98:0 -> 130.85.117.25:0 UDP
Aug 5 07:05:58 63.241.203.98:20214 -> 130.85.117.25:13720 UDP

Summary: The first two scans are indicative of a user using a RealAudio service, which is generally on port 6970.

A look at the host information confirms that these look to be some sort of streaming media sources. The host 205.188.288.17 resolves to mslb2.spinner.com, and the host 205.188.228.129 is mslb6.streamops.aol.com.

The other scan is a port scan of the machine 130.85.117.25.

Recommendation: If the University's usage policy allows users to engage in personal entertainment, then the first two scans are just noise. The other is clearly a reconnaissance for future malicious activity.

TOP 5 External Scanners

These are the external scanners who generated the greatest number of scans on the University's network over the period examined. These ISP or responsible parties for the source networks should be contacted about the problem they are generating.

216.228.171.81

```
Bend Cable BENDCABLE (NET-216-228-160-0-1)
                                  216.228.160.0 - 216.228.191.255
bend cable communications BCCI228-DOCSIS (NET-216-228-168-0-1)
                                  216.228.168.0 - 216.228.172.255
```

24.138.61.171

```
OrgName:    Access Cable Television
OrgID:      ACCA

NetRange:   24.138.0.0 - 24.138.79.255
CIDR:       24.138.0.0/18, 24.138.64.0/20
NetName:    ACCESS-BLK1
NetHandle:  NET-24-138-0-0-1
Parent:     NET-24-0-0-0-0
NetType:    Direct Allocation
NameServer: EUROPA.ACCESSCABLE.NET
NameServer: PEGGY.ACCESSCABLE.NET
Comment:
RegDate:    1997-09-05
Updated:    2002-07-24

TechHandle: JP1495-ARIN
TechName:   Potvin, Jeff
TechPhone:  +1-902-469-9540
TechEmail:  jpotvin@accesscable.com
```

161.132.205.100

```
OrgName:    Red Cientifica Peruana
OrgID:      RCP

NetRange:   161.132.0.0 - 161.132.255.255
CIDR:       161.132.0.0/16
NetName:    RCP
NetHandle:  NET-161-132-0-0-1
Parent:     NET-161-0-0-0-0
NetType:    Direct Allocation
NameServer: ICHU.RCP.NET.PE
NameServer: NS.RCP.NET.PE
Comment:
RegDate:    1992-08-24
Updated:    2002-01-10

TechHandle: ET45-ARIN
TechName:   RCP, Operador
TechPhone:  +51-1-2415689
TechEmail:  operador@rcp.net.pe
```

211.232.192.153

```
# ENGLISH
```

```
KRNIC is not ISP but National Internet Registry similar with APNIC.
Please see the following end-user contacts for IP address
information.

IP Address          : 211.232.192.0-211.232.192.255
Network Name        : CABLELINE-CATV
Connect ISP Name    : CABLELINE
Connect Date        : 20020304
Registration Date   : 20020510

[ Organization Information ]
Orgnization ID      : ORG243712
Org Name            : BANDOCABLELINE
State               : CHONBUK
Address             : 906-3 Inhu1dong Dukjin-ku
Zip Code            : 561-230

[ Admin Contact Information]
Name                : Jehong Jung
Org Name            : BANDOCABLELINE
State               : CHONBUK
Address             : 906-3 Inhu1dong Dukjin-ku
Zip Code            : 561-230
Phone               : +82-63-900-9000
Fax                 : +82-63-900-9000
E-Mail              : catv@catvnet.co.kr

[ Technical Contact Information ]
Name                : Byungduk Kim
Org Name            : BANDOCABLELINE
State               : CHONBUK
Address             : 906-3 Inhu1dong Dukjin-ku
Zip Code            : 561-230
Phone               : +82-63-900-9000
Fax                 : +82-63-900-9000
E-Mail              : ip@cableline.com
```


