Global Information Assurance Certification Paper

SANS Intrusion Detection in Depth

GCIA Practical Assignment

Version 3.0

SANS Darling Harbour, Sydney, Australia.

Jan 19-23 2002

Shane Huntley

Assignment 1 – Grim's Ping Pub Scanner

Grim's Ping http://grimsping.cjb.net/

Introduction

This paper will analyse the ftp scanning tool "Grim's Ping". The capabilities and limitations of the tool will be examined along with the signatures and possible defensive use. Snort IDS rules to monitor both incoming and outgoing Grim's Ping connections will also be provided.

Grim's Ping

Grim's Ping is a Win32 application available from http://grimsping.cjb.net/. The program performs four main functions:

1. Pinging ranges of hosts.
2. Scanning for public ftp directories.
3. Performing port scans.
4. Provision of a basic graphical FTP client

Of the four functions the most commonly used, and the advertised reason for being, is scanning of FTP servers for writable directories. Such directories are of interest as they provide a mechanism for the transfer of illegal software, video and audio files colloquially known as "warez". Sites with large amounts of storage and bandwidth are obviously prime targets but even an unattended machine on a home DSL or cable modem can be used for transfer of smaller illegal files

Detailed Description

Grim's Ping is a Visual Basic application. It has a relatively easy to use graphical user interface. There is no detailed user manual but the website has a tutorial, frequently asked questions (FAQ) and a discussion board. Novice users who are unable to deal with the command line can use the program. Installation is very simple, utilising the standard window's installer. Unlike many command line hacker tools it is easily installed by anyone capable of clicking a mouse. The primary user interface panel is shown overleaf.

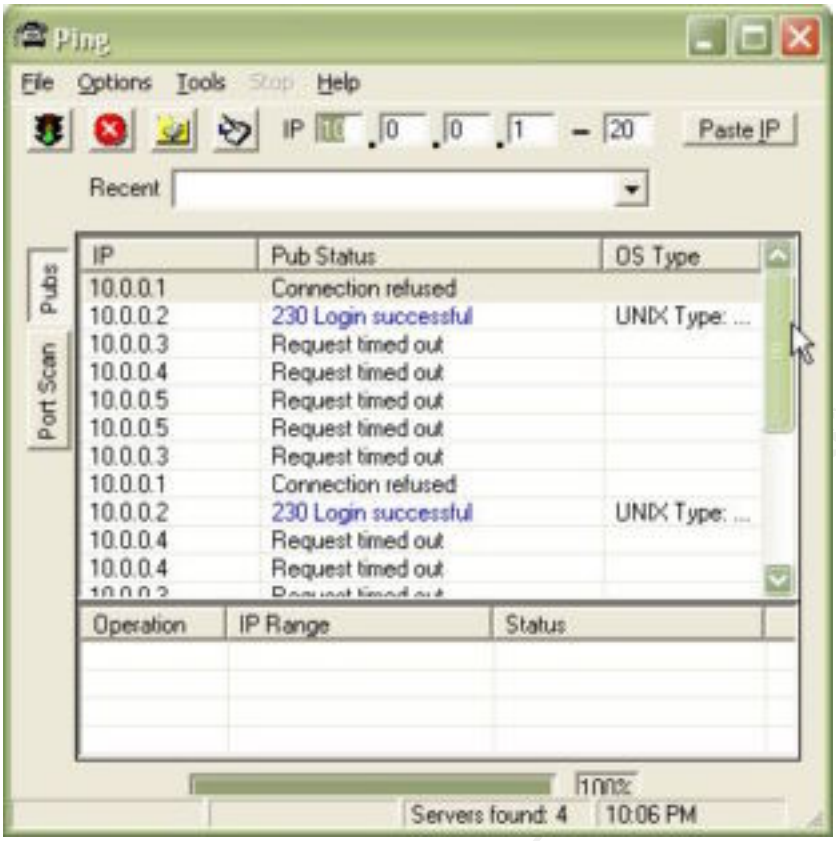


Figure 1 Grim's Ping User Interface

Pinging Ranges of Hosts

Grim's Ping allows the user to automatically ping a range of IP addresses vi the use of ICMP Echo Requests. The IP Range can be entered by the user or there is an option to select a random size of Class C address space. There is a preference dialog box which the parameters of the ICMP Echo Requests can be set. The valid ranges and defaults of those parameters are listed below:

Parameter	Default	Range
Size of Packet (Bytes)	32	1-99
TTL	255	1-255
Ping duration per IP (ms)	2000	1-99999

The size of packet option is similar to the –l option under windows ping or –s under UNIX. The number of bytes is in addition to the IP and ICMP headers which total 28 bytes, so a packet with the default size 32 will result in a 60 byte IP packet.

The following is a packet dump of a ping with default parameters (captured using tcpdump with –vv and –X options)

```
14:09:48.323601 10.0.0.1 > 10.0.0.2: icmp: echo request (DF) (ttl 255, id 34096,
len 60)
0x0000          4500 003c 8530 4000 ff01 e28d 0a00 0001      E..<.0@.........
0x0010          0a00 0002 0800 cb87 0200 3500 8ce8 1700      ..........5.....
0x0020          8c8c 1600 0000 0000 0a00 0002 1100 0000      ................
0x0030          0100 9200 0100 0000 0000 0000                ............
```

For comparison the following is a packet dump for a standard windows XP ping from the same host:

```
14:14:49.206378 10.0.0.1 > 10.0.0.2: icmp: echo request (ttl 128, id 34271, len
60)
0x0000          4500 003c 85df 0000 8001 a0df 0a00 0001      E..<............
0x0010          0a00 0002 0800 0e5c 0200 3d00 6162 6364      .......\..=.abcd
0x0020          6566 6768 696a 6b6c 6d6e 6f70 7172 7374      efghijklmnopqrst
0x0030          7576 7761 6263 6465 6667 6869                uvwabcdefghi
```

And a ping from a Linux (2.4.17) host

```
14:19:09.382022 10.0.0.2 > 10.0.0.1: icmp: echo request (DF) (ttl 64, id 0, len 84)
0x0000          4500 0054 0000 4000 4001 26a7 0a00 0002      E..T..@.@.&.....
0x0010          0a00 0001 0800 228a da08 4600 3c92 b9ad      ......"...F.<...
0x0020          0005 d424 0809 0a0b 0c0d 0e0f 1011 1213      ...$............
0x0030          1415 1617 1819 1a1b 1c1d 1e1f 2021 2223      .............!"#
0x0040          2425 2627 2829 2a2b 2c2d 2e2f 3031 3233      $%&'()*+,-./0123
0x0050          3435                                         45
```

The ICMP Echo request packet from Grim's ping is noticeably different from the other two sample packets due to the 255 TTL and the seemingly random payload. The IP ID and length give the clue that it is in fact still a windows host.

The above information should allow an analyst to make a guess when looking at ping scans as to whether or not they originated from a Grim's Ping client especially if the default parameters of TTL 255, size 32 and one host is pinged every per 2000ms.

For use by a security professional Grim's ping provides little in functionality for pinging of hosts compared to a more thorough command line based tool such as nmap.

Public FTP Directory Scanning

Grim's ping is primarily used to find writable directories. It does this through attempting to log on to the FTP server via anonymous logon. The current version of Grim's Ping uses a FTP password of ?gpuser@home.com (where ? represents a random uppercase letter).

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
03/17-11:14:55.664802 10.0.0.1:3487 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:26707 IpLen:20 DgmLen:63 DF
***AP*** Seq: 0x87039AA0  Ack: 0xC6B60B4D  Win: 0x43DB  TcpLen: 20
PASS Mgpuser@home.com..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

By default the scanner will log on only and terminate the connection with a FIN immediately. The program then provides output as to which IP addresses within the specified range allow anonymous ftp logon.

Under preferences it is possible to get Grim's ping to test for publicly writable directories. The user can specify directories to be scanned but the default list is as follows:

/	/public
/pub/incoming	/incoming
/_vti_pvt/	/pub
/upload/	

Most are standard public or upload directories of various ftp-servers. '/_vti_pvt/' is a directory used for front-page extensions on a web server.

For each directory in the list the scanner attempts to create a directory whose name is based the current date and time. For example the following create attempt:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
03/17-12:47:03.044641 10.0.0.1:3594 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:29632 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0xD9944FA5  Ack: 0x23FEA781  Win: 0x41D3  TcpLen: 20
MKD 020317124933p..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

Took place at 12:49:33 on 17 Mar 02. The time is local time so by comparing the time specified in the directory name to the create attempt in the ftp server log it is possible to tell what time zone the program is running in.

Depending on whether directory creation is allowed or not the FTP server response will either respond with a code 257:

257 "/pub/incoming/020317124933p" new directory created.

or a code 550

550 020317124933p: Permission denied on server. (Upload dirs)

If a directory is successfully created the scanner will then attempt to delete it thus:

03/17-12:47:03.084573 10.0.0.1:3594 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:29636 IpLen:20 DgmLen:59 DF
AP Seq: 0xD9944FED Ack: 0x23FEA841 Win: 0x4113 TcpLen: 20
RMD 020317124933p..

The connection is terminated after the first successful writable directory is found and the details are logged (by default to a file perms.log). Below is an example of the log file.

10.0.0.2

DIR: /pub/incoming/
DELETE STATS: nondeletable

Grim's ping also has the ability to log other details about the server. The pub scanning general and logging dialog boxes are shown below:

Operating system type is obtained from the SYST ftp command which returns the system type, default file format and number of bits per byte.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/17-16:14:41.948243 10.0.0.1:3557 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:13294 IpLen:20 DgmLen:46 DF
***AP*** Seq: 0x7F320BBD  Ack: 0x336788CF  Win: 0x40D9  TcpLen: 20
SYST..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/17-16:14:41.948538 10.0.0.2:21 -> 10.0.0.1:3557
TCP TTL:64 TOS:0x10 ID:38110 IpLen:20 DgmLen:59 DF
***AP*** Seq: 0x336788CF  Ack: 0x7F320BC3  Win: 0x16D0  TcpLen: 20
215 UNIX Type: L8..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Resumability is tested is tested by issuing a FTP REST command. This is normal behaviour for an ftp client testing resumability.

FXP is a mechanism for transferring files between two FTP servers. It works by placing one server into passive mode, meaning that it is listening on a specific port for a connection. On the other server an IP number and port to send the transfer to is specified using the PORT command. The ability to both use passive mode and also to accept a PORT command is tested by Grim's Ping.

```
03/17-16:14:41.951449 10.0.0.1:3557 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:13296 IpLen:20 DgmLen:46 DF
***AP*** Seq: 0x7F320BCB  Ack: 0x33678925  Win: 0x4083  TcpLen: 20
PASV..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/17-16:14:41.957444 10.0.0.1:3557 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:13297 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0x7F320BD1  Ack: 0x33678952  Win: 0x4056  TcpLen: 20
PORT 207,46,133,140,1,21..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The destination specified by the port command is ftp.microsoft.com:21
Most FTP servers should be able to use passive mode without problems but accepting PORT redirects is dangerous, not only because it allows users to use FXP from the server but it also could be used to trigger a denial of service attack by directing the traffic to a listening port of an 3rd party..

The speed of the server is measured by sending a 5k CWD command attempting to change directory to a directory name consisting of 5k of 'p' characters and logging the transfer time. (The first packet only shown):

```
03/17-16:14:41.962236 10.0.0.1:3557 -> 10.0.0.2:21
TCP TTL:128 TOS:0x0 ID:13298 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x7F320BEB  Ack: 0x3367896C  Win: 0x403C  TcpLen: 20
CWD
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppppp
pppppppppppppppppppppppppppppppppppppppppppppppppppp
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

The results of the various tests of the server produce an extended log entry in ‘perms.log’:

```
10.0.0.2
--------
DIR:               /pub/incoming/
DELETE STATS:     nondeletable
RUNNING OS:       UNIX Type: L8
RESUMABLE:        Yes
FXP STATS:        non-FXPable
SEND SPEED:       5124.80 bytes/s
```

Port Scanning and Proxy Scanning

The third function of Grim's Ping is elementary port scanning. This function is usually activated after a host has been found through pinging. By default it scans the following ports:

Port Type	Port Number	Service
TCP	1080	HTTP Proxy
TCP	21	FTP
TCP	22	SSH
TCP	80	WWW
TCP	8080	Proxy (WinGate)

TCP Ports can be added or removed from this list. By default most IDS and firewall systems will log attempted access to the proxy ports from external hosts. For example the following rule is included with Snort 1.83 (scan.rules)

A packet trace of a portscan from a Win XP host running Grim's Ping with standard settings (TCPDUMP format):

15:38:01.073251 10.0.0.1.3961 > 10.0.0.2.1080: S [tcp sum ok] 1770437391:1770437391(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40663, len 48)

15:38:01.075057 10.0.0.1.3962 > 10.0.0.2.21: S [tcp sum ok] 1770501126:1770501126(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40664, len 48)

15:38:01.076611 10.0.0.1.3963 > 10.0.0.2.22: S [tcp sum ok] 1770562738:1770562738(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40666, len 48)

15:38:01.078160 10.0.0.1.3964 > 10.0.0.2.80: S [tcp sum ok] 1770627892:1770627892(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40668, len 48)

15:38:01.079705 10.0.0.1.3965 > 10.0.0.2.8080: S [tcp sum ok] 1770679186:1770679186(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40670, len 48)

The ports are scanned in the order they appear on the port list within the program. There is no evidence of packet craft in these packets. When a port is open the three way handshake is completed such as in the following trace: (TCPDUMP Format)

15:38:01.076611 10.0.0.1.3963 > 10.0.0.2.22: S [tcp sum ok] 1770562738:1770562738(0) win 16384 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 40666, len 48)

15:38:01.076685 10.0.0.2.22 > 10.0.0.1.3963: S [tcp sum ok] 1803978135:1803978135(0) ack 1770562739 win 5840 <mss 1460,nop,nop,sackOK> (DF) (ttl 64, id 0, len 48)

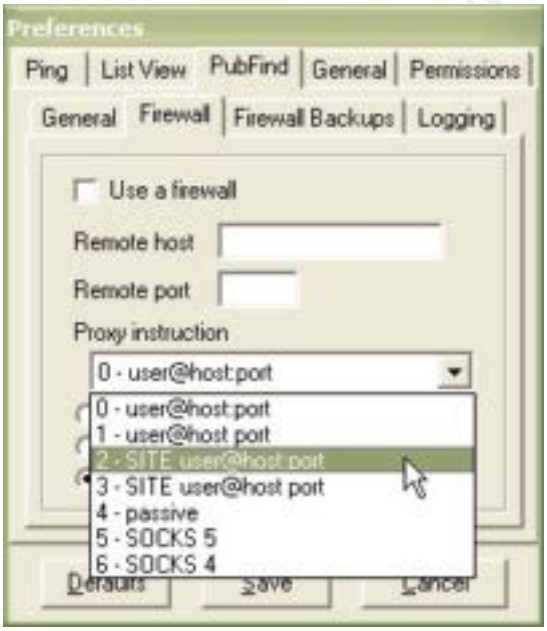
15:38:01.077098 10.0.0.1.3963 > 10.0.0.2.22: . [tcp sum ok] 1:1(0) ack 1 win 17520 (DF) (ttl 128, id 40667, len 40)

The open ports are then displayed to the user.

