Mark Wilson
SANS GIAC Level 2
Intrusion Detection In Depth
SANS GCIA Practical Assignment
Version 3.1
Atlanta, January 2002

Table of Contents

Assignment 1 – Describe the State of Intrusion Detection

Intrusion Detection Tools for the Budget Conscience

Being a Network Security Analyst at a public university, I get jealous of my counterparts in corporate America. These guys actually have a security budget and are able to purchase neat stuff like firewalls, Intrusion Detection Systems, AV software, etc. Most important, they get to develop a security policy with some teeth in it.

For the poor souls on the public dole, we must search the Internet for "free" tools and have very limited resources to purchase needed hardware. It gets to be quite challenging using these means to perform your duties as a security specialist over a large network.

This paper will discuss tools readily found and the methods used to set up an IDS for a large university.

The Hardware:

In my experience I have found not to skimp on the hardware. Because of the massive amount of traffic, it is important to separate the sensor and the analysis station on to separate hosts. For the sensor, CPU speed cannot be overemphasized. In fact, dual CPUs are recommended, though not required. Also needed are fast drives and at least 128 Mb of memory. Two network interface cards are also required and should be of good quality.

The analysis station, because it will be the dumping ground for the IDS logs, needs plenty of disk space and memory. As a rule of thumb, expect on the order of 1 to 1.5 Gbytes of data per day. If you wish to keep a months worth of logs at least 40 Gbytes of disk space is needed. Since the analysis software is a memory hog, the more the better. This is probably the where you don't want to take shortcuts. I would say at least 512 Mbytes, but would recommend 1 Gbyte.

The Setup:

Because of the prevalence of switched networks, setting up the switch with port spanning is required. For the sensor, set up one interface in promiscuous mode (and no IP address) and the other will be used for communication (ref. Northcutt/Novak). The non-IP interface will be directly connected to the spanning port on the switch. If your network runs a border firewall, placement of the sensor outside the firewall will allow you see all hostile traffic entering the network.

It is recommended not to set up the sensor as a server and run multiple applications and services. In fact the ONLY open port on the sensor should be port 22 to run secure shell (SSH). It is important to harden the host and run tcpwrappers . Its job is to simply sniff traffic and send the logs to the analysis station.

The analysis station will run the analysis software and possibly a database and web server. Perl and a C compiler will also be needed. I also find security tools such as port scanners and the expect scripting language useful. Many times when analyzing IDS logs, I find it useful to perform portscans on systems that show up in the logs. As a rule, the analysis station is the first thing I look at in the morning and having tools available on the this host (such as Nmap and Ethereal) is convenient.

Snort:
Snort (http://www.snort.org/) is fast becoming, if not already, the IDS of choice for many security professionals. As of this writing, the current version is 1.8.6. Snort bills itself as a lightweight IDS and can be installed on various flavors of Linux, Unix and Windows. The thing I like about Snort is its vast user community, the wealth of information found, and the large rule base.

Since my experience and expertise is Unix/Linux, I have only installed Snort on Linux. In order to configure and run Snort you must have libpcap and tcpdump. Although most linux distributions come with these packages, there are known problems with RedHat's libpcap. Both can be found www.tcpdump.org .

Snort comes with it's own rule set containing over 1400 rules! Daily updates are available to keep the security community current on signatures of the latest threats.

Plenty of documentation comes with the distribution along with forums to help the beginner. If you want to try writing a few rules, there are tutorials available.

Once you have the source compiled and your snort.conf file configured, you are ready to go. Beware, you may be overwhelmed at the amount of data you capture. Be prepared to tweak your snort.conf file to ignore dns servers and "chatty" devices. Also, it is recommended to run snort from a cron file. I restart Snort every 2 hours. This gets the alert, portscan , and tcpdump logs to a manageable level.

SnortSnarf:
SnortSnarf (available at www.silicondefense.com) is a Perl program designed to produce html pages from Snort alert and portscan files. What is cool is the html pages let you "drill down" and sort by signature or IP. It also displays the Top 20 source and destination IPs, according to number of alerts.

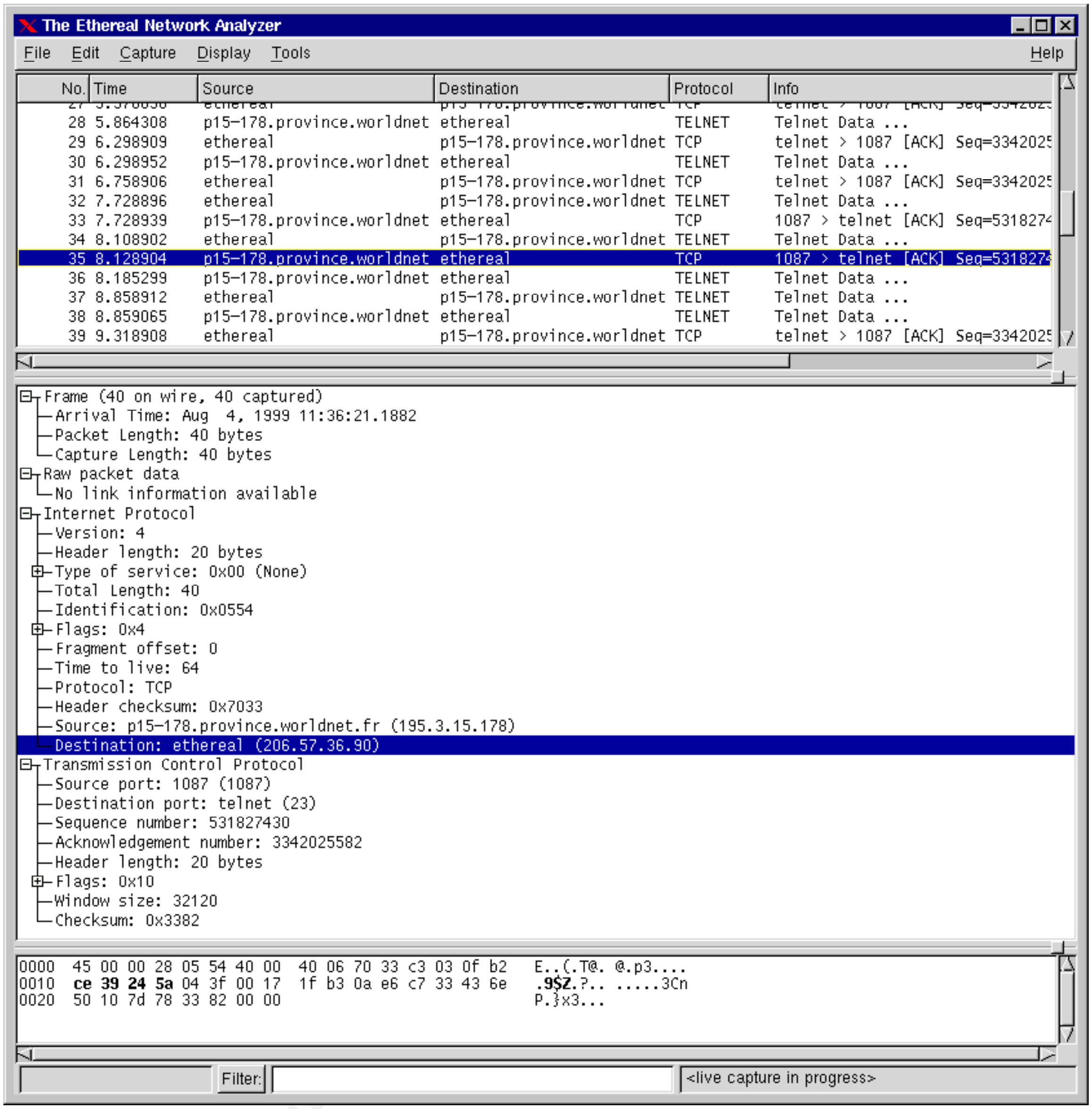
If you need more information on the signature, just click on hyperlink and you are led to Snort's site for further explanation and recommended actions. There are also hyperlinks to geektools.com and amenesi.com for whois and dns queries. This becomes especially useful to find contact information for abuse complaints. As mentioned, SnortSnarf is a memory hog and takes time to analyze the logs. Limiting the size of the alert files from

Snort will greatly enhance Snortsnarf's ability to timely analyze the data.

Ethereal:
Ethereal is a tool I use to analyze Snort's tcpdump logs. According to www.ethereal.com: "Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session."

Of course Ethereal not only interprets libpcap files, but also Sun's snoop and atmsnoop, NIA's sniffer and a host of others (http://www.ethereal.com/introduction.html). These files maybe introduced in gzip format, as Ethereal will compress on the fly.

The GUI interface allows the security analyst to view packet headers and payload.



```
No. Time     Source                    Destination               Protocol Info
 28 5.864308 p15-178.province.worldnet ethereal                  TELNET   Telnet Data ...
 29 6.298909 ethereal                  p15-178.province.worldnet TCP      telnet > 1087 [ACK] Seq=3342025
 30 6.298952 p15-178.province.worldnet ethereal                  TELNET   Telnet Data ...
 31 6.758906 ethereal                  p15-178.province.worldnet TCP      telnet > 1087 [ACK] Seq=3342025
 32 7.728896 ethereal                  p15-178.province.worldnet TELNET   Telnet Data ...
 33 7.728939 p15-178.province.worldnet ethereal                  TCP      1087 > telnet [ACK] Seq=531827
 34 8.108902 ethereal                  p15-178.province.worldnet TELNET   Telnet Data ...
 35 8.128904 p15-178.province.worldnet ethereal                  TCP      1087 > telnet [ACK] Seq=531827
 36 8.185299 p15-178.province.worldnet ethereal                  TELNET   Telnet Data ...
 37 8.858912 ethereal                  p15-178.province.worldnet TELNET   Telnet Data ...
 38 8.859065 p15-178.province.worldnet ethereal                  TELNET   Telnet Data ...
 39 9.318908 ethereal                  p15-178.province.worldnet TCP      telnet > 1087 [ACK] Seq=3342025
```

```
⊟ Frame (40 on wire, 40 captured)
  ├ Arrival Time: Aug  4, 1999 11:36:21.1882
  ├ Packet Length: 40 bytes
  └ Capture Length: 40 bytes
⊟ Raw packet data
  └ No link information available
⊟ Internet Protocol
  ├ Version: 4
  ├ Header length: 20 bytes
 ⊞├ Type of service: 0x00 (None)
  ├ Total Length: 40
  ├ Identification: 0x0554
 ⊞├ Flags: 0x4
  ├ Fragment offset: 0
  ├ Time to live: 64
  ├ Protocol: TCP
  ├ Header checksum: 0x7033
  ├ Source: p15-178.province.worldnet.fr (195.3.15.178)
  └ Destination: ethereal (206.57.36.90)
⊟ Transmission Control Protocol
  ├ Source port: 1087 (1087)
  ├ Destination port: telnet (23)
  ├ Sequence number: 531827430
  ├ Acknowledgement number: 3342025582
  ├ Header length: 20 bytes
 ⊞├ Flags: 0x10
  ├ Window size: 32120
  └ Checksum: 0x3382
```

```
0000  45 00 00 28 05 54 40 00  40 06 70 33 c3 03 0f b2   E..(.T@. @.p3....
0010  ce 39 24 5a 04 3f 00 17  1f b3 0a e6 c7 33 43 6e   .9$Z.?.. .....3Cn
0020  50 10 7d 78 33 82 00 00                            P.}x3...
```

The above screen shot from http://www.ethereal.com/image/mainwin-19990804.gif

As seen above, Ethereal has three distinct windows:

1. The top pane lists all the packets captured. When a packet is highlighted, the bottom 2 frames appear.
2. The center frame displays the details of the packet highlighted. It includes the frame, IP and TCP header information.
3. The bottom frame is where the data is viewed. This is beneficial for viewing the packet payload or the header fields.