67.104.84.142

```
OrgName:    XO Communications
OrgID:      XOXO

NetRange:   67.104.0.0 - 67.105.255.255
CIDR:       67.104.0.0/15
NetName:    XOXO-BLK-17
NetHandle:  NET-67-104-0-0-1
Parent:     NET-67-0-0-0-0
NetType:    Direct Allocation
NameServer: NAMESERVER1.CONCENTRIC.NET
NameServer: NAMESERVER2.CONCENTRIC.NET
NameServer: NAMESERVER3.CONCENTRIC.NET
NameServer: NAMESERVER.CONCENTRIC.NET
Comment:
RegDate:
```

```
Updated:    2002-02-04

TechHandle: DIA-ORG-ARIN
TechName:   DNS and IP ADMIN
TechPhone:  +1-408-817-2800
TechEmail:  hostmaster@concentric.net

OrgAbuseHandle: XCNV-ARIN
OrgAbuseName:   XO Communications, Network Violations
OrgAbusePhone:  +1-989-758-6860
OrgAbuseEmail:  abuse@xo.com

OrgTechHandle: XCIA-ARIN
OrgTechName:   XO Communications, IP Administrator
OrgTechPhone:  +1-703-547-2000
OrgTechEmail:  ipadmin@eng.xo.com
```


Events of Interest: Alerts Concerning Trojan/Rootkit Activity

Table 3.3: Alerts Concerning Trojan/Rootkit Activity

Reported Occurrences	Alert Message
877,538	Nimda – Attempt to execute cmd from campus host
123,305	Nimda – Attempt to execute root from campus host
4113	Possible Trojan server activity
628	High port 65,535 – possible Red Worm traffic
147	Port 55850 tcp – Possible myserver activity – ref. 010313-1
44	Hight port 65535 tcp – possible Red Worm – traffic
18	Port 55850 udp – Possible myserver activity – ref. 010313-1
3	Back Orifice
3	DDOS shaft client to handler

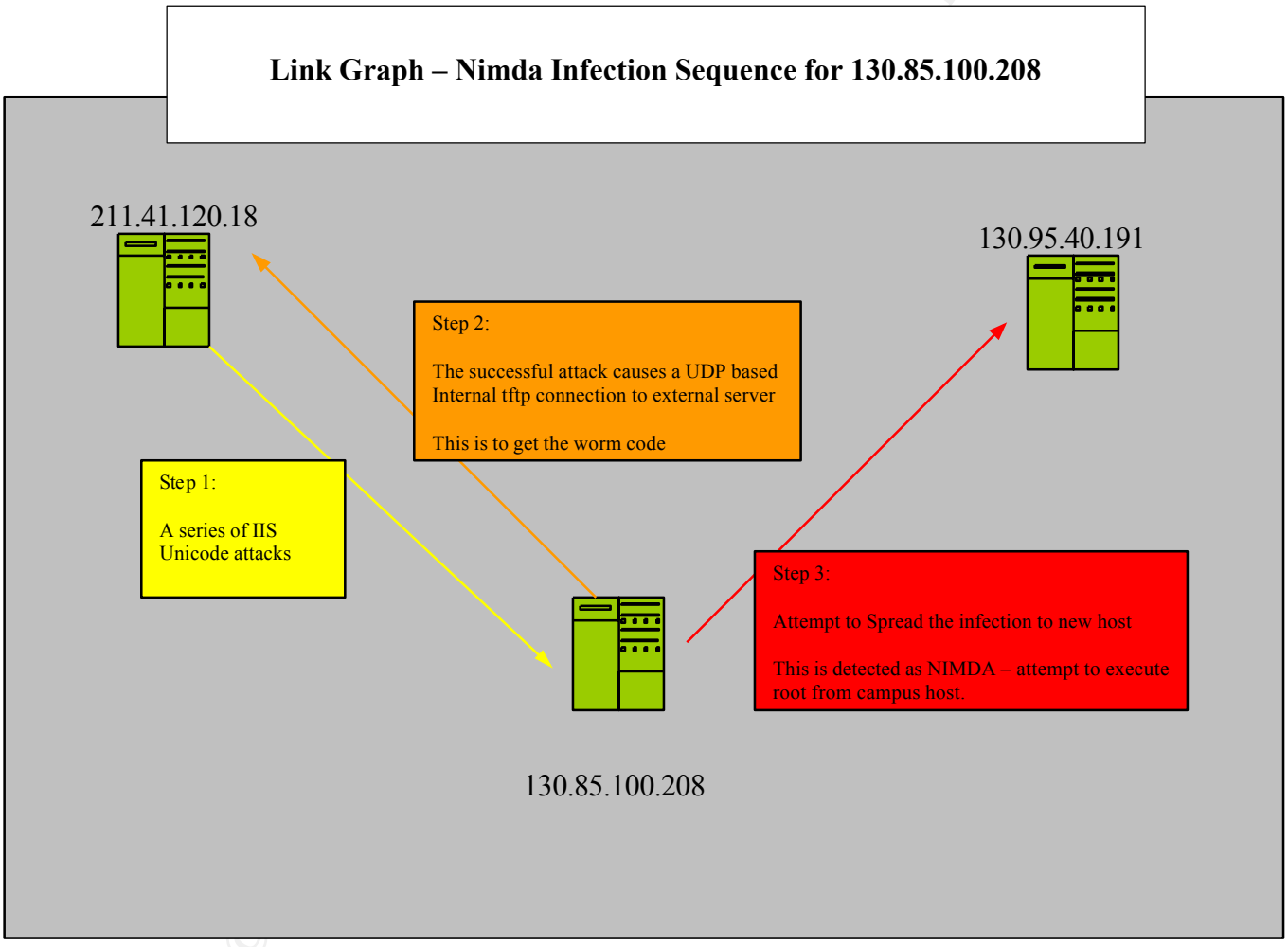
These events all indicate a possibly compromised machine on site, and as such should be a high priority for investigation. Between the activity uncovered in the frequent alert and scan analysis, we can see that the university is currently hosting a significant number of potentially and fully compromised hosts.