Proxies

Grim's Ping has the ability to utilise a variety of proxies when conducting pub scanning. This is something to be aware of when noting Grim's Ping traffic in the logs. The apparent source of the scan may be a public proxy server rather than the actual scanner.

The range of proxies able to be used is shown below.



FTP Client

Grim's Ping includes basic ftp client as displayed below.

There is not much particularly noteworthy about the client. The default password for anonymous login is ftpclient@home.com but can be easily changed in a text box prior to logon.

Why Should You Care?

Grim's Ping is not the most sophisticated attacker in use in the wild. It does not use any unique or stealth methods. This does not make it totally uninteresting to the security analyst. Grim's Ping is a noise generator. Even in cases where there is no vulnerabilities to exploit the abnormal nature of the FTP or port scanning traffic may cause a FTP log or packet trace to end up on the analyst's desk. Identifying this traffic for what it is will allow the analyst to move on to the next more interesting alert.

The main reason why Grim's ping is of interest is that activity from this scanner is a potentially useful indicator of warez/ illegal file trading activity. Apart from being a

drain on storage and bandwidth, the legal and public relations aspects should be of great concern. Having federal agents come and seize servers because they are being used as a multi gigabyte library of child pornography for instance. This could be very disruptive to operations.

Even if none of the local servers are acting as warez hosts, the use of Grim's Ping by users may indicate local users are conducting illegal file transferring. The scanning via Grim's Ping of remote servers may be seen as hostile by remote administrators.

Recommended Actions

Use Grim's Ping as a vulnerability scanner

Whilst not a particularly powerful ping client, ftp client or port scanner Grim's Ping is very capable of scanning for ftp servers within an IP range and assessing if they could potentially provide a haven for warez. Running Grim's Ping regularly, of course with due authorisation, is an efficient way to identify hosts within the IP block before they are discovered and used for malicious purposes.

Detect Incoming Grim's Ping Connections

The text string "gpuser@home.com" in an incoming FTP connection is at present a simple test for pub scanning via this tool. A suggested snort rule for detection of this attack is as follows:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"Incoming Grims FTP
Pub scan"; flags: A+; content:"gpuser@home.com"; offset:6;rev:1;)
```

Detect Outgoing Grim's Ping Connections

Sites, especially where users have the ability to install software should be aware of what traffic is leaving through the boundary to the outside world. Identifying internal users attempting to scan for public web-sites is a good step to preventing breaches of policy or illegal actions being carried out from the site.

An example snort rule for detecting outgoing Grim's Ping use is shown below:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 21 (msg:"Outgoing Grims FTP
Pub scan"; flags: A+; content:"gpuser@home.com"; offset:6;rev:1;)
```

Conclusions

Grim's ping is a commonly available tool and quite effective at what it does. With the availability and relative widespread use of this tool it is very likely that any FTP-server on the internet will be probed to examine the permissions for anonymous users. It is therefore vital that FTP servers are configured correctly. Awareness of Grim's ping and the signature traffic may be helpful in preventing abuse of FTP servers.

References

1. "Grim's Ping" grim@crystallized.com
URL http://grimsping.cjb.net/ (March 10, 2002)

2. "FTP and the Warez Scene" Shelli Crocker. 14 December 2000.
URL http://rr.sans.org/threats/warez.php (March 13, 2002).

3. "When Your Server Ends Up A Warez Site" Eye on Security
URL http://www.eyeonsecurity.net/papers/ftpscanning.html (March 16, 2002)

4. "List of Raw FTP Commands"
URL http://www.dreamhaven.net/ftp-raw.html (March 16, 2002)

5. "What is FXP?" Blue-Jam FXP
URL http://www.planetsteve.co.uk/things/faq.php?topic=24
Note: ***Possibly offensive banner ads used at site***

Assignment 2 – Network Detects

Detect 1 - Grim's Ping

```
03/04-07:23:20.768188 172.152.233.27:1227 -> MY.NET.27.68:21
TCP TTL:102 TOS:0x0 ID:2750 IpLen:20 DgmLen:63 DF
***AP*** Seq: 0xF2E66436  Ack: 0x393B73EB  Win: 0x1F4B  TcpLen: 20
50 41 53 53 20 49 67 70 75 73 65 72 40 68 6F 6D  PASS Igpuser@hom
65 2E 63 6F 6D 0D 0A                             e.com..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/04-07:23:20.812279 MY.NET.27.68:21 -> 172.152.233.27:1227
TCP TTL:64 TOS:0x10 ID:3007 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0x393B73EB  Ack: 0xF2E6644D  Win: 0x16B0  TcpLen: 20
32 33 30 2D 57 65 6C 63 6F 6D 65 2C 20 61 72 63  230-Welcome, arc
68 69 76 65 20 75 73 65 72 20 61 6E 6F 6E 79 6D  hive user anonym
6F 75 73 40 41 43 39 38 45 39 31 42 2E 69 70 74  ous@AC98E91B.ipt
2E 61 6F 6C 2E 63 6F 6D 20 21 0D 0A              .aol.com !..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
03/04-07:23:21.395968 172.152.233.27:1227 -> MY.NET.27.68:21
TCP TTL:102 TOS:0x0 ID:2780 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xF2E6644D  Ack: 0x393B7427  Win: 0x1F0F  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```

The snort capture then showed the following FTP commands and responses

```
03/04-07:23:22.187633    CWD /pub/
03/04-07:23:22.188373    250 CWD command successful...
03/04-07:23:22.658004        MKD 020303152123p
03/04-07:23:22.658587        550 020303152123p: Permission denied on
server.  (Upload dirs)
03/04-07:23:23.116034        CWD /public/..
03/04-07:23:23.116545        550 /public/: No such file or directory...
03/04-07:23:23.557331        CWD /pub/incoming/
03/04-07:23:23.568420        250 CWD command successful...
03/04-07:23:24.017092        MKD 020303152125p
03/04-07:23:24.018194        550 020303152125p: Permission denied on
server (Upload dirs)..
03/04-07:23:24.475868        CWD /incoming/
03/04-07:23:24.476389        250 CWD command successful...
03/04-07:23:24.927010        MKD 020303152125p
03/04-07:23:24.927794        550 020303152125p: Permission nied on
server (Upload dirs)..
03/04-07:23:25.376180        CWD /_vti_pvt/
03/04-07:23:25.376638        550 /_vti_pvt/:No such file or directory...
03/04-07:23:25.836439        CWD /..
03/04-07:23:25.836901        250 CWD command successful...
03/04-07:23:26.287831        MKD 020303152127p
03/04-07:23:26.288390        550 020303152127p: Permission denied on
server. (Upload dirs)..
03/04-07:23:26.717043        CWD /upload/..
03/04-07:23:26.717659        550 /upload/: No such file or directory...
03/04-07:23:27.156602        CWD /cgi-bin/
03/04-07:23:27.157066        550 /cgi-bin/: No such file or directory...
03/04-07:23:27.596415        CWD /images/
03/04-07:23:27.596880        550 /images/: No such file or directory...
03/04-07:23:28.036951        CWD /.tmp/
03/04-07:23:28.037407        550 /.tmp/: No such file or directory...
03/04-07:23:28.477548        CWD /~tmp/
03/04-07:23:28.478125        550 /~tmp/: No such file or directory...
03/04-07:23:28.916566        CWD /_tmp/
03/04-07:23:28.917026        550 /_tmp/: No such file or directory...
03/04-07:23:29.356377        CWD /tmp/
03/04-07:23:29.356836        550 /tmp/: No such file or directory...
03/04-07:23:29.776972        CWD /_vti_log/
03/04-07:23:29.777615        550 /_vti_log/: No such file or directory...
03/04-07:23:30.216534        CWD /_vti_txt/
03/04-07:23:30.217003        550 /_vti_txt/: 20  No such file or directory...
03/04-07:23:30.638109        CWD /_vti_script
03/04-07:23:30.638577        50 /_vti_script/: No such or directory...
```

```
03/04-07:23:31.076426          CWD /wwwroot/
03/04-07:23:31.076887          550 /wwwroot/: No such file or directory...
03/04-07:23:31.506874          CWD /scripts/
03/04-07:23:31.507330          550 /scripts/: No such file or directory...
03/04-07:23:31.946682          CWD /bin/
03/04-07:23:31.947247          CWD command successful...
03/04-07:23:32.408369          MKD 020303152133p..
03/04-07:23:32.410143          550 020303152133p: Permission denied on
server (Upload dirs)..
03/04-07:23:32.926575          CWD /usr/..
03/04-07:23:32.927030          550 /usr/: No such file or directory...
03/04-07:23:33.406790          CWD /c:/..
03/04-07:23:33.407237          550 /c:/: No such file or directory...
03/04-07:23:33.887988          CWD / /..
03/04-07:23:33.888445          550 / /: No such file or directory...

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

03/04-07:23:34.326813 172.152.233.27:1227 -> MY.NET.27.68:21
TCP TTL:102 TOS:0x0 ID:3258 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xF2E665D4  Ack: 0x393B7A6F  Win: 0x1E35  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
America Online, Inc. (NETBLK-AOL-172BLK)
   12100 Sunrise Valley Drive
   Reston, VA 20191
   US

   Netname: AOL-172BLK
   Netblock: 172.128.0.0 - 172.191.255.255
   Maintainer: AOL

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

   Domain System inverse mapping provided by:

   DAHA-01.NS.AOL.COM          152.163.159.233
   DAHA-02.NS.AOL.COM          205.188.157.233

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 28-Mar-2001.
   Database last updated on  5-Mar-2002 19:57:42 EDT.
```

Source Of Trace

Home Linux (Debian-Testing) system with ADSL connection to ISP.

Detect Was Generated By

Snort V1.83. The FTP Server WU-FTP on this host was installed in the days prior to the trace and not advertised anywhere to be used as a kind of honeypot. All connections to the FTP port are somewhat suspicious so and all packets logged.

Log format is standard snort for connection setup and teardown. Timestamp and application data only shown for the FTP session data.

Probability the Source Address Was Spoofed

Probably not spoofed. TCP three-way handshake is completed and data transferred in both directions. Source address may be that of an open proxy however rather than the actual attacker

Description Of Attack

Attack identified characteristic of the tool Grim's Ping. This tool scans for publicly writable directories on the ftp server.

Attack Mechanism

The attacker logs on anonymously to the FTP server then a series of FTP commands is sent. Noting how quickly they are sent appears to be done from a program rather than from a keyboard.

The mechanism of attack is to try and change directories to various common directory names and for each directory where that is successful there is an attempt to create a directory with the current timestamp. The FTP server is located is time zone (GMT+11) (Australian Eastern Summer Time). The attacker system appears to have local clock set 17 hrs behind (GMT-6) which puts attacker most likely in USA Central Standard Time which tallies with the whois report.

The list of directories checked includes more directories than the list checked by default in the current version of Grim's Ping (See assignment 1 above). Standard web server directories such as wwwroot are attacked as well as checking for UNIX and windows systems directories such as /usr and c:/.

The attacker was unable to find a directory which allowed a subdirectory to be created within it and the connection was terminated.

Correlations

Multiple traces have been posted to various message boards with signature of Grim's Ping.

http://www.incidents.org/archives/intrusions/msg03438.html
http://www.freescosoft.com/cgi-bin/ib3-freesco/ikonboard.cgi?s=3c85f8cb3bd6ffff;act=ST;f=5;t=77;hl=ftp4all
http://www1.dshield.org/pipermail/dshield/2001-October/001668.html

Similar Packet trace in GCIA practical by David Dobrotka
http://www.giac.org/practical/David_Dobrotka_GCIA.zip

Evidence of Active Targeting

No evidence of active targeting. The trace shows the properties of being an automated scan. The attacker scans for windows related directories (such as c:/) on what is clearly an *NIX Apache server

Severity

Criticality: Home test system. (2)

Lethality: Depending what directory is found to be writable by the scanner it could lead to webpage defacement, storage space for "warez" or mechanism for some other exploit (4)

System Countermeasures: Latest Patched version of WU-FTPD. No flaws in FTP permissions discovered by the scan. (5)

Network countermeasures: Nil (1)

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

=(2+4) -(1+5) = 0 (Barely adequate)

Defensive Recommendation

Examine whether this machine needs to have an FTP client running and if so whether anonymous access is desired. If this is an anonymous FTP-site the writable incoming directory should be removed unless there is a genuine need to accept files from unauthenticated users. At the moment the incoming directory is not readable so communication is one way but still it provides a mechanism for malicious code or exploit code to get into the system.

The IDS system could be configured to detect pub scanning either by detecting the signature of Grim's Ping or by flagging attempted MKDIR operations. Depending on site policies and expected legitimate use of the FTP server an automatic reset of the connection on triggering of the signature may be appropriate.

Multiple Choice Test Question

Examine the following excerpts of an anonymous FTP session:

```
03/04-07:23:24.017092    MKD 020303152125p
03/04-07:23:24.018194    550 020303152125p: Permission denied on server
                         (Upload dirs)..
```

What is most probable explanation of this traffic:

a. Normal FTP usage.
b. Wu-FTPD Buffer overflow attempt
c. Pub-Scanning
d. Web server remote administration

Answer: c

Detect 2 - FTP Probes

```
03/03-06:25:28.714477 208.46.199.201:21 -> MY.NET.27.68:21
TCP TTL:118 TOS:0x0 ID:14022 IpLen:20 DgmLen:40
******S* Seq: 0x33AD5BEA  Ack: 0x4AB1D4A1  Win: 0x8AF8  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:28.714547 MY.NET.27.68:21 -> 208.46.199.201:21
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x21AD0E84  Ack: 0x33AD5BEB  Win: 0x16B0  TcpLen: 24
TCP Options (1) => MSS: 1452
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:28.906905 208.46.199.201:21 -> MY.NET.27.68:21
TCP TTL:238 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x33AD5BEB  Ack: 0x0  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:29.464012 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:47 TOS:0x0 ID:33253 IpLen:20 DgmLen:60 DF
******S* Seq: 0x30B74484  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1412 SackOK TS: 76531041 0 NOP WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
03/03-06:25:29.464049 MY.NET.27.68:21 -> 208.46.199.201:3884
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x2149F7F9  Ack: 0x30B74485  Win: 0x1680  TcpLen: 40
TCP Options (5) => MSS: 1452 SackOK TS: 5396332 76531041 NOP
TCP Options => WS: 0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:29.657916 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:47 TOS:0x0 ID:33254 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x30B74485  Ack: 0x2149F7FA  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 76531061 5396332
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+