In my opinion, the most powerful feature is the ability to write filters. This especially is useful when you wish to sort the data by source IP, destination IP, view only TCP packets, etc. There is also the feature to include logical operators (AND, OR, NOT, etc) in filter strings.

Nmap:

Although Nmap is not considered an IDS tool, it is vital to have at the security analyst's fingertips. Nmap is considered the scanner of choice for the security community and can be obtained from http://www.insecure.org/nmap/index.html. Nmap performs O/S fingerprinting and port scanning (TCP, UDP, ICMP).

For example, when I am reviewing Snort logs and notice an event of interest (for instance a possible compromise), I fire off off Nmap to perform a portscan on a particular host. I may also scan an address space for specific ports to determine if the problem (BOTs) is widespread.

Conclusion:

There are many high quality, freely available tools available to the security analyst who wishes to set up an Intrusion Detection System. All of the tools mentioned in this paper are compatible for both the Windows and Linux operating systems. Documentation is widely available for Snort, SnortSnarf, Ethereal and Nmap so no more excuses! Get with the program because the black hats out there are actively scanning and attacking your systems.

References:

Northcutt, Stephen /Novak, Judy, Network Intrusion Detection An Analyst's Handbook, Indianapolis: New Riders Publishing, 2001. 218.

Roesch, Marty/Caswell, Brian, "Snort", URL: http://www.snort.org (16 May 2002).

JWS, "Tcpdump", 13 May 2002, URL: http://www.tcpdump.org (16 May 2002).

Hoagland, James, "SnortSnarf", 020316.1, URL: http://www.silicondefense.com/software/snortsnarf/index.htm (16 May 2002).

Combs, Gerald, "Ethereal", 0.9.3, 15 May 2002, URL: http://www.ethereal.com/introduction.html (16 May 2002).

Fyodor, "Nmap", 2.54BETA21, 27 November 2001, URL: http://www.insecure.org/

(16 May 2002).

Assignment 2 – Network Detects

Detect #1: CRC Overflow attack on ssh

```
01/15-18:18:43.743732  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.747744  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.751360  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.753314  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.852615  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.854499  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.855199  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.856437  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.858499  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.859038  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.860589  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.863135  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.864156  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.875678  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.964599  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
01/15-18:18:43.967143  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3552 -> my.edu.53.72:22
.
.
.
01/15-18:18:59.460671  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:18:59.464117  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:18:59.475935  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
```

```
01/15-18:18:59.477170  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:18:59.489723  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:18:59.491078  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:18:59.491482  [**] IDS181/shellcode_shellcode-x86-nops
[**] 193.61.121.234:3561 -> my.edu.53.72:22
01/15-18:26:55.254147  [**] IDS181/shellcode_shellcode-x86-nops
[**] 193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.255068  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.256511  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.257953  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.259108  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.260278  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.261897  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.377239  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.378293  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
01/15-18:26:55.379289  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3623 -> my.edu.53.61:22
.
.
.
01/15-18:27:12.493506  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.507609  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.527231  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.529218  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.531266  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.610144  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.611406  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
```

```
01/15-18:27:12.613880  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.615141  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
01/15-18:27:12.627875  [**] IDS181/shellcode_shellcode-x86-nops [**]
193.61.121.234:3632 -> my.edu.53.61:22
```

Type of event generator: My network (.edu) using a Snort sensor. Log file is a snort alert file.

Detect was generated by: Snort IDS, version 1.7 on Redhat 7.0 O/S. Snort Rule obtained from whitehats.com.

```
alert TCP $EXTERNAL any -> $INTERNAL any (msg:
"IDS181/shellcode_shellcode-x86-nops"; flags: A+; content: "|90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|";)
```

Probably the source address was spoofed: Nil, this was a successful integer overflow attack to port 22.

Description of attack: Attack against TCP port 22/ssh, a remote integer overflow. In some versions of SSH1, a section of code protects against exploitation of CRC32 weaknesses. This is where the integer overflow vulnerability lies (ref: http://www.kb.cert.org/vuls/id/945216) .

Attack mechanism: This attack is directed against the routine detect_attack, defined as a 16-bit variable. Since this variable is used in combination with 32-bit local variables, an integer overflow condition exists. Hence, the attacker sends input packets that exceed 2^{16} and the side effect is the execution of arbitrary code with that of the ssh daemon, usually root.
(http://www.kb.cert.org/vuls/id/945216,
http://rr.sans.org/encryption/integer.php)

Correlations: Unfortunately the tcpdump log was deleted. However, this particular snort rule has alerted many past buffer overflow attacks via the infamous NOP (multiple 90s) signature. When this was noticed, a quick look at the tcpdump log confirmed it was an overflow attack to port 22.
Port 22 is one of the "top ten" probed ports on www.dshield.org/topports.html .
This type of attack is documented by Dave Dittrich on lists.jammed.com/incidents/2001/11/0039.html.

Also, after the compromise, my.edu.53.72 started attempting the same attack on another host:

```
01/16-10:40:21.947278  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:21.948511  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
```

```
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:21.955729  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.093184  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.095604  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.240718  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.247451  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.682352  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
01/16-10:40:22.976517  [**] EXPLOIT ssh CRC32 overflow NOOP [**]
my.edu.53.72:1464 -> 164.8.16.34:22
```

It was during this time I was working on the hacked system and found entries in the messages file and found malware in the /dev directory.