Trojan/Rootkit Details

Nimda – Attempt to execute cmd from campus host
Nimda – Attempt to execute root from campus host

Summary: These two detects were discussed in the frequent alerts section of this paper. Each machine listed as generated this detect must be investigated.

The link graph that follows presents the most likely infection sequence of 130.85.100.208 based on the data provided.



Possible trojan server activity

08/01-00:01:17.167418 [**] Possible trojan server activity [**] 24.61.17.248:27374 -> 130.85.11.4:80
08/01-00:01:29.167424 [**] Possible trojan server activity [**] 24.61.17.248:27374 -> 130.85.11.4:80
08/03-09:42:12.333178 [**] Possible trojan server activity [**] 80.220.255.51:27374 -> 130.85.70.113:80

08/05-18:53:16.320629 [**] Possible trojan server activity [**] 63.196.247.234:2625 -> 130.85.85.119:27374
08/05-18:53:17.707355 [**] Possible trojan server activity [**] 63.196.247.234:1473 -> 130.85.85.114:27374

Summary: This is a fairly generic alert that is triggered whenever there is any activity to or from a host on port 27374. The port 27374 is the default listening port for the Linux based Ramen or the Windows based SubSeven Trojan. Since "27374" is a legitimate ephemeral port, this alert can generate significant false alarms.

Here the first set looks like normal web traffic, but the payload should be investigated for the second set.

Correlations: Tod Beardsley investigated similar traffic on the University network in his March 2002 investigation.

High port 65535 udp – possible Red Worm – traffic
High port 65535 tcp – possible Red Worm – traffic

08/02-14:15:50.827572 [**] High port 65535 udp - possible Red Worm - traffic [**] 80.14.16.77:65535 -> 130.85.83.146:6257

08/02-14:46:48.278308 [**] High port 65535 tcp - possible Red Worm - traffic [**] 200.216.52.59:65535 -> 130.85.168.30:1214
08/02-14:46:48.280362 [**] High port 65535 tcp - possible Red Worm - traffic [**] 130.85.168.30:1214 -> 200.216.52.59:65535

Summary: This rule is triggered based on UDP/TCP traffic to port 65535. This traffic is normal web traffic. The first connection is also shown in the Peer-to-peer file sharing traffic as relating to WebMX music sharing. The second set is likely Kazaa based p2p traffic.