03/03-06:25:32.999361 MY.NET.27.68:21 -> 208.46.199.201:3884
TCP TTL:64 TOS:0x10 ID:41082 IpLen:20 DgmLen:133 DF
***AP*** Seq: 0x2149F7FA  Ack: 0x30B74485  Win: 0x1680  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5396686 76531061
32 32 30 20 61 74 68 65 6E 61 20 46 54 50 20 73  220 athena FTP s
65 72 76 65 72 20 28 56 65 72 73 69 6F 6E 20 77  erver (Version w
75 2D 32 2E 36 2E 31 28 31 29 20 57 65 64 20 4E  u-2.6.1(1) Wed N
6F 76 20 32 38 20 30 34 3A 30 32 3A 33 31 20 47  ov 28 04:02:31 G
4D 54 20 32 30 30 31 29 20 72 65 61 64 79 2E 0D  MT 2001) ready..
0A                                               .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.199295 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:47 TOS:0x0 ID:33255 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x30B74485  Ack: 0x2149F84B  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 76531415 5396686
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.224886 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:47 TOS:0x0 ID:33256 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x30B74485  Ack: 0x2149F84B  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 76531417 5396686
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.225100 MY.NET.27.68:21 -> 208.46.199.201:3884
TCP TTL:64 TOS:0x10 ID:41083 IpLen:20 DgmLen:89 DF
***AP*** Seq: 0x2149F84B  Ack: 0x30B74486  Win: 0x1680  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5396708 76531417
32 32 31 20 59 6F 75 20 63 6F 75 6C 64 20 61 74  221 You could at
```

```
20 6C 65 61 73 74 20 73 61 79 20 67 6F 6F 64 62   least say goodb
79 65 2E 0D 0A                                    ye...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.231546 MY.NET.27.68:21 -> 208.46.199.201:3884
TCP TTL:64 TOS:0x10 ID:41084 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x2149F870  Ack: 0x30B74486  Win: 0x1680  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5396709 76531417
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.421035 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:238 TOS:0x10 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x30B74486  Ack: 0x0  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

03/03-06:25:33.437761 208.46.199.201:3884 -> MY.NET.27.68:21
TCP TTL:238 TOS:0x10 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x30B74486  Ack: 0x0  Win: 0x0  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
Dandin Group (NETBLK-QWEST-208-46-199-0)
  43730 Vista Del Mar
  Fremont, CA 94539
  US

  Netname: QWEST-208-46-199-0
  Netblock: 208.46.199.0 - 208.46.199.255

  Coordinator:
    Hendricks, Dewayne  (DH649-ARIN)  dhendricks@dandingroup.com
    510-657-5616

  Record last updated on 29-Oct-1999.
  Database last updated on  5-Mar-2002 19:57:42 EDT.
```

Source of Trace

Home Linux (Debian-Testing) system with ADSL connection to ISP.

Detect Was Generated By

Snort V1.83.   All traffic to and from the host was being captured in an attempt to collect packet traces for this assignment.

The original connection request was discovered by searching for reflective ports i.e. source port = destination port. A typical TCP connection has a connection from a high port (>1024) to a low reserved port. The filter used was 'tcp[0:2]=tcp[2:2]'

This highlighted a number of attempted connections to port 21 (FTP) from port 21.

One such detect was selected and all traffic associated with that IP extracted using filter 'host 208.46.199.201'

Packet traces are in standard snort format.

Probability the Source Address Was Spoofed

Probably not spoofed. Two TCP three-way handshakes are attempted. One is reset and one is completed. Noting that this is a probing activity, data also needs to return to the originator to be useful.

Description of Attack

Probing for FTP servers then determining version of server from FTP Banner.

Attack Mechanism

This attack is a stimulus. It begins with a lone SYN. Prior to this time no packets had been exchanged with the attacker.

The attacker is targeting FTP. The fact that the attacker used a source port of 21 for the scan is what drew attention to his actions. He may be using port 21 in an attempt to avoid detection by firewalls or filters. If filtering is being done only by port numbers traffic with a src port of 21 may be treated as a response to an internal query and allowed to pass through the boundary whereas an incoming packet with a high port number indicates an attempt to access service. Filtering that examines the TCP flags and notes the SYN sees through this.

The three way handshake is not completed for the first session, instead a reset is sent. This may be to prevent logging if only established TCP connections are being logged.

Immediately after the first probe (less than 1s after) a more normal TCP connection is established. This has high port to low port connection and the three way hand-shake is completed.

Once the FTP Banner is received the connection is terminated with a FIN. Many ftp servers (including the one running on this host) advertise the version of the server software being run. The attacker may be scanning for a known FTP server vulnerability or simply cataloguing for future reference version in use for when a new vulnerability is found.

No further contact from this address was conducted indicating the version found was not what the attacker was looking for.

Of interest in the traces is the TTL and IP ID fields. Noting that the two connection attempts happen at around the same time there are some notable differences between the first half open connection scan and the connection to get the banner.

The first SYN has an IP ID of 14022 and a TTL of 118.
The second SYN has an IP ID of 33253 and a TTL of 47

The differences here indicate that one or the other of these connections is the result of packet craft. My hypothesis is that the probe is the combination of two code fragments or programs that have been combined such as a scanning tool for open ports combined with a second tool to get the FTP banners. The use of crafted packets with such different characteristics in such a short period of time undermines the attempted stealth of the half open scan with src and dst ports of 21.

Correlations

DSHIELD reports 27 distinct attacks from this IP address on the same day:
http://www.dshield.org/subnet.php?subnet=208.46.199.201&Submit=Submit

Attempts were made to identify the tool without success.

Evidence Of Active Targeting

This trace doesn't look like active targeting initially. The attacker is scanning. Although only the one IP is being monitored the fact that there are so many hits on DSHIELD for the same period indicates there was scanning against more than this one IP address.

Coming straight back to get the FTP banner is being closer to being active targeting. The attacker has come back a second time to gather more information in response to the SYN/ACK received after the first probe.

Severity

Criticality: Home test system. (2)

Lethality: If a vulnerability is discovered in the version of the FTP server (WuFTP 2.6.1) then the system may have been catalogued as a potential target. Buffer overflows have been previously discovered and been exploited to give remote root access. (3)

System Countermeasures: Server is up to date but scan did not trigger IDS (Snort with standard rule set) and no attempt was made to hide what version of the server was

running giving out valuable data. (2)

Network countermeasures: Nil (1)

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

=(2+3) -(2+1) = 2

Defensive Recommendation

Remove information about what version of FTPD is running on the system. This will deny valuable information so an attacker will have to actually try to use various exploit code to determine if the system is vulnerable which will have a higher chance of triggering the IDS. At the moment a potential attacker can determine the what vulnerabilities the system may have simply by capturing the banner.

Multiple Choice Test Question

Examine the trace of the following incoming packet:

03/03-06:25:28.714477 208.46.199.201:21 -> MY.NET.27.68:21
TCP TTL:118 TOS:0x0 ID:14022 IpLen:20 DgmLen:40
******S* Seq: 0x33AD5BEA Ack: 0x4AB1D4A1 Win: 0x8AF8 TcpLen: 20

What about this packet is unusual for an incoming FTP connection?
a. TCP Length: 20
b. SRC Port: 21
c. DST Port: 21
d. TCP TTL: 118

ANSWER: B Connection requests should normally be high port to low port.
=+=

Detect 3 – Portscan

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 61.9.192.15 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
03/08-17:52:26.392207

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 61.9.192.15 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
03/08-17:52:26.392275

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.15: 5 connections across 1 hosts: TCP(0), UDP(5) [**]

03/08-17:53:01.764733

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.15: 5 connections across 1 hosts: TCP(0), UDP(5) [**]
03/08-17:53:01.764862

[**] [100:3:1] spp_portscan: End of portscan from 61.9.192.15: TOTAL time(0s) hosts(1) TCP(0) UDP(5) [**]
03/08-17:53:51.464207

[**] [100:3:1] spp_portscan: End of portscan from 61.9.192.15: TOTAL time(0s) hosts(1) TCP(0) UDP(5) [**]
03/08-17:53:51.464411

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 61.9.192.14 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
03/08-17:53:51.488632

[**] [100:1:1] spp_portscan: PORTSCAN DETECTED from 61.9.192.14 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
03/08-17:53:51.488707

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.14: 5 connections across 1 hosts: TCP(0), UDP(5) [**]
03/08-17:53:56.964704

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.14: 5 connections across 1 hosts: TCP(0), UDP(5) [**]
03/08-17:53:56.965125

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.14: 1 connections across 1 hosts: TCP(0), UDP(1) [**]
03/08-17:54:37.627367

[**] [100:2:1] spp_portscan: portscan status from 61.9.192.14: 1 connections across 1 hosts: TCP(0), UDP(1) [**]
03/08-17:54:37.627613

Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32773 UDP
Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32774 UDP
Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32775 UDP
Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32777 UDP
Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32778 UDP
Mar 8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32773 UDP

```
Mar  8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32774 UDP
Mar  8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32775 UDP
Mar  8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32777 UDP
Mar  8 17:52:26 61.9.192.15:53 -> MY.NET.26.199:32778 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32774 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32779 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32781 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32787 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32783 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32774 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32779 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32781 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32787 UDP
Mar  8 17:53:51 61.9.192.14:53 -> MY.NET.26.199:32783 UDP
Mar  8 17:54:37 61.9.192.14:53 -> MY.NET.26.199:32785 UDP
Mar  8 17:54:37 61.9.192.14:53 -> MY.NET.26.199:32785 UDP
```

Source Of Trace

Home Linux (Debian-Testing) system with ADSL connection to ISP.

Detect Was Generated By

Snort V1.83 standard rule set. Excerpts from alert and portscan file shown

Probability The Source Address Was Spoofed

Probably not spoofed. Although UDP does not require a three way handshake asking the question "Stimulus or Response" and taking into account what the IP in question is indicates this is a response.

Searching for other references to this IP address found the following packet:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/08-17:50:56.326651 MY.NET.26.199:32773 -> 61.9.192.15:53
UDP TTL:64 TOS:0x0 ID:10259 IpLen:20 DgmLen:67 DF
Len: 47
BC B7 01 00 00 01 00 00 00 00 00 01 32 01 30  ............2.0
01 30 02 31 30 07 69 6E 2D 61 64 64 72 04 61 72  .0.10.in-addr.ar
70 61 00 00 0C 00 01                             pa.....
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

This is the stimulus for the first packet in the portscan. Therefore what is shown in the log is a response and therefore IP Address probably not spoofed.

Description of Attack

The IP address 61.9.192.15 happens to be the primary DNS server for my ISP. Examining the traffic shows it to be DNS traffic as would be expected for port 53 so this is not an attack.

Attack Mechanism

Despite the fact this is not actually an attack something had gone wrong which triggered the flood of traffic and hence the portscan alert.

Examining the stimulus DNS lookup packet again:

```
03/08-17:50:56.326651 MY.NET.26.199:32773 -> 61.9.192.15:53
UDP TTL:64 TOS:0x0 ID:10259 IpLen:20 DgmLen:67 DF Len: 47
BC B7 01 00 00 01 00 00 00 00 00 00 01 32 01 30  .............2.0
01 30 02 31 30 07 69 6E 2D 61 64 64 72 04 61 72  .0.10.in-addr.ar
70 61 00 00 0C 00 01                             pa.....
```

This is a reverse lookup of 10.0.0.2. RFC 1918 defines addresses in the range 10.0.0.0 - 10.255.255.255 for private internets and are non-routable. Despite this, host MY.NET.26.199 is attempting to do a reverse DNS lookup with a name server external to the private network. There is a misconfiguration here. The apparent incoming portscan to port 53 is simply multiple negative replies to attempts to resolve private network host names and numbers.

Correlations

Discussion on port numbers used by BIND 8.0 including ports seen in trace.

http://www.der-keiler.de/Mailing-Lists/securityfocus/focus-sun/2001-10/0022.html

http://www.der-keiler.de/Mailing-Lists/securityfocus/focus-sun/2001-10/0026.html

Evidence Of Active Targeting

This attack is actively self-targeted. Traffic targeted in response to DNS queries.

Severity

Criticality: Home test system. (2)

Lethality: False positive from "friendly" server. (1)

System Countermeasures: System does have IDS installed but misconfiguration of DNS is of concern (2)

Network countermeasures: System is NAT'ed but not correctly. Not firewalled on that port but not expected to be considering the host is the primary DNS server. (2)

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

=(2+1) -(2+2) =-1

Defensive Recommendation

Fix DNS configuration of host so as not to trigger responses from DNS server.

Multiple Choice Test Question

What does the following packet represent?