Below are excerpts from the messages File of compromised host:
(Note: time of IDS and host not in sync)

```
Jan 15 19:21:06 palomino sshd[2814]: connect from
hacker.nmap.edu
Jan 15 19:21:06 palomino sshd[2814]: log: Connection from
193.61.121.234 port 3486
Jan 15 19:21:09 palomino sshd[2815]: connect from
hacker.nmap.edu
Jan 15 19:21:09 palomino sshd[2815]: log: Connection from
193.61.121.234 port 3487
Jan 15 19:21:10 palomino sshd[2816]: connect from
hacker.nmap.edu
Jan 15 19:21:10 palomino sshd[2816]: log: Connection from
193.61.121.234 port 3488
Jan 15 19:21:12 palomino sshd[2817]: connect from
hacker.nmap.edu
Jan 15 19:21:12 palomino sshd[2817]: log: Connection from
193.61.121.234 port 3489
Jan 15 19:21:14 palomino sshd[2818]: connect from
hacker.nmap.edu
Jan 15 19:21:14 palomino sshd[2818]: log: Connection from
193.61.121.234 port 3490
Jan 15 19:21:16 palomino sshd[2819]: connect from
hacker.nmap.edu
Jan 15 19:21:16 palomino sshd[2819]: log: Connection from
```

```
193.61.121.234 port 3491
Jan 15 19:21:18 palomino sshd[2820]: connect from
hacker.nmap.edu
Jan 15 19:21:18 palomino sshd[2820]: log: Connection from
193.61.121.234 port 3492
Jan 15 19:21:20 palomino sshd[2821]: connect from
hacker.nmap.edu
Jan 15 19:21:20 palomino sshd[2821]: log: Connection from
193.61.121.234 port 3493
Jan 15 19:21:22 palomino sshd[2822]: connect from
hacker.nmap.edu
Jan 15 19:21:22 palomino sshd[2822]: log: Connection from
193.61.121.234 port 3494
Jan 15 19:21:24 palomino sshd[2823]: connect from
hacker.nmap.edu
Jan 15 19:21:24 palomino sshd[2823]: log: Connection from
193.61.121.234 port 3495
Jan 15 19:21:26 palomino sshd[2824]: connect from
hacker.nmap.edu
Jan 15 19:21:26 palomino sshd[2824]: log: Connection from
193.61.121.234 port 3496
Jan 15 19:21:28 palomino sshd[2825]: connect from
hacker.nmap.edu
Jan 15 19:21:28 palomino sshd[2825]: log: Connection from
193.61.121.234 port 3497
Jan 15 19:21:30 palomino sshd[2826]: connect from
hacker.nmap.edu
Jan 15 19:21:30 palomino sshd[2826]: log: Connection from
193.61.121.234 port 3498
Jan 15 19:21:32 palomino sshd[2827]: connect from
hacker.nmap.edu
Jan 15 19:21:32 palomino sshd[2827]: log: Connection from
193.61.121.234 port 3499
Jan 15 19:21:34 palomino sshd[2828]: connect from
hacker.nmap.edu
Jan 15 19:21:34 palomino sshd[2828]: log: Connection from
193.61.121.234 port 3500
Jan 15 19:21:35 palomino sshd[2829]: connect from
hacker.nmap.edu
Jan 15 19:21:35 palomino sshd[2829]: log: Connection from
193.61.121.234 port 3501
Jan 15 19:21:37 palomino sshd[2830]: connect from
hacker.nmap.edu
Jan 15 19:21:37 palomino sshd[2830]: log: Connection from
193.61.121.234 port 3502
Jan 15 19:21:40 palomino sshd[2831]: connect from
```

```
hacker.nmap.edu
Jan 15 19:21:40 palomino sshd[2831]: log: Connection from
193.61.121.234 port 3503
Jan 15 19:21:41 palomino sshd[2832]: connect from
hacker.nmap.edu
Jan 15 19:21:41 palomino sshd[2832]: log: Connection from
193.61.121.234 port 3504
Jan 15 19:21:43 palomino sshd[2833]: connect from
hacker.nmap.edu
Jan 15 19:21:43 palomino sshd[2833]: log: Connection from
193.61.121.234 port 3505
Jan 15 19:21:45 palomino sshd[2834]: connect from
hacker.nmap.edu
Jan 15 19:21:45 palomino sshd[2834]: log: Connection from
193.61.121.234 port 3506
Jan 15 19:21:46 palomino sshd[2835]: connect from
hacker.nmap.edu
Jan 15 19:21:46 palomino sshd[2835]: log: Connection from
193.61.121.234 port 3507
Jan 15 19:21:48 palomino sshd[2836]: connect from
hacker.nmap.edu
Jan 15 19:21:48 palomino sshd[2836]: log: Connection from
193.61.121.234 port 3508
Jan 15 19:21:50 palomino sshd[2837]: connect from
hacker.nmap.edu
Jan 15 19:21:50 palomino sshd[2837]: log: Connection from
193.61.121.234 port 3509
Jan 15 19:21:51 palomino sshd[2838]: connect from
hacker.nmap.edu
Jan 15 19:21:51 palomino sshd[2838]: log: Connection from
193.61.121.234 port 3510
Jan 15 19:21:53 palomino sshd[2839]: connect from
hacker.nmap.edu
Jan 15 19:21:53 palomino sshd[2839]: log: Connection from
193.61.121.234 port 3511
Jan 15 19:21:55 palomino sshd[2840]: connect from
hacker.nmap.edu
Jan 15 19:21:55 palomino sshd[2840]: log: Connection from
193.61.121.234 port 3512
Jan 15 19:21:56 palomino sshd[2841]: connect from
hacker.nmap.edu
Jan 15 19:21:56 palomino sshd[2841]: log: Connection from
193.61.121.234 port 3513
Jan 15 19:21:58 palomino sshd[2842]: connect from
hacker.nmap.edu
Jan 15 19:21:58 palomino sshd[2842]: log: Connection from
```

```
193.61.121.234 port 3514
Jan 15 19:22:00 palomino sshd[2843]: connect from
hacker.nmap.edu
Jan 15 19:22:00 palomino sshd[2843]: log: Connection from
193.61.121.234 port 3515
Jan 15 19:22:01 palomino sshd[2844]: connect from
hacker.nmap.edu
Jan 15 19:22:01 palomino sshd[2844]: log: Connection from
193.61.121.234 port 3516
Jan 15 19:22:03 palomino sshd[2845]: connect from
hacker.nmap.edu
Jan 15 19:22:03 palomino sshd[2845]: log: Connection from
193.61.121.234 port 3517
Jan 15 19:22:05 palomino sshd[2846]: connect from
hacker.nmap.edu
Jan 15 19:22:05 palomino sshd[2846]: log: Connection from
193.61.121.234 port 3518
Jan 15 19:22:07 palomino sshd[2847]: connect from
hacker.nmap.edu
Jan 15 19:22:07 palomino sshd[2847]: log: Connection from
193.61.121.234 port 3519
Jan 15 19:22:08 palomino sshd[2848]: connect from
hacker.nmap.edu
Jan 15 19:22:08 palomino sshd[2848]: log: Connection from
193.61.121.234 port 3520
Jan 15 19:22:10 palomino sshd[2849]: connect from
hacker.nmap.edu
Jan 15 19:22:10 palomino sshd[2849]: log: Connection from
193.61.121.234 port 3521
Jan 15 19:22:12 palomino sshd[2850]: connect from
hacker.nmap.edu
Jan 15 19:22:12 palomino sshd[2850]: log: Connection from
193.61.121.234 port 3522
Jan 15 19:22:14 palomino sshd[2851]: connect from
hacker.nmap.edu
Jan 15 19:22:14 palomino sshd[2851]: log: Connection from
193.61.121.234 port 3523
Jan 15 19:22:16 palomino sshd[2852]: connect from
hacker.nmap.edu
Jan 15 19:22:16 palomino sshd[2852]: log: Connection from
193.61.121.234 port 3524
Jan 15 19:22:17 palomino sshd[2853]: connect from
hacker.nmap.edu
Jan 15 19:22:17 palomino sshd[2853]: log: Connection from
193.61.121.234 port 3525
Jan 15 19:22:19 palomino sshd[2854]: connect from
```

```
hacker.nmap.edu
Jan 15 19:22:19 palomino sshd[2854]: log: Connection from
193.61.121.234 port 3526
Jan 15 19:22:22 palomino sshd[2855]: connect from
hacker.nmap.edu
Jan 15 19:22:22 palomino sshd[2855]: log: Connection from
193.61.121.234 port 3527
Jan 15 19:22:26 palomino sshd[2856]: connect from
hacker.nmap.edu
Jan 15 19:22:26 palomino sshd[2856]: log: Connection from
193.61.121.234 port 3528
Jan 15 19:22:29 palomino sshd[2857]: connect from
hacker.nmap.edu
Jan 15 19:22:29 palomino sshd[2857]: log: Connection from
193.61.121.234 port 3529
Jan 15 19:22:32 palomino sshd[2858]: connect from
hacker.nmap.edu
Jan 15 19:22:32 palomino sshd[2858]: log: Connection from
193.61.121.234 port 3530
Jan 15 19:22:36 palomino sshd[2859]: connect from
hacker.nmap.edu
Jan 15 19:22:36 palomino sshd[2859]: log: Connection from
193.61.121.234 port 3531
Jan 15 19:22:39 palomino sshd[2860]: connect from
hacker.nmap.edu
Jan 15 19:22:39 palomino sshd[2860]: log: Connection from
193.61.121.234 port 3532
Jan 15 19:22:42 palomino sshd[2861]: connect from
hacker.nmap.edu
Jan 15 19:22:42 palomino sshd[2861]: log: Connection from
193.61.121.234 port 3533
Jan 15 19:22:46 palomino sshd[2862]: connect from
hacker.nmap.edu
Jan 15 19:22:46 palomino sshd[2862]: log: Connection from
193.61.121.234 port 3534
Jan 15 19:22:49 palomino sshd[2863]: connect from
hacker.nmap.edu
Jan 15 19:22:49 palomino sshd[2863]: log: Connection from
193.61.121.234 port 3535
Jan 15 19:22:52 palomino sshd[2864]: connect from
hacker.nmap.edu
Jan 15 19:22:52 palomino sshd[2864]: log: Connection from
193.61.121.234 port 3536
Jan 15 19:22:56 palomino sshd[2865]: connect from
hacker.nmap.edu
Jan 15 19:22:56 palomino sshd[2865]: log: Connection from
```

```
193.61.121.234 port 3537
Jan 15 19:22:59 palomino sshd[2866]: connect from
hacker.nmap.edu
Jan 15 19:22:59 palomino sshd[2866]: log: Connection from
193.61.121.234 port 3538
Jan 15 19:23:02 palomino sshd[2867]: connect from
hacker.nmap.edu
Jan 15 19:23:02 palomino sshd[2867]: log: Connection from
193.61.121.234 port 3539
Jan 15 19:23:06 palomino sshd[2868]: connect from
hacker.nmap.edu
Jan 15 19:23:06 palomino sshd[2868]: log: Connection from
193.61.121.234 port 3540
Jan 15 19:23:09 palomino sshd[2869]: connect from
hacker.nmap.edu
Jan 15 19:23:09 palomino sshd[2869]: log: Connection from
193.61.121.234 port 3541
Jan 15 19:23:09 palomino sshd[73]: log: Generating new 768
bit RSA key.
Jan 15 19:23:11 palomino sshd[73]: log: RSA key generation
complete.
Jan 15 19:23:13 palomino sshd[2871]: connect from
hacker.nmap.edu
Jan 15 19:23:13 palomino sshd[2871]: log: Connection from
193.61.121.234 port 3542
Jan 15 19:23:16 palomino sshd[2872]: connect from
hacker.nmap.edu
Jan 15 19:23:16 palomino sshd[2872]: log: Connection from
193.61.121.234 port 3543
Jan 15 19:23:19 palomino sshd[2873]: connect from
hacker.nmap.edu
Jan 15 19:23:19 palomino sshd[2873]: log: Connection from
193.61.121.234 port 3544
Jan 15 19:23:23 palomino sshd[2874]: connect from
hacker.nmap.edu
Jan 15 19:23:23 palomino sshd[2874]: log: Connection from
193.61.121.234 port 3545
Jan 15 19:23:26 palomino sshd[2875]: connect from
hacker.nmap.edu
Jan 15 19:23:26 palomino sshd[2875]: log: Connection from
193.61.121.234 port 3546
Jan 15 19:23:29 palomino sshd[2876]: connect from
hacker.nmap.edu
Jan 15 19:23:29 palomino sshd[2876]: log: Connection from
193.61.121.234 port 3547
Jan 15 19:23:33 palomino sshd[2877]: connect from
```

```
hacker.nmap.edu
Jan 15 19:23:33 palomino sshd[2877]: log: Connection from
193.61.121.234 port 3548
Jan 15 19:23:36 palomino sshd[2878]: connect from
hacker.nmap.edu
Jan 15 19:23:36 palomino sshd[2878]: log: Connection from
193.61.121.234 port 3549
Jan 15 19:23:39 palomino sshd[2879]: connect from
hacker.nmap.edu
Jan 15 19:23:39 palomino sshd[2879]: log: Connection from
193.61.121.234 port 3550
Jan 15 19:23:43 palomino sshd[2880]: connect from
hacker.nmap.edu
Jan 15 19:23:43 palomino sshd[2880]: log: Connection from
193.61.121.234 port 3552
Jan 15 19:23:44 palomino sshd[2881]: connect from
hacker.nmap.edu
Jan 15 19:23:44 palomino sshd[2881]: log: Connection from
193.61.121.234 port 3553
Jan 15 19:23:46 palomino sshd[2882]: connect from
hacker.nmap.edu
Jan 15 19:23:46 palomino sshd[2882]: log: Connection from
193.61.121.234 port 3554
Jan 15 19:23:48 palomino sshd[2883]: connect from
hacker.nmap.edu
Jan 15 19:23:48 palomino sshd[2883]: log: Connection from
193.61.121.234 port 3555
Jan 15 19:23:50 palomino sshd[2884]: connect from
hacker.nmap.edu
Jan 15 19:23:50 palomino sshd[2884]: log: Connection from
193.61.121.234 port 3556
Jan 15 19:23:51 palomino sshd[2885]: connect from
hacker.nmap.edu
Jan 15 19:23:51 palomino sshd[2885]: log: Connection from
193.61.121.234 port 3557
Jan 15 19:23:53 palomino sshd[2886]: connect from
hacker.nmap.edu
Jan 15 19:23:53 palomino sshd[2886]: log: Connection from
193.61.121.234 port 3558
Jan 15 19:23:55 palomino sshd[2887]: connect from
hacker.nmap.edu
Jan 15 19:23:55 palomino sshd[2887]: log: Connection from
193.61.121.234 port 3559
Jan 15 19:23:56 palomino sshd[2888]: connect from
hacker.nmap.edu
Jan 15 19:23:56 palomino sshd[2888]: log: Connection from
```

```
193.61.121.234 port 3560
Jan 15 19:23:58 palomino sshd[2889]: connect from
hacker.nmap.edu
Jan 15 19:23:58 palomino sshd[2889]: log: Connection from
193.61.121.234 port 3561
Jan 15 19:25:41 palomino syslogd 1.3-3: restart.
Jan 15 19:28:15 palomino sshd[3048]: log: Server listening
on port 22.
Jan 15 19:28:15 palomino sshd[3048]: log: Generating 768 bit
RSA key.
Jan 15 19:28:17 palomino sshd[3048]: log: RSA key generation
complete.
```

Evidence of active targeting: Since the 2 hosts were compromised this is active targeting. Both systems were running vulnerable versions of ssh, both were compromised by the same source IP, and the second host was attacked within a few minutes of the first. My guess is prior recon was performed on our network via ssh scans.

Severity: Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)
(2+5) – (2+1) = 4
Host is a Linux desktop(2); attack rooted the system(5); Novice user, vulnerable version of ssh, limited services running(2), No firewall (1).

Defensive recommendation: Unfortunately, these systems were rooted. Recommend re-install of O/S, secure system by running limited services (inetd.conf and system daemons), install/config tcpwrappers, and install current version of ssh compiled with support for tcpwrappers.
As a follow-up, perform system wide scan of ssh versions and inform university community, and specific users with vulnerable versions, of recent hacks and recommend they upgrade their systems.