Port 55850 tcp – Possible myserver activity – ref. 010313-1
Port 55850 udp – Possible myserver activity – ref. 010313-1

08/01-00:09:20.282660 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 65.200.22.8:55850 -> 130.85.6.40:25
08/01-00:09:20.283132 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 130.85.6.40:25 -> 65.200.22.8:55850
08/01-02:12:16.343268 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 130.85.104.139:55850 -> 152.163.226.89:80
08/01-02

```
08/01-06:03:16.547178 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] 62.2.172.99:55850 -> 130.85.70.207:12300
 08/01-06:03:16.565780 [**] Port 55850 udp - Possible myserver activity - ref. 010313-1 [**] 130.85.70.207:12300 -> 62.2.172.99:55850
```

Summary: This is another port based rule so is subject to a significant false positive rate. The first set looks like normal traffic - communication between the port and a mail server and the port and a web server.

The second set looks like it should be investigated because the port UDP 12300 is associated with a Trojan delivered with a BIND exploit. That is interesting if the University is hosting a myserver DDoS agent which could be controlled by the other machine which might be rooted.

Back Orifice

```
08/02-14:50:30.780519 [**] Back Orifice [**] 212.143.222.236:4019 -> 130.85.70.236:31337
08/05-16:36:39.582295 [**] Back Orifice [**] 63.240.142.227:18672 -> 130.85.117.25:31337
08/05-16:36:39.707788 [**] Back Orifice [**] 63.240.142.227:18672 -> 130.85.117.25:31337
```

Summary: This rule is triggered if there is any connection on port 31337. Since 31337 is a legitimate ephemeral port, it can be encountered in regular traffic.

DDOS shaft to client handler

```
08/03-09:33:49.613574 [**] DDOS shaft client to handler [**] 209.73.180.8:80 -> 130.85.70.161:20432
08/03-09:33:49.666687 [**] DDOS shaft client to handler [**] 209.73.180.8:80 -> 130.85.70.161:20432
08/03-09:33:49.767531 [**] DDOS shaft client to handler [**] 209.73.180.8:80 -> 130.85.70.161:20432
```

Summary: Without further information this is difficult to tell if it is legitimate traffic, or a hacker attempting to hide the connection in regular web traffic.

Top 10 Hosts to investigate

All of the hosts which generated a detect that was not deemed a false positive or routine activity should be investigated. However, the following machines should be given priority investigation based either on the significance of the detect they are associated with or the amount of traffic generated.

Top 10 to Investigate

Host
130.85.84.234
130.85.100.208
130.85.37.7
130.85.6.40
130.85.110.224
130.85.115.11
130.85.178.136
130.85.153.107

130.85.83.247
130.85.84.130

Events of Interest: Out of Spec packets

The traffic that is contained in the OOS files is composed of packets that violate TCP/IP protocols. These alerts can be evidence of corrupt packets, crafted packets, and hosts starting to use External Congestion Notification (ECN), which makes use of the TCP reserved bits.

During the period investigated, there were only two types of packets reported in the Out Of Spec files. The first is likely just a machine using the ECN traffic as you can see by the fact that the reserved bits are set on the SYN packet.

```
08/03-00:15:21.266139 195.101.94.208:4604 -> 130.85.5.96:80
TCP TTL:47 TOS:0x0 ID:19563  DF
21S***** Seq: 0x1B295B8F   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 145299428 0 EOL EOL EOL EOL
```

This host also shows up in the scan files as a SYN scanner with RESERVED BITS, but all of the 61 entries look like regular web server traffic, and there are no other indications that this machine is involved in nefarious activities.

The only suspicious packet was the following.

```
08/04-21:30:35.373910 68.80.114.202:1250 -> 130.85.5.96:80
TCP TTL:108 TOS:0x0 ID:12297  DF
21SF*P*U Seq: 0x5B3064   Ack: 0x2169   Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK
```

This is likely some sort of crafted packet because the flag setting just do not make sense. The SYN and Fin flags are set. An Ack is given, but the Ack flag is not set. This was the only packet this host sent to the University during the time monitored.

User activity Policy issues

During the course of the analysis of the University's network, two distinct activities were noticed which the University should ensure are included in its Appropriate Usage policy. These are the use of peer-to-peer based file sharing programs, and the use of streaming media applications. Usage of these applications can introduce potential legal complications for the University, and they can represent a significant drain on University resources.