```
03/08-17:50:56.326651 MY.NET.26.199:32773 -> 61.9.192.15:53
UDP TTL:64 TOS:0x0 ID:10259 IpLen:20 DgmLen:67 DF
Len: 47
BC B7 01 00 00 01 00 00 00 00 00 00 01 32 01 30  .............2.0
01 30 02 31 30 07 69 6E 2D 61 64 64 72 04 61 72  .0.10.in-addr.ar
70 61 00 00 0C 00 01                             pa.....
```

a. A reverse DNS lookup of 10.0.0.2
b. An RPC-server response
c. A DNS lookup of host name in-addr.arpa
d. A reverse DNS lookup of 2.0.0.10

Answer: A

Detect 4 – WEB-IIS ISAPI .ida attempt

```
[**] [1:1243:2] WEB-IIS ISAPI .ida attempt [**]
[**] [1:1243:2] WEB-IIS ISAPI .ida attempt [**]
[Classification: Web Application Attack] [Priority: 1]
03/08-01:02:56.776020 163.19.3.242:2308 -> MY.NET.26.199:80
TCP TTL:106 TOS:0x0 ID:39054 IpLen:20 DgmLen:1452 DF
***AP*** Seq: 0x1A69F4B0  Ack: 0x93A6F942  Win: 0x4230  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS552]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0071]

[Classification: Web Application Attack] [Priority: 1]
03/08-01:02:56.776020 163.19.3.242:2308 -> MY.NET.26.199:80
TCP TTL:106 TOS:0x0 ID:39054 IpLen:20 DgmLen:1452 DF
***AP*** Seq: 0x1A69F4B0  Ack: 0x93A6F942  Win: 0x4230  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS552]
```

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0071]

```
***************************************************************
03/08-01:02:56.776020 163.19.3.242:2308 -> MY.NET.26.199:80
TCP TTL:106 TOS:0x0 ID:39054 IpLen:20 DgmLen:1452 DF
***AP*** Seq: 0x1A69F4B0  Ack: 0x93A6F942  Win: 0x4230  TcpLen: 20
GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd
3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u90
90%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u0
0=a  HTTP/1.0..Content-type: text/xml.HOST:www.worm.com. Accept: */*.Con
tent-length:
3569....U........SVW....................p..............h.........d......G.d.=.....o.....`...............h....
..........X......w.......p............X...........X.....X......xu...X.........X...3.f..=MZ.........X....Q<
..X...3.f.....PE....y.....X....B<..X....T.x..X.....T.....T....H...X.....L.....L....:KERN..
3.....L....x.EL32.......X.....4.....T.....X....B.L.....H...........H........H.....L........L.....T.....H.
..;H.........L.......X....<.GetP........L.......X....|..rocA........H.....H.....X...
..T....H$3.f.....L.....T....Q...L....L....L.....L.....L.....L.....L.....X.....T....H......L.....L.....X...
..p.....................G.d.......p....u..8.....L...........L........L.....h................h.........u!..h.......
.P......;..CKCK..4....*....h...Q..4...R..p...;..CKCK..L..............h........h.....h........t.....
h........h....S.....h........h....M.........I.....L.............h.E.............[SS.......cx...M..Q...P.....
P....u&..j...L...P..h...
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
=+=+=+=+

03/08-01:02:56.786687 MY.NET.26.199:80 -> 163.19.3.242:2308
TCP TTL:64 TOS:0x0 ID:8958 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x93A6F942  Ack: 0x1A69FA38  Win: 0x2118  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 6761@62644

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

03/08-01:02:56.839099 MY.NET.26.199:80 -> 163.19.3.242:2308
TCP TTL:64 TOS:0x0 ID:8959 IpLen:20 DgmLen:534 DF
***AP*** Seq: 0x93A6F942  Ack: 0x1A69FA38  Win: 0x2118  TcpLen: 20
HTTP/1.1 400 Bad Request..Date: Thu, 07 Mar 2002 14:02:56 GMT..S
erver: Apache/1.3.23 (Unix) Debian GNU/Linux..Connection: close.
.Content-Type: text/html; charset=iso-8859-1....<!DOCTYPE HTML P
```

UBLIC "-//IETF//DTD HTML 2.0//EN">.<HTML><HEAD>.<TITLE>400 Bad R
equest</TITLE>.</HEAD><BODY>.<H1>Bad Request</H1>.Your browser s
ent a request that this server could not understand.<P>.Client s
ent malformed Host header<P>.<HR>.<ADDRESS>Apache/1.3.23 Server
at 127.0.0.1 Port 80</ADDRESS>.</BODY></HTML>.

Source Of Trace

Home Linux (Debian-Testing) system with ADSL connection to ISP.

Detect Was Generated By

Snort V 1.83 with –v –d –C options.

Snort Rule Triggered:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS ISAPI
.ida attempt"; uricontent:".ida?"; nocase; dsize:>239; flags:A+;
reference:arachnids,552; classtype:web-application-attack; reference:cve,CAN-
2000-0071; sid:1243; rev:2;)

Probability the Source Address Was Spoofed

Source Address is probably not spoofed as TCP three way handshake completed and web application data exchanged.

Description Of Attack

Code Red Worm. Attempt to exploit of .ida vulnerability in IIS.

Although a CVE number is quoted in the snort alert that is not the correct vulnerability. This alert is triggered via '.ida?' being found in a web query. A number of vulnerabilities caused by '.ida?' exist in unpatched versions of IIS. The vulnerability being exploited here is the .ida buffer overflow CAN-2001-500..

Microsoft Advisory
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

CERT Advisory
http://www.cert.org/advisories/CA-2001-13.html

CVE Reference
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

Attack Mechanism

Hosts infected by Code Red begin scanning random IP ranges for hosts to infect. If a connection is made to port 80 then the exploit string is sent as seen above in the packet

trace. The exploit allows execution of arbitrary code so if vulnerable the attacked host will now be infected and begin scanning to infect other hosts.

The worm will also after a certain time deface the web pages being served and at various times attempt to participate in a denial of service attempt against the IP address that used to be www.whitehouse.gov.

Details of the attack mechanism are detailed by CERT/CC at:
http://www.cert.org/incident_notes/IN-2001-08.html

Many, many papers on Code Red are available from the SANS Reading Room:
http://rr.sans.org/malicious/malicious_list.php

Correlations

Dshield reports the following for this IP:
http://www.dshield.org/ipinfo.php?ip=163.19.3.242

IP Address: 163.19.3.242
HostName: 163.19.3.242
DShield Profile: Country:
TW

Contact E-mail:
tanetadm@moe.edu.tw

Total Records against IP:
246

Number of targets:
104

Date Range:
2002-03-12 to 2002-03-13

Ports Attacked (up to 10):
Port
Attacks

104 hosts logged attacks from this machine. All were logged a few days after being logged by my system.

Evidence of Active Targeting

Nil evidence of active targeting. A Code Red infected host automatically attempts to infect other hosts at very fast rate. Even if this was not known the fact that this host is logged as an attacker by at least 104 other hosts and the attempted exploit was againt an IIS vulnerability on a clearly identified Apache web-server makes this clearly not active targeting.

Severity

Criticality: Home test system. (2)

Lethality: Harmless as not running IIS. (1)

System Countermeasures: System is running an up to date version of apache and responds appropriately to the illegal request.(5)

Network countermeasures: System has an IDS installed. As it is a webserver blocking access to port 80 is unreasonable (3)

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

=(2+1) -(5+3) =-5 (Not a threat)

Defensive Recommendation

Nil defensive recommendation. Host adequately protected against threat.

Multiple Choice Test Question

The web address www.worm.com is contained in the propagation attempts by which worm ?

a. Red Worm
b. Code Red Worm
c. Lion
d. Ramen

Answer: b Code Red worm.

Detect 5 – Proxy Scan

[**] [1:618:1] INFO - Possible Squid Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:58.288730 61.170.138.27:4272 -> MY.NET.27.68:3128
TCP TTL:50 TOS:0x0 ID:32591 IpLen:20 DgmLen:48 DF
******S* Seq: 0xA3D018BD Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

[**] [1:620:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:58.290411 61.170.138.27:4273 -> MY.NET.27.68:8080
TCP TTL:50 TOS:0x0 ID:32592 IpLen:20 DgmLen:48 DF
******S* Seq: 0xA3D0ECB9 Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

[**] [1:618:1] INFO - Possible Squid Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:58.973705 61.170.138.27:4272 -> MY.NET.27.68:3128
TCP TTL:50 TOS:0x0 ID:32725 IpLen:20 DgmLen:48 DF
******S* Seq: 0xA3D018BD Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

[**] [1:620:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:58.981054 61.170.138.27:4273 -> MY.NET.27.68:8080
TCP TTL:50 TOS:0x0 ID:32729 IpLen:20 DgmLen:48 DF
******S* Seq: 0xA3D0ECB9 Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

[**] [1:618:1] INFO - Possible Squid Scan [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:59.796153 61.170.138.27:4272 -> MY.NET.27.68:3128
TCP TTL:50 TOS:0x0 ID:32899 IpLen:20 DgmLen:48 DF
******S* Seq: 0xA3D018BD Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

[**] [1:620:1] SCAN Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/03-02:47:59.805999 61.170.138.27:4273 -> MY.NET.27.68:8080
TCP TTL:50 TOS:0x0 ID:32906 IpLen:20 DgmLen:48 DF

******S* Seq: 0xA3D0ECB9 Ack: 0x0 Win: 0x8000 TcpLen: 28
TCP Options (4) => MSS: 1412 NOP NOP SackOK

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois6.apnic.net)

inetnum: 61.169.0.0 - 61.171.255.255
netname: CHINANET-SH
descr: CHINANET Shanghai province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: XI5-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-SH
changed: hostmaster@ns.chinanet.cn.net 20001201
source: APNIC

person: Chinanet Hostmaster
address: A12,Xin-Jie-Kou-Wai Street
country: CN
phone: +86-10-62370437
fax-no: +86-10-62053995
e-mail: hostmaster@ns.chinanet.cn.net
nic-hdl: CH93-AP
mnt-by: MAINT-CHINANET
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: Wu Xiao Li
address: Room 805,61 North Si Chuan Road,Shanghai,200085,PRC
country: CN
phone: +86-21-63630562
fax-no: +86-21-63630566
e-mail: ip-admin@mail.online.sh.cn
nic-hdl: XI5-AP
mnt-by: MAINT-CHINANET-SH
changed: ip-admin@mail.online.sh.cn 20010510
source: APNIC

Source Of Trace

Home Linux (Debian-Testing) system with ADSL connection to ISP.

Detect Was Generated By

Snort V1.83 running with standard rule set. Alerts logged to /var/log/snort/alert

Probability The Source Address Was Spoofed

IP address probably not spoofed. Purpose of scan appears to be collect information on whether open proxies are running. If IP address was spoofed the attacker would not receive this information.

Description Of Attack

The attack is an attempt to connect to known proxy ports. Attack is known as a Squid Scan or Proxy Scan.

Attack Mechanism

The attacker in less that 1.5s attempts to connect to the well known ports for various proxy servers these are as follows:

Port	Service
3128	Squid, a caching proxy server
8080	Standard port for proxy servers

Proxy server perform the task of acting as an intermediary between a client and the World Wide Web. Typically in organisations as a security measure only the proxy server is able to access the outside internet and internal hosts instead query the proxy server. This can prevent leakage of internal information about network structure to the internet. It is also a means of conserving bandwidth. Typically there are many pages that are accessed by multiple users on a site. The proxy server when first retrieving a particular page can store it in a cache then serve it to subsequent users who request it without consuming external bandwidth.

One problem with proxy servers is that if misconfigured they can be used as proxy not only by internal hosts of the organisation but by any external host. This is known as an 'open' proxy. This allows a level of anonymity as the true destination will only see the proxy servers address in the logs. It also may allow the user to block administrative restrictions in force at their site

The attack seen here is a scan to try and find proxy servers which respond to external hosts.

Correlations

Proxy scans are very common on the internet. Nil entries recoded for this IP address in Dshield.

A very similar proxy scan also from China with the same source ports was noted in the message board posting:
http://www.sans.org/y2k/092200.htm

This may indicate the same tool was being used/.

Evidence Of Active Targeting

Nil evidence of active targeting. Whilst there are no other IP addresses to correlate with there is no evidence that this is anything more than a random scan of IP ranges.

Severity

Criticality: Home test system. (2)

Lethality: If proxy server running could be abused but not critical to integrity of machine. (2)

System Countermeasures: (2) System isn't running a proxy server but the ports are not blocked or filtered so information is returned to the scanner

Network countermeasures: System has an IDS installed but proxy ports are not being filtered by any border device. (2)

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

=(2+2) -(2+2) =0 (Barely adequate)

Defensive Recommendation

Filter proxy ports both at the firewall and on the system via a personal firewall or packet filter. This will deny any information whatsoever from proxy scanners.

Multiple Choice Test Question

Attempted connections to port 3128 may be evidence of:

A. Backdoor scanning
B. Back Orifice Scanning
C. Netbus Scanning
D. Squid Scanning

Answer: D

Assignment 3 – Analyze This!

Executive Summary

Alerts, port scans and out of spec traffic flagged by the MY.NET Intrusion Detection System (IDS) was examined for the period 19-23 Feb 02. Even excluding the port scans there were over 525000 alerts logged in this period.

The most often occurring and also the most potentially serious alerts were analysed. A list of the most commonly logged machines has been produced and traffic to and from the top 10 source and destination machines carried out. The analysis has been carried out without any pre knowledge of the structure of the network or the exact configuration of the IDS.

In the process of the analysis it was determined this network is a large site with a permissive policy towards applications and network traffic. From the absence of various types of alerts from outside is probable that a boundary device blocking malicious traffic

It is apparent that the IDS is producing a high number of false positives primarily because the system does not adequately distinguish between incoming traffic and normal internal traffic. The network is subject to a wide range of scanning and possible malicious activity.

There is however evidence of infected and compromised hosts within the network and possible vulnerabilities. The primary concerns are as follows:

1. The Snort IDS is configured so it triggers alerts for normal printer, web and windows network traffic. Reconfiguration of the IDS will allow much more meaningful output.

2. Hosts MY.NET.153.143 and MY.NET.153.188 appear infected with the MYPARTY virus.

3. Host MY.NET.5.83 appears to be exploiting Trojan software installed on four other internal machines:

4. There are possible indications of Adore infected Linux hosts on the network especially hosts MY.NET.152.159, MY.NET.153.187 and the MY.NET.6.x subnet

5. IIS web server MY.NET.5.56 is misconfigured, compromised and / or vulnerable.

6. There is high levels of usage of peer to peer file sharing programs such as Kazaa.

7. SNMP is used internally within the network. Given recently discovered vulnerabilities this use should be examined if it has not been already.

8. The network is targeted with a wide variety of scans and probes many of which would successfully gain intelligence about the internal structure of the network.

9. There is a great deal of high bandwidth UDP traffic between this site and China using large UDP packets.

Without knowledge of the network, hosts and applications running it is impossible to make 100% accurate diagnosis of the alerts. This report aims to highlight instead the most probable interpretations of the alerts and flag items which merit investigation by in-house systems administration and security staff.

List of Files Used For Dataset

Fives days of logs were analysed dated 19-Feb-02 through 23-Feb-02. The files were downloaded from http://www.research.umbc.edu/~andy

Alerts	OOS	Scans
alert.020219.gz	oos.020219.gz	scans.020219.gz
alert.020220.gz	oos.020220.gz	scans.020220.gz
alert.020221.gz	oos.020221.gz	scans.020221.gz
alert.020222.gz	oos.020222.gz	scans.020222.gz
alert.020223.gz	oos.020223.gz	scans.020223.gz

List of Detects

Excluding port scans the following alert types were logged over the five-day period.

Count	Alert Type
168339	Connect to 515 from inside
120343	Spp_http_decode: IIS Unicode attack detected
61985	SMB Name Wildcard
47815	MISC Large UDP Packet
30746	ICMP Echo Request L3retriever Ping
23075	SNMP public access
18812	INFO MSN IM Chat data
18722	Spp_http_decode: CGI Null Byte attack detected
9382	High port 65535 udp - possible Red Worm – traffic
5870	Watchlist 000220 IL-ISDNNET-990517
4887	ICMP Echo Request Nmap or HPING2
1851	ICMP Echo Request BSDtype
1713	ICMP Router Selection
1682	ICMP Echo Request Delphi-Piette Windows
1576	Watchlist 000219
1555	WEB-IIS view source via translate header

1506	MYPARTY - Possible My Party infection
1243	ICMP Fragment Reassembly Time Exceeded
1093	FTP DoS ftpd globbing
981	INFO Inbound GNUTella Connect request
807	SYN-FIN scan!
591	SCAN Proxy attempt
586	Incomplete Packet Fragments Discarded
507	INFO - Possible Squid Scan
491	Null scan!
415	WEB-IIS _vti_inf access
406	WEB-FRONTPAGE _vti_rpc access
286	ICMP Echo Request Windows
268	INFO Possible IRC Access
239	WEB-CGI scriptalias access
214	INFO FTP anonymous FTP
198	INFO Outbound GNUTella Connect request
188	INFO Napster Client Data
161	WEB-CGI ksh access
129	Tiny Fragments - Possible Hostile Activity
121	NMAP TCP ping!
97	ICMP traceroute
89	MISC traceroute
79	ICMP Destination Unreachable (Communication Administratively Prohibited)
70	WEB-CGI csh access
69	WEB-MISC 403 Forbidden
68	INFO Outbound GNUTella Connect accept
65	INFO Inbound GNUTella Connect accept
61	WEB-MISC Attempt to execute cmd
50	EXPLOIT x86 setgid 0
47	WEB-MISC compaq nsight directory traversal
42	Port 55850 tcp - Possible myserver activity - ref. 010313-1
36	Possible trojan server activity
36	EXPLOIT NTPDX buffer overflow
31	WEB-MISC http directory traversal
31	WEB-CGI phf access
31	EXPLOIT x86 NOOP
23	Queso fingerprint
23	FTP CWD / - possible warez site
23	Back Orifice
21	FTP passwd attempt
19	Attempted Sun RPC high port access
18	High port 65535 tcp - possible Red Worm – traffic

14	SMB CD...
14	EXPLOIT x86 setuid 0
13	ICMP Destination Unreachable (Protocol Unreachable)
12	IDS552/web-iis_IIS ISAPI Overflow ida nosize
10	Watchlist 000222 NET-NCFC
9	WEB-CGI formmail access
5	Port 55850 udp - Possible myserver activity - ref. 010313-1
5	EXPLOIT x86 stealth noop
3	WEB-MISC ICQ Webfront HTTP DOS
3	WEB-IIS encoding access
3	TFTP - Internal UDP connection to external tftp server
3	SCAN FIN
3	RFB - Possible WinVNC - 010708-1
2	WEB-MISC whisker head
2	WEB-IIS asp-dot attempt
2	WEB-IIS Unauthorized IP Access Attempt
2	TCP SRC and DST outside network
2	SUNRPC highport access!
2	BACKDOOR NetMetro File List
1	WEB-CGI redirect access
1	SCAN XMAS
1	RPC udp traffic contains bin sh
1	Probable NMAP fingerprint attempt
1	NIMDA - Attempt to execute cmd from campus host
1	External RPC call
1	EXPLOIT x86 NOPS
1	DNS named iquery attempt

Top 10 Alerts

Number 1 Alert: Connect to 515 from inside

Unique Source Addresses	153
Unique Destination Addresses	3

Top 10 Sources	Count	Dests	Count
MY.NET.153.106	21750	MY.NET.156.198	167275
MY.NET.153.119	12157	MY.NET.1.163	887
MY.NET.153.114	10506	MY.NET.153.184	187
MY.NET.153.122	8042		
MY.NET.153.117	7656		
MY.NET.153.118	6237		
MY.NET.153.109	5979		
MY.NET.153.113	5554		
MY.NET.153.111	4962		
MY.NET.153.125	4605		

Port 515 is the standard port for the lpd printer daemon. There have been known vulnerabilities in LPD servers.

Traffic logged to MY.NET.156.198 comes from 149 separate hosts. Connections are high port to low port from the MY.256.153 subnet. This looks like MY.NET.156.198 is a busy print server.

Traffic logged to MY.NET.1.163 comes from the hosts MY.NET.149.55 MY.NET.149.60, and MY.NET.149.27. The unusual thing about the traffic is that the source ports are all <1024. The pattern of the traffic otherwise is consistent for MY.NET.1.163 being a print server for the MY.NET.149.x subnet. This should be confirmed.

All traffic to MY.NET.153.184 comes from a single internal host with source port 22. This port is SSH and is indicative of SSH tunnelling of the LPR service occurring.

Recommendations:
Confirm that the three destination addresses are print servers and are patched.
Remove or limit this rule to prevent generation of an alert every time printer traffic is detected on the network.

References/Correlations:
David Leach noted this alert being triggered

http://www.giac.org/practical/David_Leach_GCIA.doc

Number 2 Alert: spp_http_decode: IIS Unicode attack detected

Unique Source Addresses	148
Unique Destination Addresses	857

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.151.108	28658	207.200.86.66	20241
MY.NET.153.127	5745	211.111.220.163	7614
MY.NET.153.147	5510	207.200.86.97	6762
MY.NET.153.110	4793	211.115.213.202	5659
MY.NET.153.193	4735	211.115.213.207	5064
MY.NET.153.182	4195	211.111.214.125	4156
MY.NET.153.145	3313	64.12.184.141	1951
MY.NET.153.171	3161	211.233.28.44	1424
MY.NET.153.149	2906	211.111.214.168	1346
MY.NET.152.161	2387	211.32.117.31	1260

The IIS Unicode attack exploits a vulnerability in unpatched IIS web servers which allows normally forbidden commands or directory traversals to pass if encoded as Unicode.

Only 32 of these many alerts were generated by external hosts.

The top destination is http://my.netscape.com/ (207.200.86.66) and (207.200.86.97)

Also in the top ten is http://home.netscape.com/ (64.12.184.141) and websites hosted by Korea Network Information Centre.

Randomly selecting destinations from further down the destination list locates a wide variety of foreign language websites.

The snort FAQ contains information on this alert and mentions netscape.com as being a trigger for this alert. http://www.snort.org/docs/faq.html#4.17

From the list of websites in the destination list the rule appears to be triggered by the large number of foreign language websites legitimately using Unicode.

Incoming alerts came from the following external hosts.

Count	Source IP
7	130.212.23.245

7	212.120.95.195
7	217.80.130.125
6	61.175.15.2
2	217.226.14.167
1	130.203.162.143
1	212.59.7.80
1	66.92.162.51

Checks should be made of all IIS webservers to check if vulnerable to this attack.

Recommendation: Seriously consider whether these alerts from the http_decode processor are worthwhile. It is suggested to at least ignore outgoing http traffic via the method recommended in the Snort FAQ:

```
snort -d -A fast -c snort.conf not (src net MY.NET and dst port 80)
```

http://rr.sans.org/threats/unicode.php
(CVE-2000-0884)
http://archives.neohapsis.com/archives/sf/ids/2001-q2/0281.html

Number 3 Alert SMB Name Wildcard

Unique Source Addresses	255
Unique Destination Addresses	282

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.11.7	12719	MY.NET.11.7	12727
MY.NET.11.6	12637	MY.NET.11.6	12593
MY.NET.11.5	4600	MY.NET.11.5	4575
MY.NET.152.158	820	MY.NET.152.158	835
MY.NET.152.163	787	MY.NET.152.163	787
MY.NET.152.157	742	MY.NET.5.4	753
MY.NET.152.167	680	MY.NET.152.157	748
MY.NET.152.160	649	MY.NET.152.167	684
MY.NET.152.171	631	MY.NET.152.160	652
MY.NET.152.184	616	MY.NET.152.171	629

SMB Name wildcards are a means of determining available windows shares on a network. All traffic was between MY.NET hosts except for 13 alerts from 169.254.22.29

A full description of the alert is at available from the SANS website:
http://www.sans.org/newlook/resources/IDFAQ/port_137.htm

Seeing this traffic between internal hosts is normal if file sharing is enabled. With the volume of traffic noted though there is a small possibility this is a worm exploiting shared drives. Description from CERT:

http://www.cert.org/incident_notes/IN-2000-02.html

Even if there is no worm infection there appears to be a great amount of SMB traffic on the network. This has the potential to open up many vulnerabilities especially if misconfigured to allow access to system drives.

Conducting a whois query on the seemingly external source host 169.254.22.29 reveals:

```
 IANA (NETBLK-LINKLOCAL)
   Internet Assigned Numbers Authority
   4676 Admiralty Way, Suite 330
   Marina del Rey, CA 90292-6695
   US

   Netname: LINKLOCAL
   Netblock: 169.254.0.0 - 169.254.255.255

   Coordinator:
     Internet Corporation for Assigned Names and Numbers  (IANA-ARIN)  res-
ip@iana.org
     (310) 823-9358

   Domain System inverse mapping provided by:

   BLACKHOLE-1.IANA.ORG              192.0.32.18
   BLACKHOLE-2.IANA.ORG              192.0.32.19

   Record last updated on 12-Oct-2001.
   Database last updated on  22-Mar-2002 19:57:54 EDT.
```

As can be seen these are reserved addresses. Research turned up the fact that unconfigured interfaces on Windows hosts are assigned 169.254.x.x addresses by default. This account for the anomalous host IP address being a misconfigured windows host.

http://archives.neohapsis.com/archives/incidents/2000-04/0042.html

Recommendation

Examine policy on use of SMB shares. Disable File and Print sharing if not required.

Correlations

This traffic has been seen in many recent practicals. In some practicals such as http://www.giac.org/practical/David_Leach_GCIA.doc this traffic was seen entering network from outside which is of greater concern. It appears that filtering at the border device is prventing external SMB traffic to enter the network which is good.

Number 4 Alert: MISC Large UDP Packet

Unique Source Addresses	40
Unique Destination Addresses	34

Top 10 Sources	Count	Top 10 Dests	Count
209.177.65.18	15840	MY.NET.152.168	5516
63.240.15.205	5464	MY.NET.152.163	5366
210.220.161.101	3817	MY.NET.153.197	5088
216.106.172.150	2176	MY.NET.152.169	4958
167.216.132.199	2018	MY.NET.152.12	4201
211.233.10.47	1933	MY.NET.153.182	3917
216.106.173.154	1741	MY.NET.153.210	2204
61.177.56.226	1620	MY.NET.152.167	2175
148.122.1.224	1527	MY.NET.153.141	1527
62.253.169.246	1411	MY.NET.152.184	1411

This alert is triggered by large sized (>4000) UDP packets. The rule is documented in the Snort Database. http://www.snort.org/snort-db/sid.html?id=521

This could attempts at denial of service through UDP flooding. (See CERT Advisory http://www.cert.org/advisories/CA-1996-01.html)
The other option is that UDP is being used to transport large quantities of data such as for streaming video or TFTP.

Examining the data in snortsnarf it appears that the rate of data whilst being quite high is not a credible DoS threat to a major university. To seriously conduct a UDP flood these days multiple hosts under the control of a master are usually used.

Shelby Gray in a previous practical http://www.giac.org/practical/Shelby_Gray_GCIA.zip indicated that sort traffic was likely a DoS attack. One of the items used as evidence was that many of the IP addresses came from Asia. In particular a number of 61.x.x.x source addresses were noted.

It is not believed sufficient that source adddresses in Asia to be used as theonly real criteria. There does appear to be significant amount of connections to foreign sites which is not unusual due to the multicultural nature of modern universities.

Number 5 Alert: ICMP Echo Request L3retriever Ping

Total of 30746 alerts, all of which from internal traffic.

This alert is generated from a snort rule looking for a particular pattern in a ICMP Echo request ("ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI")

http://www.snort.org/snort-db/sid.html?id=466

As noted on the snort mailing list this pattern is triggered by a standard Windows 2000 Ping.

http://archives.neohapsis.com/archives/snort/2001-08/1224.html

As such pings between internal users are of low concern. These alerts were not investigated further.

Recommendation: Turn off this rule.

Number 6 Alert: SNMP public access

Unique Source Addresses	17
Unique Destination Addresses	113

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.88.240	11901	MY.NET.150.195	11924
MY.NET.150.198	3326	MY.NET.152.109	5413
MY.NET.150.41	2298	MY.NET.151.114	1804
MY.NET.153.220	2000	MY.NET.153.219	1495
MY.NET.186.10	1399	MY.NET.150.84	583
MY.NET.150.245	787	MY.NET.88.187	97
MY.NET.88.225	554	MY.NET.88.160	96
MY.NET.150.197	306	MY.NET.104.200	58
MY.NET.150.49	263	MY.NET.150.231	35
MY.NET.84.155	161	MY.NET.88.240	34

This rule is designed to detect SNMP access from outside by detecting traffic to port 161 from $EXTERNAL_NET to $HOME_NET. The reference in the snort database is http://www.snort.org/snort-db/sid.html?id=1412

In the case of the network under test it is apparent that $EXTERNAL_NET is set to also encompass MY.NET and this rule is triggering off SNMP access internal to the network. The fact that there is no SNMP access from external to the network is a good sign.

Internally it appears SNMP is fairly heavily used. At the time of preparation of this report, vulnerabilities in SNMP have been made apparent as noted in the following CERT/CC advisory.

http://www.cert.org/advisories/CA-2002-03.html

This advisory recommends disabling SNMP where possible, patching systems and checking security of community strings. This should be carried out if it has not been already.

CVE reference for recent SNMP vulnerabilities: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012

Number 7 Alert: INFO MSN IM Chat data

This snort rule (from policy. rules) is triggered by external access to port 1863. This is indicative of use of the Microsoft Network Internet Messenger chat program.

This alert was triggered 18812 times. Noting MY.NET is a university usage of MSN IM is not surprising. This rule should be removed as it is not providing any useful intrusion detection. If use of MSN IM is not permitted due to local policy then port 1863 should be blocked at the firewall.

Number 8 Alert spp_http_decode: CGI Null Byte attack detected

Unique Source Addresses	23
Unique Destination Addresses	17

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.153.197	6116	209.10.239.135	12698
MY.NET.153.150	3245	216.241.219.14	3659
MY.NET.153.176	2497	216.241.219.22	1637
MY.NET.153.210	2258	192.151.52.111	282
MY.NET.152.20	1673	MY.NET.5.96	235
MY.NET.153.146	1401	199.104.95.15	58
MY.NET.153.199	840	192.151.52.164	43
MY.NET.153.186	325	216.33.88.53	32
MY.NET.222.154	112	63.251.152.70	31
MY.NET.223.102	110	205.188.180.57	13

Despite the large number of alerts there are relatively few source and destination addresses.

The number 1 destination is www.ifilm.com a source of short films and trailers.

This signature is well known for high false positives. It is very similar to the Unicode attack above. In this case however Null byte (Bytes with value 0x00) are included which in some web servers allows bypassing of security controls.

The snort FAQ contains information on this alert.