Multiple Choice Question:

The NOOP sled (multiple 90s in payload) is an indicator of
a) Denial of Service attack
b) Buffer overflow
c) Teardrop attack
d) Fragmented packet
Answer: c

Detect #2 BIND version query
02/25-01:32:26.227436 [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4533 -> my.edu.79.139:53

```
02/25-02:38:07.569808  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4733 -> my.edu.199.114:53
02/25-03:21:49.655059  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:2154 -> my.edu.207.122:53
02/25-03:59:26.707445  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1211 -> my.edu.56.84:53
02/25-05:04:19.330702  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4574 -> my.edu.98.182:53
[...]
02/25-22:43:59.045197  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1444 -> my.edu.32.7:53
02/25-23:47:41.237835  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3302 -> my.edu.14.136:53
02/26-00:30:23.193086  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3582 -> my.edu.155.68:53
02/26-00:31:48.297838  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1083 -> my.edu.16.152:53
02/26-02:46:49.277235  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1122 -> my.edu.45.125:53
02/26-08:28:25.642965  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4691 -> my.edu.109.104:53
02/26-11:52:15.860816  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4206 -> my.edu.212.191:53
02/26-13:20:55.618348  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4255 -> my.edu.110.40:53
02/27-01:50:43.805226  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:2881 -> my.edu.165.18:53
02/27-03:28:55.088826  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4759 -> my.edu.54.168:53
02/27-03:59:13.353139  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4234 -> my.edu.141.221:53
02/27-04:49:26.270907  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4333 -> my.edu.201.100:53
[...]
02/27-15:18:33.674177  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4804 -> my.edu.92.177:53
02/27-17:44:34.310298  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4296 -> my.edu.205.94:53
02/27-19:32:06.585539  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3929 -> my.edu.134.190:53
02/27-20:08:17.204746  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1527 -> my.edu.25.70:53
02/27-20:25:23.691780  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3243 -> my.edu.43.207:53
[...]
```

```
02/28-09:40:10.298662  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3962 -> my.edu.65.172:53
02/28-12:25:45.377612  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3740 -> my.edu.213.210:53
02/28-16:20:17.367770  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1650 -> my.edu.129.208:53
03/01-17:57:43.872583  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1279 -> my.edu.16.55:53
03/01-18:07:51.780758  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3757 -> my.edu.60.184:53
03/01-18:25:14.176560  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1778 -> my.edu.118.190:53
03/01-21:12:36.395928  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3437 -> my.edu.123.17:53
03/01-22:29:59.328078  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:3659 -> my.edu.94.4:53
03/02-00:11:23.159980  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4941 -> my.edu.36.190:53
03/02-01:02:21.490039  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1810 -> my.edu.121.113:53
03/02-02:57:13.225347  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4943 -> my.edu.114.71:53
[...]
03/02-18:21:42.417405  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:4166 -> my.edu.120.212:53
03/02-19:25:24.071070  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:2263 -> my.edu.24.184:53
03/02-20:57:10.719947  [**] IDS278/dns_named-probe-version [**]
202.98.196.66:1450 -> my.edu.30.161:53
```

Type of event generator: My network (.edu) using a Snort sensor. Log file is a snort alert file.

Detect was generated by: Snort IDS, version 1.7 on Redhat 7.0 O/S. Rule obtained from whitehat.com rulebase.

Probability the source address was spoofed: Very unlikely as this appears to be information gathering and source needs the info.

Description of Attack: Source IP is checking for BIND version. There are numerous vulnerabilities with various versions of BIND (ref: CVE-1999-0009 - 0011, CVE-1999-0024, CVE-1999-0184, CVE-1999-0833, 0835, 0837, 0848, 0849, 0851, CVE-2000-0887, 0888, CVE-2001-0010 – 0013, CAN-1999-1499, CAN-1001-0497).

Attack Mechanism: This activity is both reconnaissance and a slow, stealthy, network scan (of sorts). Notice how the packets arrive at random times all during the day, for several days, and all directed at port 53 (DNS). It appears the attacker is directing this nefarious activity toward the entire network, perhaps to get around any IDS sensors. In this he is able to accomplish scanning the entire network for open port 53 and, if open, obtain the BIND version. This was done all in one sweep and stealthy at that.

Correlations: Below is Snort's tcpdump log showing BIND version query.

```
00:11:23.159980 P 202.98.196.66.4941 > my.edu.36.190.domain: 4660
[b2&3=0x80] TXT CHAOS)? version.bind. (30)

                          E^@ ^@ : .. x ^@^@  6^Q  u^K .. b .. B
                         ....  $.. ^S M ^@ 5 ^@ & .... ^R 4 ^@..
                         ^@^A ^@^@ ^@^@ ^@^@ ^G v  e r  s i  o n
                         ^D b  i n  d^@ ^@^P ^@^C
01:02:21.490039 P 202.98.196.66.1810 > my.edu.121.113.domain: 4660
[b2&3=0x80] TXT CHAOS)? version.bind. (30)

                          E^@ ^@ : .. 4 ^@^@  6^Q  T.. .. b .. B
                         ....  y q ^G^R ^@ 5 ^@ &  8^_ ^R 4 ^@..
                         ^@^A ^@^@ ^@^@ ^@^@ ^G v  e r  s i  o n
                         ^D b  i n  d^@ ^@^P ^@^C
```

According to incidents.org, domain consistently shows up on "Top 10 ten ports probed" list (http://www.dshield.org/topports.html).

Evidence of active targeting: The evidence does not suggest active targeting. This guy is basically looking for DNS servers on our network and isn't concerned if it takes several days. He probably knows the poor reputation university networks have for security and he is basically looking for low hanging fruit.

Severity:
Severity = (Criticality +Lethality) – (System Counters + Network Counters)
DNS servers are critical targets (5), reconnaissance and network scanning (2),
All DNS servers are patched and running BIND versions 8.2.3-REL or later. However there may be hosts on network (linux) running vulnerable BIND versions (3), No firewall, unrestricted traffic (2)
(5+2) – (3+2) = 2

Defensive Recommendation:
Scan Network for open port 53 and do a little "friendly" recon to determine what is vulnerable. For those "unapproved" DNS hosts, seek to educate owners and

have named service discontinued. Inform sys admins who support official campus domain servers to check and secure their systems and suggest they configure named to not give BIND version when queried.

Multiple Choice Question:
In current BIND distributions, hiding the version of BIND from reconnaissance probes can be accomplished by:

a) Configuring the options statement "version" as you require
b) Edit the /etc/named.version file
c) Compile BIND will compile directive –version-query-disable
d) It is not possible

Answer: a

Detect # 3 WU-FTPD Heap Corruption Exploit:
I wish to add a personal thanks to Mark Cooper (SANS Incidents Handler) for providing information and technical assistance for help in identifying this exploit.

```
03/09-23:10:26.624088  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2043 -> my.edu.100.9:21
03/09-23:10:28.079632  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2044 -> my.edu.100.9:21
03/09-23:10:29.488025  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2045 -> my.edu.100.9:21
03/09-23:10:30.974451  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2046 -> my.edu.100.9:21
03/09-23:10:32.489625  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2047 -> my.edu.100.9:21
03/09-23:10:33.951182  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2048 -> my.edu.100.9:21
03/09-23:10:35.333018  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2049 -> my.edu.100.9:21
03/09-23:10:38.416736  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2050 -> my.edu.100.9:21
03/09-23:10:39.847531  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2051 -> my.edu.100.9:21
03/09-23:10:41.323316  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2052 -> my.edu.100.9:21
[…]
03/09-23:25:48.878925  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2581 -> my.edu.100.9:21
03/09-23:25:50.167247  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2582 -> my.edu.100.9:21
03/09-23:25:51.511888  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2583 -> my.edu.100.9:21
03/09-23:25:52.946778  [**] IDS181/shellcode_shellcode-x86-nops [**]
```

```
203.253.206.116:2584 -> my.edu.100.9:21
03/09-23:25:54.479363  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2585 -> my.edu.100.9:21
03/09-23:25:55.996089  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2586 -> my.edu.100.9:21
03/09-23:25:57.359074  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2587 -> my.edu.100.9:21
03/09-23:26:00.367430  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2588 -> my.edu.100.9:21
03/09-23:26:21.216437  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2589 -> my.edu.100.9:21
03/09-23:26:59.099291  [**] IDS487/ftp_dos-ftpd-globbing [**]
203.253.206.116:2589 -> my.edu.100.9:21
03/09-23:34:14.247513  [**] IDS181/shellcode_shellcode-x86-nops [**]
203.253.206.116:2590 -> my.edu.100.9:21
03/09-23:34:14.828210  [**] IDS364/ftp_ftp-bad-login [**] my.edu.100.9:21 -
> 203.253.206.116:2590
```

Type of event generator: Detects from my network (.edu) via Snort IDS version 1.7, alert file. Snort rule obtained the defunct website, whitehats.com.

```
alert TCP $EXTERNAL any -> $INTERNAL any (msg:
"IDS181/shellcode_shellcode-x86-nops"; flags: A+; content: "|90 90 90 90 90
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|";)
```

Probably the source address was spoofed: Source not spoofed. This was a successful buffer overflow attack to the system and system was compromised.

Note: For "Description of attack" and "Attack mechanism" sections, Jennifer Allen's GCIH Practical "WU-FTPD Heap Corruption Vulnerability" was used as a reference (http://www.giac.org/practical/Jenn_Allen_GCIH.doc)

Description of attack: Remote exploits can be executed via specially crafted globbing commands to wu-ftpd 2.6.1 (CVE candidate CAN-2001-0550).   Since the ftp daemon normally runs via root user, the attacker is able to compromise the system and gain root privilege.

Attack mechanism: Previous scans of our network for ftp were logged in the snort portscan file. Notice, during the port scan, where the source port is 21, however, when my.edu.100.9 is probed, the source port is 1920:

```
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.100.1:21 SYN ******S*
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.100.10:21 SYN ******S*
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.100.13:21 SYN ******S*
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.100.14:21 SYN ******S*
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.99.252:21 SYN ******S*
Mar  9 23:01:45 203.253.206.116:1920 -> my.edu.100.9:21 SYN ******S*
Mar  9 23:01:42 203.253.206.116:21 -> my.edu.100.15:21 SYN ******S*
```

I believe the attacker was mapping our network for open ftp servers. Whenever an open port 21 is found, perhaps a telnet probe was made (coming from a higher source port) to determine FTP version. This may explain why these high non-privileged source ports pop up from time to time in the port scan. But why didn’t the attacker probe dst. port 21, from src. Port 21, before the src. 1920 -> dst 21, on my.edu.100.9? The reason is the same attack was executed some 9 hours earlier on my.edu.100.9. The only difference is the source IP was different and the box was not root’d. Either the attacker was the same, coming from a different IP, or a group of hackers knew this host was vulnerable and another hacker tried later in the day (and compromised the host).

Jennifer Allen explains, in her GCIH practical, remote exploits are made using malformed globbing commands because wu-ftpd 2.6.1 improperly handles globbing. The attacker only needs access via anonymous or a valid FTP account.
The exploit comes packaged in two C programs, forcer.c and woot-exploit.c, both working in tandem. Either a “test” run is performed using the /bin/route command to test if the command executed as expected or a “real” run is tried, using /bin/sh, to provide a shell.