The table below indicates hosts on the University's network that seem to be engaging in these types of activities

Gnutella/Kazaa	WebMX	Streaming Media
130.85.70.180	130.85.150.46	130.85.15.22
130.85.80.118	130.85.165.24	130.85.151.70
130.85.84.228	130.85.53.31	130.85.151.105
130.85.87.111	130.85.83.146	130.85.109.62
130.85.88.201	130.85.83.150	
130.85.91.106	130.85.84.130	
130.85.91.181		
130.85.100.158		
130.85.100.224		
130.85.104.104		
130.85.116.68		
130.85.117.137		
130.85.117.150		
130.85.137.18		
130.85.139.51		
130.85.145.247		
130.85.162.251		
130.85.163.107		
130.85.168.82		

Conclusions and Defensive Recommendations

After a significant examination of the data provided by the University, I have drawn three primary conclusions. There is evidence of significant compromise most of an easily preventable nature which may have been prevented with a comprehensive configuration management plan. Significant improvements can be made to the University's network perimeter, and the appropriate usage policy needs to be evaluated.

The indications of a NIMDA infestation are the most significant example of the kind of compromise that is easily preventable. The patches had been available for some time from the vendor, and the publicity surrounding the event should have encouraged site administrators to give this priority. A configuration management program that ensures that patches are applied as they are released and which also ensures that patches are reapplied as machines are rebuilt and modified is in order.

The University has a very open perimeter, and it seems there are far too many machines offering externally accessible web services. Web servers are one of the most commonly attacked classifications of machines, and steps should be taken to reduce the University's exposure where possible. In addition, there are several "best practices" related to routing that the University does not seem to practice. None of the Microsoft OS based protocol ports should be permitted to cross a perimeter. Finally, ingress and egress filtering of non-routable IP addresses should be addressed.

Finally, there were a significant number of detects related to user activities from peer-to-peer file sharing, streaming media, and multicast traffic. The users need to be made aware of the risks associated with such activity if the University is going to permit it.

List of hosts to Investigate

The lists of hosts in the table blow are hosts that were involved in a significant alert detect, or during the course of the investigation of scanning activity there was some evidence of some behavior that needs further investigation.