```
Q What about "CGI Null Byte attacks"?
```

A: It's a part of the http preprocessor. Basically, if the http decoding routine finds a %00 in an http request, it will alert with this message. Sometimes you may see false positives with sites that use cookies with urlencoded binary data, or if you're scanning port 443 and picking up SSLencrypted traffic . If you're logging alerted packets you can check the actual string that caused the alert. Also, the unicode alert is subject to the same false positives with cookies and SSL. Having the packet dumps is the only way to tell for sure if you have a real attack on your hands, but this is true for any content-based alert

--- SNORT FAQ http://www.snort.org/docs/faq.html#4.17

Like Unicode it does not appear worthwhile to have an alert triggered for this for outgoing http connections. Probability of identifying as internal user attacking an external host is minimal noting the positive rate from normal web traffic

The one external source of this alert was 12.91.164.13 which generated 13 alerts against internal host MY.NET.5.96 over a period of 20 seconds.

Whois query for 12.91.164.13 (13.washington-31rh15rt.dc.dial-access.att.net)

AT&T ITS (NET-ATT)
200 Laurel Avenue South
Middletown, NJ 07748
US

Netname: ATT
Netblock: 12.0.0.0 - 12.255.255.255
Maintainer: ATTW

Coordinator:
Kostick, Deirdre (DK71-ARIN) help@IP.ATT.NET
(888)613-6330

Domain System inverse mapping provided by:

DBRU.BR.NS.ELS-GMS.ATT.NET199.191.128.106
DMTU.MT.NS.ELS-GMS.ATT.NET12.127.16.70
CBRU.BR.NS.ELS-GMS.ATT.NET199.191.128.105
CMTU.MT.NS.ELS-GMS.ATT.NET12.127.16.69

Record last updated on 06-Nov-2000.
Database last updated on 22-Mar-2002 19:57:54 EDT.

This alert is of concern as it may be a possible attack upon the web server. No other types of alerts were logged during the 5 day period for this attacker.

Recommendations

Turn off logging for this alert for outbound http traffic as discussed in Snort FAQ.

Check that web server MY.NET.5.96 is up to date with current patches If possible check web server logs of this server for session with 12.91.164.13 to check if any compromise occurred.

Number 9 Alert: High port 65535 udp - possible Red Worm – traffic

Unique Source Addresses	201
Unique Destination Addresses	180

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.6.49	2615	MY.NET.152.179	253
MY.NET.6.52	1974	MY.NET.153.187	202
MY.NET.6.48	1849	MY.NET.152.159	197
MY.NET.6.50	1571	MY.NET.152.171	191
MY.NET.6.60	185	MY.NET.153.193	187
MY.NET.6.53	160	MY.NET.153.177	186
MY.NET.6.45	127	MY.NET.152.170	186
MY.NET.60.43	86	MY.NET.152.173	159
12.25.239.5	63	MY.NET.152.160	157
64.124.157.32	48	MY.NET.152.21	154

Number 10 Alert: Watchlist Activity

Watchlist IL-ISDNNET-990517

This watchlist rule targeting an Israel ISP is not included in the current rule set. This rule dates back to 17-May-1999, almost 3 years ago.

Traffic logged to from this site is either web traffic to www.imesh.com (imesh is a peer to peer client) or KAZAA file sharing traffic on port 1214. Neither of which are particular surprising or of great concern for a university network.

What is of concern is the inclusion of this old snort rule in the rule set. Checks should be made as to which snort rules are / are not running. This rule should be removed unless there is evidence of particular concern from this ISP.

Correlation:
Mentioned in numerous GCIA practicals including:
http://www.giac.org/practical/David_Oborn_GCIA.html#watchlist

Back at this time it was Napster traffic instead of Kazaa though.

Watchlist NET 000219
This watchlist picks up traffic from a different ISDN net IP range. The only traffic to/ from this range is to the Israel Defence Force home page.

Rule should be removed.

Watchlist 000222 NET-NCFC
This watchlist flags traffic from Chinese Academy of Sciences.
There is a small number of these alerts. Most is Napster but there is one anomalous transaction.

```
02/20-18:53:47.275836  [**] NMAP TCP ping! [**] 159.226.208.40:80 ->
MY.NET.88.215:16200
02/20-18:53:47.277013  [**] Watchlist 000222 NET-NCFC [**]
159.226.208.40:1048 -> MY.NET.88.215:16200
02/20-18:53:47.544062  [**] Watchlist 000222 NET-NCFC [**]
159.226.208.40:1048 -> MY.NET.88.215:16200
```

Other (Possibly) Significant Alerts

(Note: only selected Alerts of interest examined)

Alert: MYPARTY - Possible My Party infection

Rank	Total # Alerts	**Source IP**	# Signatures triggered	Destinations involved
Rank #1	1437 alerts	**MY.NET.153.143**	1 signatures	209.151.250.170
Rank #2	69 alerts	**MY.NET.153.188**	1 signatures	209.151.250.170

Two hosts appear to be infected with the "MYPARTY" virus.

This is a windows virus spread via email attachment. The virus also attempts to contact the host 209.151.250.170 to activate a back door.

Although there does not appear to be a listing for this in the standard snort rule set. The alert would have been triggered by the attempted connections to 209.151.250.170.

A full description on the virus can be found at.
http://securityresponse.symantec.com/avcenter/venc/data/w32.myparty@mm.html

These hosts should be cleaned of the virus and a up to date virus scanner installed.

Alert: Possible trojan server activity

Host MY.NET.5.83 appears to be exploiting Trojan software installed on four other internal machines:

```
02/20-05:04:59.221127 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.77:27374
02/20-05:04:59.269475 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.77:27374
02/20-05:04:59.302591 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.77:27374
02/20-05:04:59.312434 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.77:27374
02/21-01:19:39.770878 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.5.29:27374
02/21-01:19:39.771194 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.5.29:27374
02/21-01:19:39.771327 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.5.29:27374
02/21-01:19:39.771394 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.5.29:27374
02/21-10:55:18.961959 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.58:27374
02/21-10:55:18.985742 [**] Possible trojan server activity [**]
MY.NET.5.83:8330 -> MY.NET.5.58:27374
```

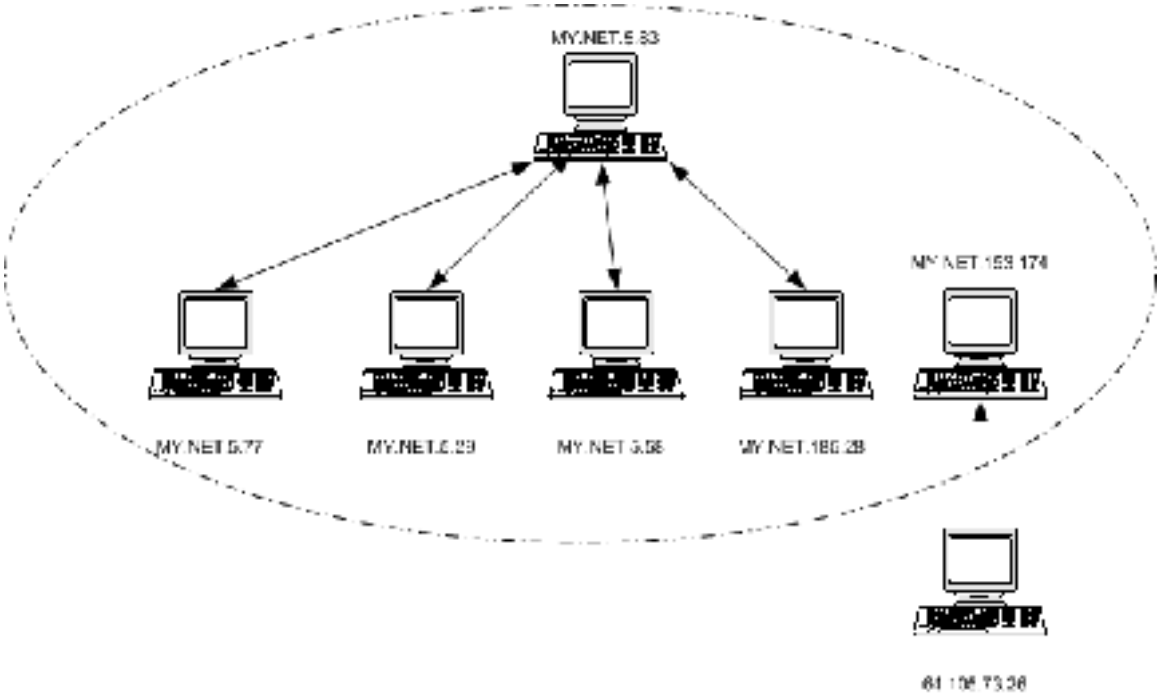
```
02/21-12:57:43.460816 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.185.28:27374
02/21-12:57:43.462625 [**] Possible trojan server activity [**]
MY.NET.5.83:7938 -> MY.NET.185.28:27374
02/23-13:05:50.322378 [**] Possible trojan server activity [**]
MY.NET.5.83:9321 -> MY.NET.5.77:27374
02/23-13:05:50.349040 [**] Possible trojan server activity [**]
MY.NET.5.83:9321 -> MY.NET.5.77:27374
02/23-13:05:50.350541 [**] Possible trojan server activity [**]
MY.NET.5.83:9321 -> MY.NET.5.77:27374
02/23-13:05:50.360474 [**] Possible trojan server activity [**]
MY.NET.5.83:9321 -> MY.NET.5.77:27374
```

The infected machines are:
MY.NET.5.77
MY.NET.185.28
MY.NET.5.58
MY.NET.5.29

This rule was triggered by UDP traffic going to/from UDP port 27374, a well known Trojan port. This port is used by at least the following trojans: Bad Blood, SubSeven , SubSeven 2.1 Gold, SubSeven 2.1.4 DefCon 8.

The owners of the infected machines should be notified and the trojan programs removed. Investigation into who the attacker using machine MY.NET.5.83 is, and their motives should be a high priority. Once the trojan in question is fully identified a full search of the network should be conducted for other infected hosts. Other hosts may be infected but the backdoor not utilised during the timeframe of these logs.

Note there were occasional spurious attempted connections to 27374 from some other hosts but as no response was received it was ignored as part of the "background noise".



Link graph of UDP port 27374 traffic

The above link graph shows clearly who the central host is in the possible trojan use. The one way nature of the traffic to MY.NET.153.174 and the fact there are no other connections to/from wither hosts allows the traffic to be assigned a low priority for examination.

References:

1. "What port numbers do well-known trojan horses use?" Joakim von Braun URL http://www.sans.org/newlook/resources/IDFAQ/oddports.htm (March 10, 2002)

Alert: IIS Attacks

Signature	Alerts	#Sources	Dests
WEB-IIS asp-dot attempt	2	1	1
WEB-IIS Unauthorized IP Access Attempt	2	1	1
WEB-IIS encoding access	3	2	1
IDS552/web-iis_IIS ISAPI Overflow ida nosize	12	12	7
WEB-IIS _vti_inf access	415	148	2
WEB-IIS view source via translate header	1555	60	2

Unique Source Addresses	148
Unique Destination Addresses	7

Top 10 Sources	Count	Dests	Count
68.33.210.35	95	MY.NET.5.96	1967
208.58.225.238	70	MY.NET.150.83	11
141.157.124.123	70	MY.NET.5.79	3
68.55.180.51	62	MY.NET.5.92	2
68.50.29.89	62	MY.NET.5.241	2
68.55.0.142	60	130.212.23.245	2
68.55.205.170	57	MY.NET.5.97	1
63.208.190.96	51	MY.NET.5.95	1
64.198.134.166	48		
172.129.187.218	43		

These alerts are triggered by attempts on known exploits for the Microsoft IIS Web Server. IIS has had more than its share of problems over the past few years. There is a high level of "background noise" of attempts to exploit these vulnerabilities both by worms and scripts.

Patches available from Microsoft (www.microsoft.com) cure all vulnerabilities related to these alerts.

Most of the alerts were generated by traffic to MY.NET.5.96 and are related to the Front Page extensions. (WEB-IIS _vti_inf access and WEB-IIS view source via translate header)

Recommendations

As a priority examine web server MY.NET.5.96 and ensure it is patched and correctly configured. See discussion of this host under top talkers list in the next section.

Other destination hosts should be examined. If they are running IIS then patch level should be confirmed.

http://www.securiteam.com/windowsntfocus/Translate_f_vulnerability_exposes_IIS_files_source.html

Alert: FTP DoS Globbing

Unique Source Addresses	9
Unique Destination Addresses	7

Sources	Count	Dests	Count
66.54.213.252	712	MY.NET.153.190	712
208.194.4.82	114	MY.NET.150.46	173
80.134.239.123	108	MY.NET.153.157	60
128.252.105.75	61	MY.NET.153.180	54
147.226.221.227	51	MY.NET.153.197	51
206.213.40.100	30	MY.NET.153.152	36
66.20.28.21	7	MY.NET.153.194	7
155.225.149.222	6		
192.160.165.63	4		

There are known vulnerabilities in various ftp servers relating to filename globbing (the use of wildcards). The destination hosts may need to be checked that they are patched and up to date. The sheer quantity of the alerts may be indicative of a false positive.

Vulnerability references:
http://www.eeye.com/html/Support/Retina/RTHs/FTP_Servers/815.html
http://online.securityfocus.com/advisories/3701

BUGTRAQ ID: CA-2001-33
CVE-MITRE: CAN-2001-0550

Primary source host:

University of California San Francisco (NETBLK-UCSF-2NET)
250 Executive Park Blvd., #2100
San Francisco, CA 94134
US

Netname: UCSF-2NET
Netblock: 64.54.0.0 - 64.54.255.255

Coordinator:
Koehler, Charles Walter (CWK1-ARIN) cwk@itsa.ucsf.edu
415-476-8767 (FAX) 415-502-8185

Domain System inverse mapping provided by:

UCSFNS1.UCSF.EDU 128.218.254.10
UCSFNS2.UCSF.EDU 128.218.254.40

Record last updated on 19-Apr-2000.

Database last updated on 24-Mar-2002 19:56:58 EDT.

Alert: BACKDOOR NetMetro File List

```
Logged traffic:

02/21-15:21:06.778255  [**] BACKDOOR NetMetro File List [**]
MY.NET.153.194:1329 -> 129.22.41.183:5032
02/21-15:21:54.951694  [**] BACKDOOR NetMetro File List [**]
MY.NET.153.194:1329 -> 129.22.41.183:5032
```

Rule triggering: http://www.snort.org/snort-db/sid.html?id=159

alert tcp $HOME_NET any -> $EXTERNAL_NET 5032 (msg:"BACKDOOR NetMetro File List"; flags: A+; content:"|2D 2D|"; reference:arachnids,79; sid:159; classtype:misc-activity; rev:3;)

NETMETRO is a trojan program which listens on TCP Port 5032.

This alert is triggered by traffic to an external host with the bytes 2D 2D somewhere in the packet.

It is possible that MY.NET.153.194:1329 is connecting to an infected host external to the network. There is also a probability this is just a coincidence.

Performing a whois on the target:

Case Western Reserve University
(NET-CWRUNET)
Campus Communications Network - Network Services
Crawford Hall, Room 426
Cleveland, OH 44106
US

Netname: CWRUNET
Netblock: 129.22.0.0 - 129.22.255.255

Coordinator:
Gumpf, Jeffrey A (JAG3-ARIN) Gumpf@INS.CWRU.EDU
(216) 368-2982

Domain System inverse mapping provided by:

NS.CWRU.EDU	129.22.4.1
NS2.CWRU.EDU	129.22.4.3

NCNOC.NCREN.NET 192.101.21.1

Record last updated on 22-Oct-1999.
Database last updated on 23-Mar-2002 19:56:37 EDT.

The target is another university computer.

Noting the IP of the target is not noted elsewhere in other practicals, Google or elsewhere in alerts this more likely to be a false alert.

The high port – high port connection at first glance seems strange but this could be anything from an online game, to a chat program using dynamic ports fro transferring data. With a signature on average 1 in 65535 pairs of bytes will trigger this alert if the port 5032 is allocated to a connection.

Alert: Fragmentation

Signature	# Alerts	# Sources	# Dests
Tiny Fragments - Possible Hostile Activity	129	3	3
Incomplete Packet Fragments Discarded	586	12	5
ICMP Fragment Reassembly Time Exceeded	1243	56	84

Top 10 Sources	Count	Top 10 Dests	Count
202.103.214.71	545	MY.NET.152.11	545
MY.NET.88.165	199	61.150.5.19	199
MY.NET.150.120	180	211.233.10.47	192
68.36.9.212	119	12.25.239.5	163
MY.NET.88.181	101	MY.NET.88.162	125
MY.NET.153.152	100	211.174.59.74	84
MY.NET.152.176	87	211.233.70.162	68
MY.NET.153.171	86	211.106.66.156	52
MY.NET.153.165	82	211.233.27.144	42
MY.NET.153.145	67	211.233.27.142	36

The number one source and destination are linked. There is a large amount of UDP traffic passing between these hosts and alerts are triggered for large ICMP packets and fragments discarded.

Earliest alert at **15:35:23**.645349 *on 02/21/2002*
Latest alert at **16:00:25**.491464 *on 02/21/2002*

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	High port 65535 udp - possible Red Worm - traffic	1	1	1	Summary
N/A	ICMP Fragment Reassembly Time Exceeded	2	1	1	Summary
N/A	Incomplete Packet Fragments Discarded	545	1	1	Summary
N/A	MISC Large UDP Packet	1266	1	1	Summary

In a short period of time there was a large transfer of information between these hosts using large UDP packets. Fragmentation was necessary and along the way fragments were lost. This could be malicious activity or it could be high bandwidth straming media. It is not unusual for a proportion of packets to be lost in high bandwidth applications. When fragmentation is occurring the loss of a single fragment will result is the Incomplete Packet Fragments Discarded alert.

Tiny Fragments

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
68.36.9.212	119	119	1	1
218.183.116.26	6	6	1	1
68.42.17.243	4	4	1	1

Tiny fragments are indications of either malicious activity or of the need to pass through a network segment with a small maximum segment size. These days most connections handle the Ethernet MSS of approx 1500 bytes so really small fragments may be attempts to attack by braking up a possible attack signature to avoid IDS or firewall detection or to crash older TCP/IP stack which cannot handle crafted situations like overlapping fragments.

It could be also an attempt at a Denial of Service by forcing the recipient to expend processing time and temporary storage in the reassembly process. This is what the host 68.36.9.212 may be attempting to achieve. After the flood of tiny fragments over a few seconds the recipient MY.NET.88.162 responds with ICMP messages indicating Reassembly time exceeded. This may be because the host has been temporarily overwhelmed.

Out of Spec Fragmentation
The OOS file also contained information showing possible malicious fragmentation of packets such as the following:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+0
2/23-16:46:26.737195 64.171.1.236 -> MY.NET.150.145
TCP TTL:108 TOS:0x0 ID:12390  DF MF
Frag Offset: 0x0   Frag Size: 0x22
25 17 72 39 2D CA FF 49 D0 DE B5 C3 B3 CE 50 57  %.r9-..I......PW
F9 E8 65 CC 1D 76 9E 26 DD B8 EC BC 41 E2 96 E6  ..e..v.&....A...
7F 93                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/23-16:46:28.314320 64.171.1.236 -> MY.NET.150.145
TCP TTL:108 TOS:0x0 ID:12404  DF MF
Frag Offset: 0x0   Frag Size: 0x22
25 17 72 39 2D CA FF 49 D0 DE B5 C3 B3 CE 50 57  %.r9-..I......PW
F9 E8 65 CC 1D 76 9E 26 DD B8 EC BC 41 E2 96 E6  ..e..v.&....A...
7F 93                                            ..
```

These packets show signs of packet craft having such a small fragment size. There is no details of any subsequent fragments. This may mean they were not sent or that they were not flagged as out of spec.

This traffic could either be a DoS attack or a fingerprint attempt.

Alert: NIMDA - Attempt to execute cmd from campus host

02/19-16:22:49.876764 [**] NIMDA - Attempt to execute cmd from campus host [**] MY.NET.88.137:1127 -> 207.46.235.160:80

This host was being flagged as a NIMDA infected host. This is a local rule but from the description I take it to have been triggered by a CMD.exe attempt from a host within MY.NET.

The target is http://www.microsoft.com/downloads/search.asp?
I would assume this is a false alarm. If the host was infected by NIMDA there would be more alerts than this. It is also unlikely given the target that this is a successful exploit (hopefully!).

Details of Nimda:
http://www.incidents.org/react/nimda.pdf

Recommendation: Ignore

Top Talkers List

Top ten source IP's for alerts (not including portscans)

Top 10 Sources	Count	Top 10 Dests	Count
MY.NET.151.108	28662	MY.NET.150.198	167270
MY.NET.153.106	22718	MY.NET.11.7	27989
209.177.65.18	15840	MY.NET.11.6	27457
MY.NET.153.119	13494	207.200.86.66	20241
MY.NET.11.7	12719	209.10.239.135	12698
MY.NET.11.6	12637	MY.NET.150.195	11943
MY.NET.153.114	12110	MY.NET.11.5	9246
MY.NET.88.240	11903	211.111.220.163	7614
MY.NET.153.117	8727	207.200.86.97	6762
MY.NET.153.110	8240	MY.NET.152.163	6190

Top 10 Port Scan Source	
MY.NET.60.43	434328
MY.NET.6.45	144682
MY.NET.60.11	71940
MY.NET.6.49	63451
MY.NET.6.52	50614
MY.NET.152.22	50196
MY.NET.6.48	49586
MY.NET.6.53	46569
MY.NET.6.60	46156
MY.NET.6.50	39959

The idea of a top talkers list is to try and identify hosts of interest. The raw top-talkers list as it stands is not particularly good at this. As discussed in the alerts section, many of the top occurring alerts are actually false positives triggered by normal net usage such as using a printer, accessing a page using Unicode or using MSN IM.

For instance the top alert source (MY.NET.151.108) was the source for 28662 alerts. Of these all but 13 were Unicode alerts triggered by using www.netscape.com or foreign language sites.

In order to make a more meaningful top talkers list the following alert types were excluded:

Alert	Reason
connect to 515 from inside	False positive on printer usage
spp_http_decode:	High false positive from normal web traffic
SMB Name Wildcard	High false positive from windows shares
MISC Large UDP Packet	Includes valid streaming Media

All Echo alerts	Low priority
All INFO alerts	File sharing / MSN IM usage
SNMP Public Access	Triggered by internal SNMP use
Watchlist	Out of date lists

After filtering, 21441 alerts remained and the following "top talkers" list was obtained:

Top 10 Sources	**Count**	**Top 10 Dests**	**Count**
MY.NET.6.49	2624	MY.NET.5.96	2904
MY.NET.6.52	1988	224.0.0.2	1713
MY.NET.6.48	1869	209.151.250.170	1506
MY.NET.6.50	1579	MY.NET.153.190	794
MY.NET.153.143	1437	MY.NET.152.11	581
66.54.213.252	712	MY.NET.88.162	276
202.103.214.71	546	MY.NET.152.179	255
61.142.242.218	470	MY.NET.150.137	212
208.51.213.254	403	MY.NET.152.159	208
208.46.44.160	378	MY.NET.153.187	205

A side benefit was that the resulting filtered list was short enough to make analysis via Snortsnarf practical.

Sources 1-4 (MY.NET.6.x)

The top four sources interestingly are all on the same subnet and have almost contiguous IP addresses.

Rank	Total # Alerts	**Source IP**	# Signatures triggered	Destinations involved
Rank #1	2624 alerts	**MY.NET.6.49**	4 signatures	(120 destination IPs)
Rank #2	1988 alerts	**MY.NET.6.52**	5 signatures	(110 destination IPs)
Rank #3	1869 alerts	**MY.NET.6.48**	5 signatures	(114 destination IPs)
Rank #4	1579 alerts	**MY.NET.6.50**	4 signatures	(112 destination IPs)

For the top-talker:

4 different signatures are present for *MY.NET.6.49* as a source

- 2 instances of *ICMP Fragment Reassembly Time Exceeded*
- 2 instances of *Attempted Sun RPC high port access*

- 5 instances of *Back Orifice*
- 2615 instances of *High port 65535 udp - possible Red Worm - traffic*

(#2 and #3 hosts have very similar alert patterns but also have one instance of Port 55850 udp - Possible myserver activity - ref. 010313-1)

The activity coming from these four hosts is definitely suspicious. Port 65535 is indicative of backdoor traffic associated with the Adore Worm (also known as Red worm). Each host also attempts to connect to port 31337 which is a well known backdoor port.

Two options:

1. These four hosts are infected or being used as attack platforms.
2. These hosts are vulnerability scanners.

Either way these four hosts need to be examined. Details on the Adore worm can be found from SANS at http://www.sans.org/y2k/adore.htm including links to utilities for locating infected hosts.

Source 5 (MY.NET.153.143)

Source #5 is one of two MYPARTY infected hosts identified in the alerts section.

Source 6 (64.54.213.252)

See FTP DoS Globbing in Alerts Section

Source 7 (202.103.214.71)

See Incomplete Packet Fragments Discarded in Alerts Section

Source 8 (61.142.242.218)

Source #8 is a proxy scanner scanning 306 different hosts.

This is fairly common behaviour. Not of particular concern unless open proxies are running on the site. It may be beneficial to block access to proxy ports at the firewall.

```
% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois7.apnic.net)

inetnum:     61.140.0.0 - 61.143.255.255
netname:     CHINANET-GD
descr:       CHINANET Guangdong province network
descr:       Data Communication Division
descr:       China Telecom
```

country: CN
admin-c: CH93-AP
tech-c: WM12-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-GD
changed: hostmaster@ns.chinanet.cn.net 20000601
source: APNIC

person: Chinanet Hostmaster
address: A12,Xin-Jie-Kou-Wai Street
country: CN
phone: +86-10-62370437
fax-no: +86-10-62053995
e-mail: hostmaster@ns.chinanet.cn.net
nic-hdl: CH93-AP
mnt-by: MAINT-CHINANET
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: WU MIAN
address: NO.1,RO.DONGYUANHENG,YUEXIUNAN,GUANGZHOU
country: CN
phone: +086-20-83877223
fax-no: +86-20-83877223
e-mail: ipadm@gddc.com.cn
nic-hdl: WM12-AP
mnt-by: MAINT-CHINANET-GD
changed: ipadm@gddc.com.cn 20010820
source: APNIC

This particular IP address is not found in previous practicals or the DSHIELD database but performing a google search locates numerous logs from proxy servers all over the world with this IP address as a listed user indicating that the scanning is turning up open proxies.

Source 9 (208.51.213.254)

Source 9 conducted a SYN-FIN scan of 403 hosts on MY.NET on 22/2/02. An example scan is

02/22-14:45:53.475599 [**] SYN-FIN scan! [**] 208.51.213.254:21 -> MY.NET.5.25:21

The attributes of SYN-FIN and mirrored source and destination ports is quite common is scanning software.

No other alerts are triggered from this host.

Global Crossing (NET-GBLX-6)
960 Hamlin Court
Sunnyvale, CA 94089
US

Netname: GBLX-6
Netblock: 208.48.0.0 - 208.51.255.255
Maintainer: GBLX

Coordinator:
Global Crossing (IA12-ORG-ARIN) ipadmin@gblx.net
+1 800 404-7714

Domain System inverse mapping provided by:

NAME.ROC.GBLX.NET209.130.187.10
NAME.PHX.GBLX.NET206.165.6.10

No correlations for this IP address was found except that it at one stage hosted a MUD (Multi User Dungeon) game.

http://www.users.voicenet.com/~redlace/Resume.htm

Source 10 (208.46.44.160)

Very similar pattern to Source 9. Both IP addresses start with 209 but belong to different organisations. There is a significant amount of traffic from 209.x.x.x. This may be cooincidnece or due to a relationship between the IP numbers of MY.NET and 209.x.x.x Noting most scanning tools begin targetting IP numbers close to the attackers.

Destination 1 (MY.NET.5.96)

Earliest: 03:27:50.777636 on 02/19/2002
Latest: 23:44:54.552699 on 02/23/2002

17 different signatures are present for MY.NET.5.96 as a destination

2 instances of High port 65535 tcp - possible Red Worm - traffic
2 instances of IDS552/web-iis_IIS ISAPI Overflow ida nosize
2 instances of WEB-IIS asp-dot attempt
3 instances of WEB-IIS encoding access
3 instances of SCAN Proxy attempt
3 instances of WEB-MISC ICQ Webfront HTTP DOS
3 instances of SYN-FIN scan!
7 instances of WEB-MISC http directory traversal
8 instances of Port 55850 tcp - Possible myserver activity - ref. 010313-1

15 instances of WEB-MISC Attempt to execute cmd
31 instances of WEB-CGI phf access
70 instances of WEB-CGI csh access
161 instances of WEB-CGI ksh access
239 instances of WEB-CGI scriptalias access
395 instances of WEB-FRONTPAGE _vti_rpc access
409 instances of WEB-IIS _vti_inf access
1551 instances of WEB-IIS view source via translate header

There are 246 distinct source IPs in the alerts.

Something is wrong here! This web server is triggering alerts for a number of CGI and frontpage vulnerabilities.

This server could be taking hits as it may be the main web-server of the organisation but even still the number of Frontpage and cgi related alerts is of concern.

Recommendation:

Thoroughly audit this web server. It appears to be an IIS box so ensuring it is patched to latest version is vital. A number of the alerts relate to Front Page extensions. If not required these extensions should be turned off.

Destination 2 (224.0.0.2)

1 different signatures are present for 224.0.0.2 as a destination
1713 instances of ICMP Router Selection

224.0.0.2 is a multicast address. By default windows hosts attempt router discovery via this multicast address as discussed in:

http://www.nwconnection.com/2001_03/ICMP/

This behaviour does not appear malicious or dangerous. Whether it indicates a configuration problem is a matter for examination

Destination 3 (209.151.250.170)

1 different signatures are present for 209.151.250.170 as a destination
1506 instances of MYPARTY - Possible My Party infection

The host number 209.151.250.170 is hard coded into the MYPARTY virus. Infected hosts attempt to contact this IP address. As discussed in the alerts section 2 hosts are infected in MY.NET triggering the 1506 alerts.