Correlations: The following was logged in Snort’s tcpdump log:
Note: some packets modified to remove numerous NOOP characters.

```
23:26:00.367430 P leto.cheju.ac.kr.2588 > diglib.lib.my.edu.ftp: P
1967931374:1967932605(1231) ack 1973243876 win 32120
<nop,nop,timestamp 131038539 158764043> (DF)
```

```
 E^@ ^E^C  8..  @^@  1^F ..^M .... .. t
....  d^I ^J^\ ^@^U  u L  ?..  u..  O..
..^X  } x  w^M ^@^@ ^A^A ^H^J ^G..  } K
^I v ..^K  u s e r   f t p ^J p a s
 s   h t t p : /  / m  p 3  . c  o m
 / c  o s  v          .. y ^I^H ^J s
 i t  e   e x e c  .. .... .... ....
.... .... .... .... ^L^G ^H^T  F^H ^H..
.... .... .... .... .... .... .... ^L^G
^H^T  F^H ^H.. .... .... .... .... ....
.... .... ^L^G ^H^T  F^H ^H.. .... ....
.... .... .... .... .... ^L^G ^H^T  F^H
^H.. .... .... .... .... .... .... ....
^L^G ^H^T  F^H ^H.. .... .... .... ....
[…]
```

```
                    .... .. M ^D..  =.. .... ....  u^H .. M
                    ^L.. ^K..  M^H .. U ^L.. .. 1 .... ^A..
                    .... .... .... .... .. /  s b  i n  / r
                     o u  t e ^@^J  s t  a t    ~  {^J  q u
                     i t ^J
23:26:21.216437 P leto.cheju.ac.kr.2589 > diglib.lib.my.edu.ftp: P
1988729704:1988730935(1231) ack 1994972242 win 32120
<nop,nop,timestamp 131040625 158766124> (DF)

                     E^@  ^E^C  8..  @^@  0^F .... .... .. t
                    ....  d^I  ^J^] ^@^U  v.. .. h  v.. .. R
                    ..^X  } x ..^R  ^@^@  ^A^A  ^H^J  ^G.. .. q
                    ^I v .. ,  u s  e r    f  t p ^J p  a s
                     s    h t  t p  : /  / m  p 3  . c  o m
                     / c  o s  v          .. y  ^I^H  ^J s
                     i t  e    e x  e c   .. .... .... ....
                    .... .... .... ....  ^L^G  ^H^T  F^H  ^H..
                    […]
                    .... .... .... .... ....  U.. .. 1 .. 1
                    .. 1 .... ^W.. ....  ... ....  C ^  .. '
                    .. ^  ^I.. .... .. 1 .. 1 ....  =.. ....
                     . .  /.. ....  ]^D ..^P .. U ^D.. ..^C
                    .... .. M ^D..  =.. .... ....  u^H .. M
                    ^L.. ^K..  M^H .. U ^L.. .. 1 .... ^A..
                    .... .... .... .... .. /  b i  n /  / /
                     / /  s h ^@^J  s t  a t    ~  {^J  q u
                     i t ^J
23:26:59.099291 P leto.cheju.ac.kr.2589 > diglib.lib.my.edu.ftp: P
1233:1247(14) ack 2204 win 32120 <nop,nop,timestamp 131044414
158766524> (DF)

                     E^@  ^@ B  8..  @^@  0^F .... .... .. t
                    ....  d^I  ^J^] ^@^U  v.. .. 9  v.. ....
                    ..^X  } x  F^E  ^@^@  ^A^A  ^H^J  ^G.. .. >
                    ^I v ....  r m    /  v a  r /  l o  g /
                     *^J
23:34:14.247513 P leto.cheju.ac.kr.2590 > diglib.lib.my.edu.ftp: P
2472826660:2472827891(1231) ack 2485054510 win 32120
<nop,nop,timestamp 131087936 158813431> (DF)

                     E^@  ^E^C  9 V  @^@  1^F .. W .... .. t
                    ....  d^I  ^J^^  ^@^U .. d  W $ ..^^  .. .
                    ..^X  } x  R..  ^@^@  ^A^A  ^H^J  ^G..  > @
                    ^I w  L..  u s  e r    f  t p ^J p  a s
                     s    h t  t p  : /  / m  p 3  . c  o m
```

```
                         / c o s v          .. y ^I^H ^J s
                         i t e   e x e c  .. .... .... ....
                        .... .... .... .... ^L^G ^H^T  F^H ^H..
                        [...]
                        .... .. M ^D..  =.. .... ....  u^H .. M
                        ^L.. ^K..  M^H .. U ^L.. .. 1 .... ^A..
                        .... .... .... .... .. /  b i n /  / /
                         / /  s h ^@^J  s t a t   ~  {^J  q u
                         i t ^J
23:34:14.828210 P diglib.lib.my.edu.ftp > leto.cheju.ac.kr.2590: FP
96:314(218) ack 1231 win 31856 <nop,nop,timestamp 158813517
131087936> (DF) [tos 0x10]

                         E^P ^A^N ....  @^@  >^F .... ....  d^I
                        .... .. t ^@^U ^J^^ ..^^ .... .. d  [..
                        ..^Y  | p ..^N ^@^@ ^A^A ^H^J ^I w  M M
                        ^G..  > @  3 3  1   G u e s t   l o
                         g i n   o k ,   s e n d   y o u
                         r   c o m p l e t e   e - m a i
                         l   a d d r e s s   a s   p a s
                         s w  o r  d . ^M^J  5 3  0   L o g i
                         n   i n c o r r e c t . ^M^J  5 3
                         0   P l  e a s e   l o g i n   w
                         i t h   U S E R   a n d   P A S
                         S . ^M^J  5 3  0   P l  e a s e   l
                         o g  i n   w i t h   U S E R   a
                         n d   P A S S . ^M^J  5 3  0   P l
                         e a s e  l o g i n   w i t h
                         U S E R   a n d   P A S S . ^M^J
                         2 2  1   G o o d b y e . ^M^J
```

Notice the first packet contains the string "/bin/route". This was the last in a string of multiple similar packets. This is where the "test" runs are made. The next packet has the "/bin/sh" string and waa-laa, a shell is born! The next packet is where the attacker deletes /var/log/*. It looks like later an ftp connection is made back to the attacker's server. I guess he wanted to check out the functionality of the shell after he root'd the box.

Other correlations are that on the compromised host, all log files we deleted and the /etc/ftpusers file was modified on 3/9/2002 at 23:33. He added anonymous. I guess he didn't want anyone else to hack the box since he now owned it.

Evidence of active targeting: Definitely as previous port scans reveal and the fact this host was subjected to the same attack on the same day, from separate

IPs.

Severity:
Severity = (Criticality +Lethality) – (System Counters + Network Counters)
Linux FTP server (3), attacker can gain root access remotely (5), even though limited services were run on server and O/S was up to date, anonymous FTP was open and wu-ftpd was not patched (2), ftp allowed through firewall (1)
(3+5) – (2+1) = 5

Defensive recommendation: Alert university community of compromise and provide info on dangers of running pre-2.6.1 wu-ftpd and anonymous accounts. Provide additional info on patches available and links. Scan for ftp and get a handle on what is out there.

Multiple choice question:
The Wu-ftp globbing attack is

a) Crafted packets with the signature GLOB imbedded in the payload
b) Only successful when the user anonymous is disabled.
c) A buffer overflow attack via the ftp glob() function
d) Not an attack because it never worked.

Answer: c

Analyze This! – Assignment 3

Executive Summary:

We appreciate the opportunity to provide a security audit for State University. This analysis covers the following Snort IDS log files: alert.020320.tar.gz, alert.020321.tar.gz, alert.020322.tar.gz, alert.020323.tar.gz, alert.020324.tar.gz, scans.020320.tar.gz, scans.020321.tar.gz, scans.020322.tar.gz, scans.020323.tar.gz scans.020324.tar.gz, oos_Mar.20.2002.tar.gz, oos_Mar.21.2002.tar.gz, oos_Mar.22.2002.tar.gz, oos_Mar.23.2002.tar.gz, oos_Mar.24.2002.tar.gz

This analysis covered the Top 10 alerts as determined by number of alerts per Snort rule. It is obvious many false positives can be reduced as noted in this report. Streaming audio, chatty boxes, peer-to-peer traffic are producing most of these false alerts.

Being a university and largely open environment leaves the network open to many exploits and hackers ready to take advantage of this. Unpatched and poorly managed systems, on a fast network, are "low hanging fruit" to the black hat community.

It is important the University recognizes this and put in place the necessary resources to protect their assets.

Table of Alerts for alert files dated March 20, 2002 through March 24, 2002

	A. Signature	# alerts	# sources	# dest.
1	connect to 515 from inside	90687	148	4
2	SMB Name Wildcard	61366	185	193
3	spp_http_decode: IIS Unicode attack detected	53702	142	732
4	SNMP public access	36882	23	145
5	ICMP Echo Request L3retriever Ping	30443	120	14
6	MISC Large UDP Packet [arachNIDS]	16008	24	15
7	INFO MSN IM Chat data	12181	104	101
8	INFO Inbound GNUTella Connect request	7644	6003	12
9	spp_http_decode: CGI Null Byte attack detected	6516	13	16
10	ICMP Echo Request Nmap or HPING2	5162	63	421
11	High port 65535 udp - possible Red Worm - traffic	5016	137	142
12	WEB-MISC Attempt to execute cmd	3812	27	33
13	Watchlist 000220 IL-ISDNNET-990517	3483	18	10
14	FTP DoS ftpd globbing	2691	35	6
15	Possible trojan server activity	1966	17	16
16	SCAN Proxy attempt [help.undernet.org]	1589	24	409
17	ICMP Fragment Reassembly Time Exceeded	1246	35	76
18	INFO Outbound GNUTella Connect request	1182	12	783
19	ICMP Router Selection [arachNIDS]	1051	125	1
20	INFO - Possible Squid Scan	715	14	308
21	WEB-IIS view source via translate header [BUGTRAQ] [arachNIDS]	701	35	2

22	WEB-IIS _vti_inf access	363	116	2
23	WEB-FRONTPAGE _vti_rpc access [BUGTRAQ]	346	109	2
24	INFO napster login	328	1	35
25	SYN-FIN scan!	316	2	315
26	ICMP Echo Request Windows	312	25	17
27	INFO FTP anonymous FTP	208	5	25
28	Null scan!	179	18	9
29	WEB-MISC 403 Forbidden	129	11	14
30	WEB-IIS Unauthorized IP Access Attempt	119	6	9
31	NMAP TCP ping!	117	13	6
32	INFO Possible IRC Access	85	18	14
33	ICMP Destination Unreachable (Communication Administratively Prohibited)	73	1	1
34	EXPLOIT x86 NOOP	60	15	20
35	ICMP traceroute [arachNIDS]	57	21	6
36	SCAN Synscan Portscan ID 19104	43	41	7
37	WEB-CGI csh access [CVE]	30	1	1
38	WEB-MISC http directory traversal [arachNIDS]	30	5	2
39	Watchlist 000222 NET-NCFC	29	2	2
40	WEB-CGI scriptalias access [BUGTRAQ] [CVE] [arachNIDS]	24	3	1
41	Port 55850 tcp - Possible myserver activity - ref. 010313-1	24	7	7
42	Incomplete Packet Fragments Discarded	21	3	3
43	ICMP Destination Unreachable (Host Unreachable)	20	1	1
44	Attempted Sun RPC high port access	17	4	12
45	WEB-MISC compaq nsight directory traversal	15	3	3
46	INFO Napster Client Data	15	4	8
47	RFB - Possible WinVNC - 010708-1	15	7	7
48	Queso fingerprint	15	10	6
49	SUNRPC highport access!	13	1	1
50	INFO Inbound GNUTella Connect accept	12	4	8
51	FTP CWD / - possible warez site	11	1	11
52	TCP SRC and DST outside network	11	2	1
53	MYPARTY - Possible My Party infection	9	2	1
54	EXPLOIT x86 setgid 0	7	7	7
55	Port 55850 udp - Possible myserver activity - ref. 010313-1	6	4	5
56	ICMP Destination Unreachable (Protocol Unreachable)	6	2	1
57	Back Orifice	6	4	5
58	EXPLOIT NTPDX buffer overflow	6	4	3
59	IDS552/web-iis_IIS ISAPI Overflow ida nosize	3	3	2
60	EXPLOIT x86 setuid 0	3	3	3
61	EXPLOIT x86 stealth noop	2	2	2
62	WEB-CGI formmail access	2	2	1
63	ICMP Echo Request BSDtype	2	1	1
64	WEB-FRONTPAGE author.exe access	2	1	1
65	WEB-MISC whisker head	2	2	1
66	RPC tcp traffic contains bin_sh	2	2	2