130.85.10.175
130.85.10.31
130.85.10.86
130.85.100.158
130.85.100.208
130.85.100.224
130.85.104.104
130.85.104.141
130.85.104.49
130.85.105.10
130.85.105.19
130.85.105.22
130.85.106.176
130.85.107.141
130.85.108.46
130.85.109.11
130.85.109.13
130.85.109.26
130.85.109.62
130.85.109.77
130.85.109.83
130.85.110.139
130.85.110.224
130.85.110.227
130.85.110.52
130.85.111.145
130.85.111.173
130.85.111.196
130.85.111.204
130.85.111.213
130.85.111.214
130.85.111.221
130.85.111.222
130.85.111.225
130.85.111.30
130.85.113.4
130.85.115.11
130.85.115.132
130.85.115.186
130.85.115.66
130.85.116.37
130.85.116.52
130.85.116.68
130.85.116.84
130.85.117.137
130.85.117.150
130.85.130.132
130.85.130.20
130.85.130.73
130.85.137.18
130.85.139.51
130.85.139.511
130.85.140.143
130.85.140.196
130.85.140.79
130.85.143.107
130.85.145.215
130.85.145.247
130.85.145.27
130.85.146.55
130.85.146.94
130.85.15.179
130.85.15.212
130.85.15.22
130.85.15.222
130.85.150.103
130.85.150.165
130.85.150.207
130.85.150.46
130.85.150.97
130.85.151.105
130.85.151.18
130.85.151.70
130.85.152.11
130.85.152.170
130.85.152.171
130.85.152.180
130.85.152.184
130.85.152.19
130.85.152.213
130.85.153.105
130.85.153.107
130.85.153.109
130.85.153.110
130.85.153.111
130.85.153.114
130.85.153.116
130.85.153.117
130.85.153.118
130.85.153.119
130.85.153.120
130.85.153.121
130.85.153.122
130.85.153.123
130.85.153.124
130.85.153.141
130.85.153.142
130.85.153.143
130.85.153.145
130.85.153.146
130.85.153.150
130.85.153.152
130.85.153.153
130.85.153.154
130.85.153.157
130.85.153.159
130.85.153.160
130.85.153.162
130.85.153.163
130.85.153.165
130.85.153.167
130.85.153.168
130.85.153.176
130.85.153.177
130.85.153.180
130.85.153.184
130.85.153.185
130.85.153.186
130.85.153.188
130.85.153.189
130.85.153.190
130.85.153.191
130.85.153.193
130.85.153.194
130.85.153.195
130.85.153.196
130.85.153.197
130.85.153.205
130.85.153.206
130.85.153.211
130.85.153.46
130.85.153.71
130.85.157.105
130.85.157.108
130.85.158.75
130.85.162.156
130.85.162.22
130.85.162.251
130.85.162.68
130.85.162.91
130.85.163.107
130.85.163.132
130.85.165.19
130.85.165.24
130.85.168.13
130.85.168.167
130.85.168.177
130.85.168.231
130.85.168.82
130.85.17.54
130.85.178.110
130.85.178.119
130.85.178.136
130.85.178.137
130.85.178.181
130.85.178.57
130.85.178.78
130.85.18.30
130.85.18.36
130.85.180.10
130.85.182.60
130.85.182.91
130.85.182.95
130.85.183.14
130.85.183.25
130.85.183.26
130.85.183.55
130.85.184.40
130.85.190.16
130.85.190.41
130.85.198.12
130.85.37.7
130.85.53.120
130.85.53.146
130.85.53.147
130.85.53.160
130.85.53.175
130.85.53.177
130.85.53.189
130.85.53.31
130.85.53.35
130.85.53.36
130.85.53.37
130.85.53.42
130.85.53.45
130.85.53.46
130.85.53.47
130.85.53.51
130.85.53.54
130.85.53.55
130.85.53.59
130.85.53.60
130.85.53.67
130.85.55.93
130.85.6.40
130.85.70.101
130.85.70.144
130.85.70.16
130.85.70.169
130.85.70.180
130.85.70.232
130.85.70.42
130.85.70.50
130.85.80.118
130.85.80.134
130.85.80.143
130.85.80.159
130.85.80.96
130.85.81.37
130.85.82.87
130.85.83.131
130.85.83.146
130.85.83.150
130.85.83.176
130.85.83.189
130.85.83.247
130.85.83.95
130.85.84.130
130.85.84.141
130.85.84.142
130.85.84.145
130.85.84.147
130.85.84.167
130.85.84.180
130.85.84.185
130.85.84.188
130.85.84.190
130.85.84.194
130.85.84.195
130.85.84.202
130.85.84.203
130.85.84.213
130.85.84.216
130.85.84.228
130.85.84.233
130.85.84.234
130.85.84.239
130.85.84.245
130.85.84.249
130.85.84.250
130.85.84.251
130.85.84.5
130.85.85.53
130.85.85.74
130.85.85.86
130.85.87.111
130.85.87.121
130.85.87.193
130.85.87.37
130.85.87.6
130.85.88.11
130.85.88.137
130.85.88.143
130.85.88.151
130.85.88.201
130.85.88.220
130.85.88.3
130.85.88.5
130.85.88.52
130.85.88.78
130.85.90.43
130.85.90.59
130.85.91.100
130.85.91.101
130.85.91.103
130.85.91.104
130.85.91.105
130.85.91.106
130.85.91.16
130.85.91.160
130.85.91.181
130.85.91.26
130.85.91.53
130.85.91.62
130.85.91.91
130.85.91.95
130.85.91.97
130.85.99.165

References

Eriksson, Hans. "MBONE: The Multicast Backbone". Communications of the ACM 37,8 (August 1994), pp. 54-60.

Roesch, Marty. Yarochkin, Fyoder, et al. "Snort FAQ" March 25, 2002. http://www.snort.org/docs/faq.html#4.12 . (November 19, 2002).

CenterGate Research Group. "Whois Proxy" URL: http://www.geektools.com/cgi-bin/proxy.cgi (Sept 14, 2002)

Caswell and Roesch. "Snort: the Open Source Network Intrusion Detection System" 2002. URL: http://www.snort.org (Sept 14, 2002)

Ahmad, Dave. "Nimda Worm." Security Focus's BugTraq. Sep 18, 2001. URL: http://online.securityfocus.com/archive/1/215177 (November 6, 2002).