Destination 4 (MY.NET.153.190)

Earliest: 09:51:31.644918 on 02/19/2002
Latest: 16:57:22.053814 on 02/22/2002

6 different signatures are present for MY.NET.153.190 as a destination

1 instances of Attempted Sun RPC high port access
1 instances of EXPLOIT x86 setuid 0
2 instances of SYN-FIN scan!
14 instances of SCAN Proxy attempt
64 instances of High port 65535 udp - possible Red Worm - traffic
712 instances of FTP DoS ftpd globbing

There are 17 distinct source IPs in the alerts.

This host made the top 10 because of the FTP DoS ftpd globbing alerts discussed in the alerts section.

Destination 5 (MY.NET.152.11)

Earliest: 11:55:49.835167 on 02/19/2002
Latest: 14:52:08.181985 on 02/22/2002

5 different signatures are present for MY.NET.152.11 as a destination

1 instances of Back Orifice
2 instances of SYN-FIN scan!
3 instances of SCAN Proxy attempt
30 instances of High port 65535 udp - possible Red Worm - traffic
545 instances of Incomplete Packet Fragments Discarded

See "Fragmentation" in the alerts section

Destination 6 (MY.NET.88.162)

Earliest: 12:39:22.883384 on 02/19/2002
Latest: 13:59:29.101828 on 02/23/2002

11 different signatures are present for MY.NET.88.162 as a destination

1 instances of External RPC call
1 instances of EXPLOIT x86 setuid 0
2 instances of SCAN Proxy attempt
3 instances of SYN-FIN scan!
3 instances of High port 65535 tcp - possible Red Worm - traffic
6 instances of Incomplete Packet Fragments Discarded
9 instances of Port 55850 tcp - Possible myserver activity - ref. 010313-1

12 instances of MISC traceroute
37 instances of NMAP TCP ping!
83 instances of Null scan!
119 instances of Tiny Fragments - Possible Hostile Activity

See discussion of Fragmentation in the alerts section.

Destination 7 (MY.NET.152.179)

Earliest: 09:28:01.146066 on 02/19/2002
Latest: 10:00:15.544476 on 02/23/2002

2 different signatures are present for MY.NET.152.179 as a destination

2 instances of SYN-FIN scan!
253 instances of High port 65535 udp - possible Red Worm - traffic

There are 7 distinct source IPs in the alerts.

Recommendation: Scan this host for the Adore worm discussed earlier. The amount of traffic to port 65535 should be identified.

Destination 8 (MY.NET.150.137)

Earliest: 11:35:25.564704 on 02/19/2002
Latest: 12:53:25.458989 on 02/23/2002

3 different signatures are present for MY.NET.150.137 as a destination

1 instances of SCAN Proxy attempt
2 instances of SYN-FIN scan!
209 instances of Null scan!

Destination host for scanning.

Destination 9 (MY.NET.152.159)

Earliest: 08:08:47.723848 on 02/19/2002
Latest: 16:55:03.223693 on 02/23/2002

5 different signatures are present for MY.NET.152.159 as a destination

1 instances of EXPLOIT x86 setgid 0
1 instances of Queso fingerprint
2 instances of SYN-FIN scan!
7 instances of SCAN Proxy attempt

197 instances of High port 65535 udp - possible Red Worm - traffic

There are 13 distinct source IPs in the alerts of the type on this page.

Recommendation: Scan this host for the Adore worm discussed earlier. The amount of traffic to port 65535 should be identified.

Destination 10 (MY.NET.153.187)

Earliest: 17:59:43.701863 on 02/19/2002
Latest: 16:11:35.588224 on 02/23/2002

3 different signatures are present for MY.NET.153.187 as a destination

1 instances of EXPLOIT x86 setgid 0
2 instances of SYN-FIN scan!
202 instances of High port 65535 udp - possible Red Worm – traffic

Recommendation: Scan this host for the Adore worm discussed earlier. The amount of traffic to port 65535 should be identified

Port Scans

UDP and SYN scans were omitted from the analysis due to the high number of false positives generated by these scans.

Top Source and Destinations

Top 10 Scan Sources		Top 10 Scan Dests	
208.51.213.254	403	MY.NET.150.133	1789
208.46.44.160	378	MY.NET.88.162	222
MY.NET.186.16	217	MY.NET.150.137	211
64.105.73.26	168	MY.NET.153.174	170
148.63.147.90	77	MY.NET.150.41	105
148.64.28.108	71	MY.NET.150.247	69
148.64.24.52	71	MY.NET.150.145	27
148.64.83.144	64	MY.NET.150.220	24
148.64.12.190	64	MY.NET.5.96	11
148.63.92.238	60	MY.NET.150.44	8

Most of the scan destinations and sources have been seen previously in alert lists for things such as NULL scans etc. The exception is the host MY.NET.150.133. At first it was suspected there was an error in the scripts that produced this table as this host received more scans were produced from the top 10 sources.

Examining the files however a large number of logged packets of the following form were present.

```
Feb 19 03:58:50 148.63.132.41:3398 -> MY.NET.150.133:1214 VECNA ****P***
Feb 19 10:41:30 148.63.221.13:3124 -> MY.NET.150.133:1214 VECNA ****P***
Feb 19 13:42:33 148.63.76.13:4409 -> MY.NET.150.133:1214 VECNA ****P***
Feb 19 14:33:53 148.63.233.97:3229 -> MY.NET.150.133:1214 VECNA ****P***
Feb 19 16:05:41 148.63.214.244:1404 -> MY.NET.150.133:1214 VECNA
****P***
Feb 19 16:09:51 148.63.234.10:3839 -> MY.NET.150.133:1214 VECNA ****P***
Feb 19 16:28:01 148.63.233.145:2336 -> MY.NET.150.133:1214 VECNA
****P***
Feb 19 16:42:45 148.63.225.163:4134 -> MY.NET.88.162:1214 VECNA ****P***
Feb 19 16:43:31 148.63.225.163:4134 -> MY.NET.88.162:1214 VECNA ****P***
Feb 19 16:51:44 148.63.87.125:2356 -> MY.NET.150.133:1214 SYN ******S*
```

The incoming VECNA ****P*** packets are coming from a wide range of hosts in the 148.63 and 148.64 address ranges aimed at port 1214, the port used by the Kazaa file sharing program. This also explains the presence of these entries in the source lists.

The only correlations able to be found were the following message board discussions:

http://archives.neohapsis.com/archives/snort/2002-01/0127.html
http://www.ultraviolet.org/mail-archives/snort-users.2001/1687.html

These posts confirm this traffic is related to KAZAA file sharing client which is not in itself of great concern.

Scan Types

FIN	7
FULLXMAS	2
INVALIDACK	62
NMAPID	3
NOACK	76
NULL	352
SPAU	2
SYNFIN	810
UNKNOWN	42
VECNA	2085
XMAS	3

Ignoring the VECNA scans related to Kazaa almost the full range of possible scans present. Most were logged as scans in the alerts section and are indicative of attempts to fingerprint the Operating System or avoid triggering a firewall or IDS.

Fingerprinting works by examining the response of these invalid combinations of flags. As the behaviour is not fully defined by the relevant RFC's each implementation of the TCP/IP stack reacts differently. Tools such as nmap can successfully narrow down an operating system type from the returns.

Other combinations of flags can be used as reconnaissance. Many simple firewall implementations filter only SYN packets. Probes which do not have the SYN flag set will pass straight through and not be logged. Similarly if the byte value of the flags in the packet is checked rather than the just the SYN bit a dumb firewall may let through a SYN/FIN which is treated as a lone SYN by many operating systems.

Out Of Spec OOS files

The out of spec (OOS) file contain packet dumps of packets found to not meet "normal requirements"

Analysing the files by hand they primary consist of the following:

- SYN/FIN (predominate type)
- Strange fragmentation
- Unusual combination of Flags or TCP options

The SYN/FIN scans are characteristic of many portscanning tools. Alerts were generated for SYN/FIN scans.

Fragmentation has been previously discussed. The data from these OOS files assisted in analysis of some of the fragmentation alerts.

Searching for the source hosts for other unusual combinations of flags determined that these had been captured in the logs under portscans and detailed in the tables in the previous section.

Analysis Method

Noting that analysis of snort logs is often repeated task I sought out what tools were already available rather than diving in to "reinvent the wheel" by writing scripts.

Considering how many available assignments I had to draw upon I hoped to combine a variety of methods to the data.

My analysis system consisted of a Win32 box running CYGWIN and ActiveState Perl. Such a system was chosen as it allowed the best of both worlds: i.e. access to a good

command line shell and the useful gnu command line tools whilst still providing access to Word and Excel for producing the report.

Initially the alert files were concatenated and the file description header removed so the data from the entire 5 day period could be analysed at once.

The primary analysis tools used were:

- Chris Kueth's Perl Scripts
- Sed
- My custom perl script
- Snortsnarf
- Grep

The scripts written by Chris Kueth allowed the files to be parsed and for lists of alerts and hosts with counts to be produced. This was used as the starting point.

SnortSnarf was examined. Initial attempts to use on the entire dataset proved futile given the memory and processing power available to me. I considered using a database for queries as some had done previously but I rapidly discovered grep was very capable of querying data sets.

For instance to get all alerts mentioning NIMDA

```
grep 'NIMDA' alerts
```

or to get all alerts for host 12.34.56.78

```
grep '12.34.56.78' alerts
```

The in depth analysis was done through combinations of greps to weed out alerts then parsing the resultant output through Perl scripts or through Snortsnarf. Snortsnarf was easily able to handle portions of the data containing selected alerts or selected hosts or subnets to allow analysis. This allowed correlations within the data to be made more apparent.

Snortsnarf did not however like the substitution of MY.NET for the first two octets of the IP addresses. Alias commands to convert MY.NET to 256.256 and back were created. Snortsnarf has no problems with illegal IP addresses such as 256.256.3.4 and by using these illegal values there was no chance of confusion with external addresses.

A custom script used to produce a table of top 10 sources and destinations was written in Perl.

The steps used in the analysis were as follows:

1. Separate port scans from alerts.
2. List alert types.
3. Analyse top 10 occurring alerts.
4. Analyse other possibly significant alerts.
5. Produce top talker source and destinations.
6. Filter out high false positive alerts identified in step 2.
7. Produce new top talker lists.
8. Analyse top 10 source and destinations.
9. Analyse port scan information and correlate with alerts
10. Analyse Out of Spec files (OOS) and correlate with alerts and port scans

List of References

Note: All hyperlinks checked 25 Mar 02

1. "SANS Intrusion Detection FAQ Port 137 Scan" Bryce Alexander
URL http://www.sans.org/newlook/resources/IDFAQ/port_137.htm

2. "Exploitation of Unprotected Windows Networking Shares" CERT/CC
URL http://www.cert.org/incident_notes/IN-2000-02.html

3. "Incident Mailing List Archives"
URL http://archives.neohapsis.com/archives/incidents/2000-04/0042.html

4. "GCIA Practical Assignment" David Leach
URL http://www.giac.org/practical/David_Leach_GCIA.doc Mar 25 2002

5. CERT® Advisory CA-1996-01 UDP Port Denial-of-Service Attack
URL http://www.cert.org/advisories/CA-1996-01.html

6. "GCIA Practical Assignment" Shelby Gray
URL http://www.giac.org/practical/Shelby_Gray_GCIA.zip

7. "Snort Mailing list archives"
http://archives.neohapsis.com/archives/snort/

8, "CERT® Advisory CA-2002-03 Multiple Vulnerabilities in SNMP"
URL http://www.cert.org/advisories/CA-2002-03.html

9. "CVE Vulnerability Database"
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012

10. "Snort Frequently Asked Questions (FAQ)"
URL http://www.snort.org/docs/faq.html

11. "GCIA Practical Assignment David Oborn"
URL http://www.giac.org/practical/David_Oborn_GCIA.html#watchlist

12. "Symantec Security Response w32.myparty@mm"
URL http://securityresponse.symantec.com/avcenter/venc/data/w32.myparty@mm.html

13. "What port numbers do well-known trojan horses use?" Joakim von Braun
URL http://www.sans.org/newlook/resources/IDFAQ/oddports.htm

14. " Translate:f vulnerability exposes IIS files source" Securiteam
URLhttp://www.securiteam.com/windowsntfocus/Translate_f_vulnerability_exposes_IIS_files_source.html

15. "wu-ftpd File Globbing Vulnerability" eEye Digital Security
URL http://www.eeye.com/html/Support/Retina/RTHs/FTP_Servers/815.html

16. "CERT Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD" CERT/CC
URL http://www.cert.org/advisories/CA-2001-33.html

17. "Snort Signatures Database"
URL http://www.snort.org/snort-db/sid.html?id=159

18. "NIMDA worm" GIAC
URL http://www.incidents.org/react/nimda.pdf

19. "Adore Worm" GIAC
URL http://www.sans.org/y2k/adore.htm

20. "Routing Sequences for ICMP" Laura Chappell
URL http://www.nwconnection.com/2001_03/ICMP/

21. "Snort-users Mailing list Archives:
URL http://www.ultraviolet.org/mail-archives/snort-users.2001/1687.html

22. "Unicode Vulnerability – How & Why?" Andrew Brannan
URL http://rr.sans.org/threats/unicode.php

23. "GCIA Practical Assignment Chris Kueth"
URL http://www.giac.org/practical/chris_kuethe_gcia.html

24. "Snortsnarf" Silicon Defense
URL http://www.silicondefense.com/software/snortsnarf/

Appendix A – Scripts

This is a script to produce table of top 10 source and destinations IPs. (Calls alertcount.pl written by Chris Kueth http://www.giac.org/practical/chris_kuethe_gcia.html)

```
#!/usr/bin/perl
#Note: very quick and dirty script.  (I do code better than this normally…honest)
print"Top 10 Sources\tCount\tTop 10 Dests\tCount\n";
$fname=shift;
system("perl -s alertcount.pl -s -q $fname |sort -r -n |head >src");
system("perl -s alertcount.pl -d -q $fname |sort -r -n |head >dst");
open (SRC,"src");
open (DST,"dst");
while($srcline=<SRC>) {
chomp($srcline);
$dstline=<DST>;
chomp($dstline);
($srccount,$srchost) = split("\t",$srcline);
($dstcount,$dsthost) = split("\t",$dstline);
print "$srchost\t$srccount\t$dsthost\t$dstcount\n";
}
```

Alias commands to convert MY.NET to 256.256 and back:

```
alias ssconv='sed "s/MY.NET/256.256/g"'
alias ssunconv='sed "s/256.256/MY.NET/g"'
```