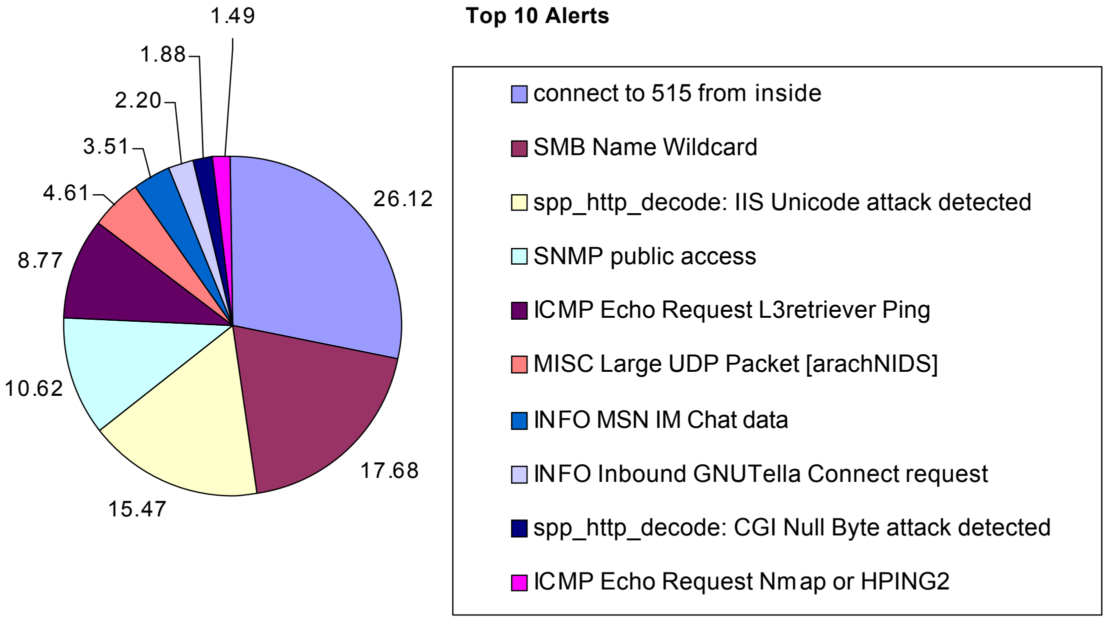
67	BACKDOOR NetMetro Incoming Traffic	1	1	1
68	BACKDOOR SIGNATURE - Q ICMP	1	1	1
69	IDS50/trojan_trojan-active-subseven	1	1	1
70	MISC PCAnywhere Startup	1	1	1
71	ICMP Address Mask Reply	1	1	1
72	WEB-MISC webdav search access [arachNIDS]	1	1	1
	Total	347144		

Top 10 Talkers:

Rank	Source IP	# of Alerts	Destination IP	# of Alerts
1	MY.NET.70.177	20333	MY.NET.150.198	90624
2	MY.NET.11.6	16182	MY.NET.11.6	34921
3	MY.NET.11.7	11234	MY.NET.11.7	24212
4	MY.NET.153.119	8336	211.115.213.202	6782
5	MY.NET.153.171	7375	MY.NET.153.197	6516
6	MY.NET.153.123	6090	MY.NET.150.195	5998
7	MY.NET.150.198	5014	209.10.239.135	5896
8	208.191.18.173	4934	MY.NET.11.5	4877
9	MY.NET.153.164	4735	MY.NET.5.96	3970
10	MY.NET.153.124	4708	MY.NET.152.109	3650

Many of these addresses are covered in the analysis however a few should be mentioned. 208.191.18.173 appeared to be directing attacks to 7 internal systems. These attacks took place on 3/20/2002 and lasted 7 hours. The attacks came in the form of known IIS exploits. It is recommended this IP be put on a watch list. Internal host MY.NET.5.96 needs to be examined by security personnel. This IP was the target of 21 different alerts and may be vulnerable to several exploits.

Alert Analysis:



The above graph represents 92 % of the alerts logged by Snort

connect to 515 from inside:

Description of Alert:
LPRng print service software runs on port 515/tcp. There are known vulnerabilities associated with this service (http://www.kb.cert.org/vuls/id/382365). These alerts indicate connections to port 515 from State University's network.

Sample traces from alert file:

```
03/20-08:00:28.416776  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
03/20-08:00:28.446096  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
03/20-08:00:28.449999  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
03/20-08:00:28.457970  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
03/20-08:00:28.468156  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
03/20-08:00:28.469382  [**] connect to 515 from inside [**] MY.NET.153.112:1436 -> MY.NET.150.198:515
```

Top Five Source/Destination Addresses:

Source IP	# of Alerts	Dest. IP	# of Alerts
MY.NET.153.119	7034	MY.NET.150.198	90613
MY.NET.153.123	5173	MY.NET.1.63	60
MY.NET.153.124	4554	MY.NET.5.35	13
MY.NET.153.171	4509	MY.NET.150.41	1
MY.NET.153.164	4441	N/A	N/A

Analysis and Discussion:
It is quite evident from the data that the vast majority of these alerts originate from hosts

on the 153 subnet. It is also noted that MY.NET.150.198 (a Top 10 talker) is the destination for 90613 of the 90687 alerts. Even without the tcpdump file, it is safe to say these alerts are false positives and MY.NET.150.198 is a print server for a department or large group of users.

It is suggested a snort "pass" rule for this signature be included for MY.NET.150.198. This will reduce the high amount of false positives.

SMB Name Wildcard:
Description of Alert:
This signature is associated with a windows machine NetBIOS query. According to Robert Graham, http://www.robertgraham.com/pubs/firewall-seen.html#netbios,

> "Windows machines use both a source port of 137 as well as a destination port of 137. In contrast, if UNIX machines attempt to resolve NetBIOS names (via SAMBA), they will use dynamic ports above 1024.
> If the Windows box is trying to find the name for the IP address 192.0.2.21, it will do the following steps:
>
> - Lookup the DNS "PTR" record for 21.2.0.192.in-addr.arpa; this request is sent to the local DNS server, which recursively forwards the query to the appropriate DNS server as required.
> - If the DNS answer comes back, it *won't* query NetBIOS. If a negative response comes back, it will immediately query NetBIOS. If the DNS server times-out, it will wait 14-seconds, then query NetBIOS.
> - When resolving with NetBIOS, it will send out a "NodeStatus" query that is sent to the 192.0.2.12:137 from x.x.x.x:137. (I.e. the query is sent to the IP address being resolved to its port 137, and is sent from the Windows machine port 137).
> - The NetBIOS request is a "NodeStatus" query that looks up the name "*". It is 50 bytes worth of data (58 including the UDP header, 78 including the IP header, 92 including an Ethernet header).
> - Three NetBIOS queries are sent with a 1.5 second timeout.

Hence the wildcard character "*" is part of the signature.

Sample traces from alert file:

```
03/22-00:00:29.019960  [**] SMB Name Wildcard [**] MY.NET.152.245:137 -> MY.NET.11.6:137
03/22-00:00:29.020391  [**] SMB Name Wildcard [**] MY.NET.11.6:137 -> MY.NET.152.245:137
03/22-00:00:36.736545  [**] SMB Name Wildcard [**] MY.NET.152.252:137 -> MY.NET.11.6:137
03/22-00:00:36.736892  [**] SMB Name Wildcard [**] MY.NET.11.6:137 -> MY.NET.152.252:137
03/22-00:01:12.370486  [**] SMB Name Wildcard [**] MY.NET.152.169:137 -> MY.NET.11.7:137
03/22-00:01:12.371018  [**] SMB Name Wildcard [**] MY.NET.11.7:137 -> MY.NET.152.169:137
03/22-00:01:13.589813  [**] SMB Name Wildcard [**] MY.NET.152.175:137 -> MY.NET.11.7:137
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.11.6	16182	MY.NET.11.6	16164
MY.NET.11.7	11234	MY.NET.11.7	11176
MY.NET.11.5	2415	MY.NET.11.5	2405
MY.NET.152.159	1097	MY.NET.152.159	1099
MY.NET.152.165	700	MY.NET.152.165	704

Analysis and Discussion:
The data does not suggest any active scanning for open window shares or information gathering. Over 44% of the NetBIOS probes are from IPs MY.NET.11.6 and MY.NET.11.7. Also, 100 percent of the probes are internal.

Robert Graham (http://www.robertgraham.com/pubs/netbios) mentions "NetBIOS requests to UDP port 137 are the most common item you will see in your firewall reject logs. This comes about from a *feature* in Microsoft's Windows: when a program resolves an **IP address** into a **name**, it *may* send a NetBIOS query to IP address. This is part of the *background radiation* of the Internet, and is nothing to be concerned about."

spp_http_decode: IIS Unicode attack detected

Description of Alert:
One powerful feature of snort is the preprocessor (spp). According to James Kipp's GIAC paper Using Snort as an IDS and Network Monitor in Linux, http://rr.sans.org/intrusion/monitor.php :
"Preprocessors are directives that examine the packets before the actual rules are applied. It can be used to filter out packets that you don't want being processed by Snort or to modify parts of the packets before being analyzed by Snort rules"

The spp_http_decode preprocessor examines packets for the common Unicode attack on some versions of Microsoft's IIS web server application. Specially crafted CGI URL strings directed to IIS servers, using Unicode characters, can bypass the IIS security check and result in an attacker exploiting the server by means of command execution or file access. For more information on the Unicode vulnerability, please see Andrew Brannan's paper at http://rr.sans.org/threats/unicode.php.

Sample traces from alert file:

```
03/20-10:56:09.193949  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2458 -> MY.NET.88.217:80
03/20-10:56:09.200378  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2459 -> MY.NET.88.217:80
03/20-10:56:09.340129  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2460 -> MY.NET.88.217:80
03/20-10:56:09.442522  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2467 -> MY.NET.88.217:80
```

```
03/20-10:56:MY.NET00115  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2466 -> MY.NET.88.217:80
03/20-10:56:10.473387  [**] spp_http_decode: IIS Unicode attack detected [**] 208.191.18.173:2473 -> MY.NET.88
.217:80
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.153.127	3389	211.115.213.202	6782
MY.NET.150.232	3276	211.115.213.207	1703
MY.NET.153.113	2738	211.233.29.207	1614
208.191.18.173	2784	211.233.29.216	1301
MY.NET.153.153	2149	211.233.29.212	988

Analysis and Discussion:

There has been discussion of flaws in the spp_http_decode preprocessor on incidents.org. It appears the same packet is flagged multiple times as having the IIS Unicode attack (http://www.incidents.org/archives/intrusions/msg04079.html). What this results in are multiple alerts for "spp_http_decode: IIS Unicode attack detected" giving the false impression of the magnitude of this "problem". Below is a sample of the multiple date/time stamp problem:

```
 03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
03/21-10:31:59.327775  [**] spp_http_decode: IIS Unicode attack detected [**] MY.NET.153.127:1947 -> 144.126.75.22:80
```

Matthew Fiddler' practical, http://www.giac.org/practical/Matthew_Fiddler_GCIA.doc, discusses the high false positive rate for this detect.