Vision, Max. "Re: [snort] 'SMB Name Wildcard.'" Archives.Neohapsis.Com. Jan 17, 2000. URL: http://archives.neohapsis.com/archives/snort/2000-01/0220.html (November 18, 2002).

Red Hat, Inc. "The Ramen Worm – What Red Hat Linux Users Can Do About It." Security & Worm Alerts. URL: http://www.redhat.com/support/alerts/ramen_worm.html (November 18, 2002).

Buchanan. J. "Working around ISP port blocks" (2002) http://homepage.ntlworld.com/j.buchanan/winmx/blocked.html (November 18, 2002)

Blubster. "Client Documentation: Blubster, Connecting to the network." http://www.blubster.net/php/article.php?sid=34 (November 18, 2002)

"Multicast" http://www.tack.ch/multicast/ (November 18, 2002

Appendix A Methodologies

Tools and Methodology

Major platforms, tools, and services used in the analysis include:

- Linux 6.2
- Microsoft Excel 2000
- Snort
- Google (http://www.google.com)
- Geektools (http://www.geektools.com)
- The SANS Institute (http://www.sans.org)
- Snort Signatures Database (http://www.snort.org/snort-db)
- Snort Ports Database (http://www.snort.org/ports.html)
- Whitehats ArachNIDS Database (http://www.whitehats.com/ids/)
- SnortSnarf
- Andrew Baker's snort_sort.pl

In order to analyze the data presented, the first thing I did was to combine all of the individual files into a single file, and remove all of the portscan alerts because they are covered in the scan files. Because the files I was working with did not have the IP addresses obfuscated, I was able to run SnortSnarf on the data. There also seemed to be some issues with the files themselves. There were some detect lines that were not complete, like they had been hand edited and some characters or line ends deleted. Unfortunately, with the quantity of data provided, SnortSnarf was unable to process the files in a timely fashion. I gave up after over 6 days of cpu time passed, and the program was still running using almost 2 GB of memory. I then ran the files with SnortSnarf, only this time just the individual days after having removed all of the NIMDA detects which I also processed separately. That was not as helpful as I had hoped and still took several days to complete. At this point, I used snort_sort.pl to get an overall picture of the data, and made use of the summary data provided by that script.

Beyond that all of the data I processed, I did using system commands and a little utility that sorts IP addresses.
The most useful commands follow:

- % cut –f -d " " filename >
- % cat filename | wc –l
- % ls –lShr
- % sort –u filename >
- vi filename

Had I been more conversant and sensible, I probably would have used a database, because it would have been MUCH faster.

Appendix B complete list of Detects

There were 2,236,823 detects during the five day period covered by the alert logs. The following table presents all of the alert categories for the period ranked in descending order by number of events.

Alert Detects by Descending Frequency

877538	NIMDA - Attempt to execute cmd from campus host	NIMDA uses cmd to exploit other hosts this rule seems to be modified to trigger when "cmd" is seen in outgoing traffic
494119	spp_http_decode: IIS Unicode attack detected	Many worms use Unicode translation at the final host to attempt to exploit IIS
482402	IDS552/web-iis_IIS ISAPI Overflow ida INTERNAL nosize	Code Red Worm attempt to compromise IIS machine via an unchecked buffer
123305	NIMDA - Attempt to execute root from campus host	Code Red and Nimda both exploit web servers using a copy of the command interpreter, which has been renamed root.exe. Presumably, this rule has been tailored to trigger for an on campus host.
106883	UDP SRC and DST outside network	An indication of bad traffic, bad router configuration, or crafted/spoofed packet created on the local network.
53562	spp_http_decode: CGI Null Byte attack detected	Any use of the Unicode null character %00 in a packet destined for a web server
30083	SMB Name Wildcard	Represents NetBIOs name resolution traffic this is usually normal behavior on a local network
24220	TFTP - External UDP connection to internal tftp server	TFTP is an insecure protocol, no external traffic should access TFTP

14578	External RPC call	Traffic to 111 the portmapper port that allows a user to determine what RPC services are running on the machine. RPC programs have many known vulnerabilities. RPC traffic should never pass a perimeter.
11921	Watchlist 000220 IL-ISDNNET-990517	Possibly a local rule to watch for traffic originating on specific subnets?
4113	Possible trojan server activity	Looks for traffic on port 27374 used by SubSeven
2543	SUNRPC highport access!	Looks for successful access to high ports commonly used by RPC programs
2054	IRC evil - running XDCC	IRC is running XDCC bot which can allow access to the machine as administrator
1305	Watchlist 000222 NET-NCFC	This watches traffic from a specific subnet identified by NCFC. There are some indications that this is a Chinese University network.
1293	EXPLOIT x86 NOOP	Potential Binary data or Buffer Overflow attempt in the data payload as NOOPS are often used to pad data.
1120	Queso fingerprint	Queso is a tool used to determine OS of remote hosts.
927	SNMP public access	The data payload for the packet contains the default community string “public” for readable SNMP parameters.
788	Connect to 515 from outside	Port 515 is the LPR server port that has many known vulnerabilities, and should never see traffic from outside the network perimeter.

730	Attempted Sun RPC high port access	Attempted access to a high numbered port which may be used by an RPC program
679	Samba client access	This triggers when external traffic directed internally with the string "|00| UNIX |00| Samba" in the payload. This type of traffic should not cross network perimeters.
628	High port 65535 udp - possible Red Worm - traffic	This is potentially the signature for the Red/Adore worm.
314	IDS552/web-iis_IIS ISAPI Overflow ida nosize	An attempt to gain SYSTEM access to the web server
260	ICMP SRC and DST outside network	A sign of bad router configuration, or spoofed traffic originating on the home network.
236	SMB C access	Attempt to access administrative share on Window's machine
173	TFTP - Internal UDP connection to external tftp server	TFTP traffic should never pass a perimeter because of the insecure nature of the protocol
166	beetle.ucs	UNKNOWN – local rule?
147	Port 55850 tcp - Possible myserver activity - ref. 010313-1	myserver is a DDOS agent which is known to listen on port 55850
136	Incomplete Packet Fragments Discarded	This may be a sign of a set of crafted packets which may be an attempted denial of service
106	Null scan!	This is potentially sign of a crafted packet
88	NMAP TCP ping!	NMAP is a port scanning tool
58	EXPLOIT x86 setuid 0	This may indicated an exploit attempt where the attacker sent a x86 system call for setuid(0) which is the privileged user.

53	Tiny Fragments - Possible Hostile Activity	Tiny fragments can be attempts to hide activity from the IDS
48	EXPLOIT x86 stealth noop	Potential buffer overflow or binary data in the payload
44	High port 65535 tcp - possible Red Worm - traffic	This is potentially a signature for the Red/Adore worm.
42	STATDX UDP attack	An attack on rpc.statd
38	EXPLOIT x86 setgid 0	This may indicated an exploit attempt where the attacker sent a x86 system call for setgid(0) which is the privileged group.
18	Port 55850 udp - Possible myserver activity - ref. 010313-1	myserver is a DDOS agent which is known to listen on port 55850
13	SMB CD...	Possible access of a hidden directory
13	TCP SRC and DST outside network	A sign of bad router configuration, or spoofed traffic originating on the home network
11	130.85.30.4 activity	UNKNOWN – local rule?
11	External FTP to HelpDesk 130.85.70.50	Locally relevant access rules
11	HelpDesk 130.85.70.50 to External FTP	Locally relevant access rules
9	HelpDesk 130.85.70.49 to External FTP	Locally relevant access rules
8	External FTP to HelpDesk 130.85.70.49	Locally relevant access rules
6	TFTP - External TCP connection to internal tftp server	TFTP traffic should never pass a perimeter because of the insecure nature of the protocol
5	EXPLOIT NTPDX buffer overflow	Indicates buffer overflow attempt against NTPD
4	HelpDesk 130.85.83.197 to External FTP	Locally relevant access rules
3	Back Orifice	Potential Trojan activity

3	DDOS shaft client to handler	Inbound access to port 20432 used by shaft DDOS tool for communication
3	RFB - Possible WinVNC - 010708-1	VNC is a remote control tool for Window's desktops
2	SYN-FIN scan!	A packet has been crafted with the SYN and FIN flags set
2	Traffic from port 53 to port 123	Connection from DNS to NTPD
1	130.85.30.3 activity	UNKNOWN – local rule?