"The IIS Unicode attack alert is a very common “False Positive” This alert attempts to identify hostile traffic by interpreting unicode data as an attempt to obfuscate an attack. Based on the varying distribution of source and destination addresses these alerts appear to be false positives. GIAC University may want to investigate removing this alert from their configuration.
http://archives.neohapsis.com/archives/snort/2001-08/0528.html".

This appears to be the case here. From reviewing the data, all of the "Top Five" source IPs visited / revisited a limited number of sites and the time intervals spent at each site suggest web surfing.

A WHOIS on 208.191.18.173:

American Association of Petroleum (NETBLK-SBCIS81285)

225 1/2 North 3rd Okemah, OK 74859 US

Netname: SBCIS81285

Netblock: 208.191.18.168 - 208.191.18.175

Coordinator:

Southwestern Bell Internet Services (ZS44-ARIN) ipadmin@swbell.net 888-212-5411

Record last updated on 11-Feb-2000.

Database last updated on 12-May-2002 19:57:36 EDT.

It is recommended to decrease the number of false positives due to this alert, the preprocessor string, in snort.conf , should resemble:

preprocessor http_decode: 80 -unicode –cginull

SNMP public access:

Description of Alert:

The Simple Network Management Protocol runs on port 161. It is a tool network administrators use to gather information from and manage network devices, such as routers. By means of "public" and "private" default community strings, an attacker can gain information about a device (public) and write configuration information (private) to the device. Please refer to www.sans.org/newlook/resources/IDFAQ/SNMP.htm for further information.

Sample traces from alert file:

```
03/20-00:01:14.872178  [**] SNMP public access [**] MY.NET.150.41:1026 -> MY.NET.152.109:161
03/20-00:01:19.320878  [**] SNMP public access [**] MY.NET.153.191:1029 -> MY.NET.150.147:161
03/20-00:01:19.320988  [**] SNMP public access [**] MY.NET.153.191:1029 -> MY.NET.150.147:161
03/20-00:01:21.763457  [**] SNMP public access [**] MY.NET.150.41:1026 -> MY.NET.152.109:161
03/20-00:01:27.778444  [**] SNMP public access [**] MY.NET.150.41:1026 -> MY.NET.152.109:161
03/20-00:01:33.789587  [**] SNMP public access [**] MY.NET.150.41:1026 -> MY.NET.152.109:161
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.70.177	20310	MY.NET.150.195	5927
MY.NET.150.198	5013	MY.NET.152.109	3650
MY.NET.153.220	1725	MY.NET.5.248	2610
MY.NET.88.203	1260	MY.NET.5.143	2557
MY.NET.88.145	1235	MY.NET.5.137	2516

Analysis and Discussion:

A total of 36882 alerts were logged for this signature of which the Top 5 source IPs were responsible for 29534 or 80.1%. There was no evidence of SNMP queries from outside entering the State University network or SNMP traffic from inside to outside State's address space.

MY.NET.70.177 (Top 10 talker) was very active. However, from reviewing the portscan logs, this IP performed regular polling to port 161 at regular intervals to a group of IPs on subnet 5.

```
Mar 20 01:08:29 MY.NET.70.177:4662 -> MY.NET.5.31:32774 SYN ******S*
Mar 20 01:08:29 MY.NET.70.177:1068 -> MY.NET.5.31:161 UDP
Mar 20 01:08:29 MY.NET.70.177:4661 -> MY.NET.5.31:111 SYN ******S*
Mar 20 01:08:29 MY.NET.70.177:4666 -> MY.NET.5.37:135 SYN ******S*
Mar 20 01:08:29 MY.NET.70.177:4670 -> MY.NET.5.37:1032 SYN ******S*
Mar 20 01:08:29 MY.NET.70.177:1068 -> MY.NET.5.37:161 UDP
Mar 20 01:13:34 MY.NET.70.177:4710 -> MY.NET.5.79:111 SYN ******S*
Mar 20 01:13:34 MY.NET.70.177:4711 -> MY.NET.5.79:32774 SYN ******S*
Mar 20 01:13:36 MY.NET.70.177:4714 -> MY.NET.5.31:111 SYN ******S*
Mar 20 01:13:36 MY.NET.70.177:4715 -> MY.NET.5.31:32774 SYN ******S*
Mar 20 01:13:36 MY.NET.70.177:1068 -> MY.NET.5.31:161 UDP
Mar 20 01:13:37 MY.NET.70.177:4717 -> MY.NET.5.83:135 SYN ******S*
Mar 20 01:13:37 MY.NET.70.177:4719 -> MY.NET.5.83:1029 SYN ******S*
Mar 20 01:13:37 MY.NET.70.177:1068 -> MY.NET.5.83:161 UDP
Mar 20 01:32:22 MY.NET.70.177:4753 -> MY.NET.5.92:135 SYN ******S*
Mar 20 01:32:22 MY.NET.70.177:4755 -> MY.NET.5.92:1029 SYN ******S*
Mar 20 01:32:22 MY.NET.70.177:1068 -> MY.NET.5.92:161 UDP
Mar 20 01:32:22 MY.NET.70.177:4756 -> MY.NET.5.96:135 SYN ******S*
Mar 20 01:32:22 MY.NET.70.177:4758 -> MY.NET.5.96:1030 SYN ******S*
Mar 20 01:32:22 MY.NET.70.177:1068 -> MY.NET.5.96:161 UDP
Mar 20 01:32:23 MY.NET.70.177:4762 -> MY.NET.5.128:135 SYN ******S*
Mar 20 01:32:23 MY.NET.70.177:4764 -> MY.NET.5.128:1030 SYN ******S*
Mar 20 01:32:24 MY.NET.70.177:4765 -> MY.NET.5.127:135 SYN ******S*
Mar 20 01:32:24 MY.NET.70.177:4768 -> MY.NET.5.127:1030 SYN ******S*
Mar 20 01:32:24 MY.NET.70.177:1068 -> MY.NET.5.127:161 UDP
Mar 20 01:32:25 MY.NET.70.177:1068 -> MY.NET.5.143:161 UDP
Mar 20 01:32:25 MY.NET.70.177:4772 -> MY.NET.5.141:135 SYN ******S*
Mar 20 01:32:25 MY.NET.70.177:4774 -> MY.NET.5.141:1031 SYN ******S*
Mar 20 01:32:25 MY.NET.70.177:1068 -> MY.NET.5.141:161 UDP
Mar 20 01:32:28 MY.NET.70.177:1068 -> MY.NET.5.137:161 UDP
Mar 20 02:08:31 MY.NET.70.177:4803 -> MY.NET.5.31:111 SYN ******S*
Mar 20 02:08:31 MY.NET.70.177:4804 -> MY.NET.5.31:32774 SYN ******S*
Mar 20 02:08:31 MY.NET.70.177:1068 -> MY.NET.5.31:161 UDP
Mar 20 02:08:31 MY.NET.70.177:4801 -> MY.NET.5.37:135 SYN ******S*
Mar 20 02:08:31 MY.NET.70.177:4805 -> MY.NET.5.37:1032 SYN ******S*
Mar 20 02:08:32 MY.NET.70.177:1068 -> MY.NET.5.37:161 UDP
Mar 20 02:13:36 MY.NET.70.177:4847 -> MY.NET.5.79:111 SYN ******S*
Mar 20 02:13:36 MY.NET.70.177:4848 -> MY.NET.5.79:32774 SYN ******S*
Mar 20 02:13:38 MY.NET.70.177:4851 -> MY.NET.5.31:111 SYN ******S*
Mar 20 02:13:38 MY.NET.70.177:4850 -> MY.NET.5.31:32774 SYN ******S*
Mar 20 02:13:38 MY.NET.70.177:1068 -> MY.NET.5.31:161 UDP
Mar 20 02:13:39 MY.NET.70.177:4853 -> MY.NET.5.83:135 SYN ******S*
Mar 20 02:13:39 MY.NET.70.177:4855 -> MY.NET.5.83:1029 SYN ******S*
Mar 20 02:13:39 MY.NET.70.177:1068 -> MY.NET.5.83:161 UDP
Mar 20 02:32:22 MY.NET.70.177:4885 -> MY.NET.5.92:135 SYN ******S*
Mar 20 02:32:22 MY.NET.70.177:4887 -> MY.NET.5.92:1029 SYN ******S*
Mar 20 02:32:22 MY.NET.70.177:1068 -> MY.NET.5.92:161 UDP
Mar 20 02:32:22 MY.NET.70.177:4888 -> MY.NET.5.96:135 SYN ******S*
Mar 20 02:32:22 MY.NET.70.177:4890 -> MY.NET.5.96:1030 SYN ******S*
Mar 20 02:32:22 MY.NET.70.177:1068 -> MY.NET.5.96:161 UDP
Mar 20 02:32:23 MY.NET.70.177:4894 -> MY.NET.5.128:135 SYN ******S*
Mar 20 02:32:23 MY.NET.70.177:4896 -> MY.NET.5.128:1030 SYN ******S*
Mar 20 02:32:24 MY.NET.70.177:4897 -> MY.NET.5.127:135 SYN ******S*
Mar 20 02:32:24 MY.NET.70.177:4899 -> MY.NET.5.127:1030 SYN ******S*
Mar 20 02:32:24 MY.NET.70.177:1068 -> MY.NET.5.127:161 UDP
Mar 20 02:32:25 MY.NET.70.177:1068 -> MY.NET.5.143:161 UDP
Mar 20 02:32:25 MY.NET.70.177:4903 -> MY.NET.5.141:135 SYN ******S*
Mar 20 02:32:25 MY.NET.70.177:4905 -> MY.NET.5.141:1031 SYN ******S*
Mar 20 02:32:25 MY.NET.70.177:1068 -> MY.NET.5.141:161 UDP
Mar 20 02:32:28 MY.NET.70.177:1068 -> MY.NET.5.137:161 UDP
Mar 20 03:08:33 MY.NET.70.177:4925 -> MY.NET.5.31:111 SYN ******S*
Mar 20 03:08:33 MY.NET.70.177:4926 -> MY.NET.5.31:32774 SYN ******S*
```

MY.NET.10.177 appears to be a legitimate SNMP management tool. There was no evidence of portscans being performed from this host.

The alert logs indicate a total of 23 hosts querying 145 targets via the SNMP "public" string. It appears this SNMP traffic is not malicious in nature but perhaps State University should take an inventory to determine which devices are truly SNMP management devices. Another suggestion would be to write a pass rule in Snort for MY.NET.70.177 to reduce the amount of alerts.

ICMP Echo Request L3retriever Ping:

Description of Alert:

According to http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids311&view=event, the L3retriever ping "may indicate that someone is scanning your network using the L3 "Retriever 1.5" security scanner. This legitimate security tool is for authorized security assessment and should not be used on unauthorized networks. "

Sample traces from alert file:

```
03/20-00:00:19.756538  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.19 -> MY.NET.11.6
03/20-00:00:23.426629  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.185 -> MY.NET.11.7
03/20-00:00:26.795532  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.251 -> MY.NET.11.6
03/20-00:00:32.130625  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.13 -> MY.NET.11.6
03/20-00:00:40.152217  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.247 -> MY.NET.11.7
03/20-00:00:59.454899  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.22 -> MY.NET.11.6
03/20-00:02:16.642948  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.183 -> MY.NET.11.6
03/20-00:02:31.715843  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.46 -> MY.NET.11.7
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.152.159	1097	MY.NET.11.6	16333
MY.NET.152.165	734	MY.NET.11.7	11215
MY.NET.152.172	672	MY.NET.11.5	2472
MY.NET.152.157	659	MY.NET.5.4	249
MY.NET.152.160	576	MY.NET.10.49	73

Analysis and Discussion:

30443 alerts were logged for ICMP Echo Request L3retriever Ping and 27548 (90.5%) were directed towards MY.NET.11.6 and 11.7. Information from whitehats.com (http://www.whitehats.com/IDS/311) suggests this signature results in false positives from Win2k boxes communicating with a domain controller.

If we look at the snort signature for L3Retriever Ping and whitehats' IDS169/PING-WINDOWS9X2000, there are similarities:

L3Retriever:

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; content: "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; itype: 8; icode: 0; depth: 32; reference:arachnids,311; classtype:attempted-recon; sid:466; rev:1;)
```

IDS169/PING-WINDOWS9X2000:

```
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS169/icmp_ping-windows9x2000"; dsize: 32; itype: 8; content: "abcdefghijklmnopqrstuvwabcdefghi"; depth: 32; classtype: info-attempt; reference: arachnids,169;)
```

And if we hone in on 11.7 and look at sample alerts, we notice a pattern:

```
03/20-00:05:23.621714  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.252 -> MY.NET.11.7
03/20-00:05:23.621885  [**] SMB Name Wildcard [**] MY.NET.152.252:137 -> MY.NET.11.7:137
03/20-00:05:23.622121  [**] SMB Name Wildcard [**] MY.NET.11.7:137 -> MY.NET.152.252:137
03/20-00:05:29.853299  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.172 -> MY.NET.11.7
03/20-00:05:29.853770  [**] SMB Name Wildcard [**] MY.NET.152.172:137 -> MY.NET.11.7:137
03/20-00:05:29.854201  [**] SMB Name Wildcard [**] MY.NET.11.7:137 -> MY.NET.152.172:137
03/20-00:05:30.407419  [**] ICMP Echo Request L3retriever Ping [**] MY.NET.152.246 -> MY.NET.11.7
03/20-00:05:30.408839  [**] SMB Name Wildcard [**] MY.NET.152.246:137 -> MY.NET.11.7:137
03/20-00:05:30.409194  [**] SMB Name Wildcard [**] MY.NET.11.7:137 -> MY.NET.152.246:137
```

Each L3Retriever ping is followed up with a SMB Name Wildcard alert. As mentioned earlier in this report, the SMB Name Wildcard is a false positive associated with windows hosts attempting name resolution, via NetBIOS, by contacting domain controllers.

This lends credence to the whitehats.com site mentioning that L3Retriever alerts are also false positives due to windows hosts communicating with domain controllers.

MISC Large UDP Packet:

Description of Alert:
An unusually large UDP packet that is greater than 4000 bytes triggers this event. It may indicate a Denial of Service attack or covert channel (per www.whitehats.com/IDS/247).

Sample traces from alert file:

```
03/22-15:38:27.894657  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
03/22-15:38:29.137553  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
03/22-15:38:29.232780  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
03/22-15:38:29.429994  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
03/22-15:38:29.533086  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
03/22-15:38:30.614972  [**] MISC Large UDP Packet [**] 210.94.0.146:0 -> MY.NET.153.196:0
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
63.240.15.204	2546	MY.NET.153.197	6435
63.240.15.199	2526	MY.NET.153.196	2600
202.98.15.138	2385	MY.NET.153.152	2385
63.240.15.207	1837	MY.NET.153.208	1375
63.240.15.205	1357	MY.NET.153.184	1297

Analysis and Discussion:

Below, please find a breakdown of the Top 5 Source IP traffic for this signature and the top destination IPs:

```
  41    MISC Large UDP Packet [**] 63.240.15.204:40733 -> MY.NET.153.184:2028
 945    MISC Large UDP Packet [**] 63.240.15.204:58031 -> MY.NET.153.196:2370
 238    MISC Large UDP Packet [**] 63.240.15.204:58693 -> MY.NET.153.197:1780
 660    MISC Large UDP Packet [**] 63.240.15.199:45869 -> MY.NET.153.196:2461
 789    MISC Large UDP Packet [**] 63.240.15.199:56446 -> MY.NET.153.197:1828
1830    MISC Large UDP Packet [**] 63.240.15.207:21010 -> MY.NET.153.197:1883
2007    MISC Large UDP Packet [**] 202.98.15.138:1832 -> MY.NET.153.152:1171
1222    MISC Large UDP Packet [**] 63.240.15.205:2560 -> MY.NET.153.197:1753
```

A Whois for the 63.240.15.204, 63.240.15.199, and 63.240.15.207, and 63.240.15.205:

```
[whois.arin.net]
AT&T CERFnet (NETBLK-CERFNET-BLK-5)
  P.O. Box 919014
  San Diego, CA  92191
  US

  Netname: CERFNET-BLK-5
  Netblock: 63.240.0.0 - 63.242.255.255
  Maintainer: CERF

  Coordinator:
    AT&T Enhanced Network Services  (CERF-HM-ARIN)  dns@CERF.NET
    (619) 812-5000

  Domain System inverse mapping provided by:

  DBRU.BR.NS.ELS-GMS.ATT.NET   199.191.128.106
  CBRU.BR.NS.ELS-GMS.ATT.NET   199.191.128.105
  DMTU.MT.NS.ELS-GMS.ATT.NET   12.127.16.70
  CMTU.MT.NS.ELS-GMS.ATT.NET   12.127.16.69

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
```

```
Record last updated on 06-Aug-2001.
Database last updated on  14-May-2002 19:59:13 EDT.
```

202.98.15.138:

```
inetnum:     202.98.15.0 - 202.98.15.255
netname:     CC-MULTI-MEDIA-NET
descr:       Changchun City, Multi-media Communication Network, Jilin Province. China.
country:     CN
admin-c:     ZB17-AP
tech-c:      ZB17-AP
mnt-by:      MAINT-CHINANET-JL
changed:     wtg@mail.jl.cn 20000825
source:      APNIC

person:      ZHAO BO
address:     96,JieFang Road ChangChun 130021 China
country:     CN
phone:       +86-431-8984045
fax-no:      +86-431-8984040
e-mail:      kejyfw@public.cc.jl.cn
nic-hdl:     ZB17-AP
mnt-by:      MAINT-CHINANET-JL
changed:     kejyfw@public.cc.jl.cn 20000614
source:      APNIC
```

Todd Chapman mentioned in his practical (www.giac.org/practical/Todd_Chapman_GCIA.doc) , that these large UPD packets were streaming media apps and non-malicious. By reviewing the data, I noticed the majority of these packets were going to subnet 153.   If this is the subnet for student housing, then this traffic can be explained as students streaming media using Windows Media Services.

According to

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q189416, "When using UDP streams, the client first makes a connection to the Windows Media server using TCP port 1755. After this connection is established, the client and the server choose the UDP port that will be used by the server to stream the Windows Media content down to the client."

If the client makes a connection to the server on port 1755, perhaps the portscan logs will show client connection. Well, sure enough, it did:

```
Mar 21 11:36:03 MY.NET.153.184:2024 -> 63.240.15.204:1755 SYN ******S*
Mar 21 16:01:12 MY.NET.153.196:2395 -> 63.240.15.199:1755 SYN ******S*
Mar 22 10:30:35 MY.NET.153.197:1749 -> 63.240.15.205:1755 SYN ******S*
Mar 22 10:45:49 MY.NET.153.197:1879 -> 63.240.15.207:1755 SYN ******S*
```

This correlates with the alert logs showing clients in the 152 subnet-initiated communication to 63.240.15.x. This traffic is streaming media to media servers on the ATT netblock . The large UPD packets triggered the alert.

A further look portscan logs at traffic from 202.98.15.138 reveals the following:

```
Mar 21 11:24:32 MY.NET.153.152:1170 -> 202.98.15.138:1755 UDP
Mar 21 11:25:17 202.98.15.138:0 -> MY.NET.153.152:0 UDP
Mar 21 11:25:11 202.98.15.138:9418 -> MY.NET.153.152:18793 UDP
Mar 21 11:25:17 202.98.15.138:1832 -> MY.NET.153.152:1171 UDP
Mar 21 11:25:13 202.98.15.138:47217 -> MY.NET.153.152:1846 UDP
Mar 21 11:25:14 202.98.15.138:25956 -> MY.NET.153.152:29999 UDP
Mar 21 11:25:21 202.98.15.138:0 -> MY.NET.153.152:0 UDP
Mar 21 11:25:21 202.98.15.138:1832 -> MY.NET.153.152:1171 UDP
Mar 21 11:25:21 202.98.15.138:28518 -> MY.NET.153.152:8308 UDP
Mar 21 11:25:25 202.98.15.138:0 -> MY.NET.153.152:0 UDP
Mar 21 11:25:25 202.98.15.138:1832 -> MY.NET.153.152:1171 UDP
Mar 21 11:25:24 202.98.15.138:52096 -> MY.NET.153.152:41059 UDP
Mar 21 11:25:25 202.98.15.138:18354 -> MY.NET.153.152:27938 UDP
```

It does appear that a streaming media session was initiated to 202.98.15.138:1755 from MY.NET.153.152 and the ephemeral ports established between client and server were 1832 and 1171 respectively. However, what's all this other UDP traffic? Evidently these packets are smaller than 4000 bytes. The high ephemeral ports could indicate trojan activity. It is recommended 202.98.15.138 be put on a watchlist and the host MY.NET.153.152 be checked out

INFO MSN IM Chat Data:

Description of Alert:
Microsoft Instant Messenger Service allows users to communicate with other users over the Internet. It allows users to "talk" via messages, send files, and establish voice communication (http://www.giac.org/practical/jeffrey_widom_GSEC.doc). The ability to send files over this channel opens up the risk to malware being transferred to victim's computers.

This rule alerts to MSN IM packets communicating over source port 1863.

Sample traces from alert file:

```
3/20-09:55:48.260800  [**] INFO MSN IM Chat data [**] 64.4.12.182:1863 -> MY.NET.153.110:2453
03/20-09:55:50.387724  [**] INFO MSN IM Chat data [**] 64.4.12.196:1863 -> MY.NET.153.142:1711
03/20-09:55:50.989238  [**] INFO MSN IM Chat data [**] MY.NET.153.110:2453 -> 64.4.12.182:1863
03/20-09:56:04.248117  [**] INFO MSN IM Chat data [**] MY.NET.153.110:2453 -> 64.4.12.182:1863
03/20-09:56:04.696509  [**] INFO MSN IM Chat data [**] 64.4.12.182:1863 -> MY.NET.153.110:2453
03/20-09:56:12.194404  [**] INFO MSN IM Chat data [**] MY.NET.153.142:1711 -> 64.4.12.196:1863
03/20-09:56:20.839467  [**] INFO MSN IM Chat data [**] 64.4.12.196:1863 -> MY.NET.153.142:1711
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
64.4.12.191	1111	MY.NET.153.111	1178
MY.NET.153.111	671	64.4.12.191	869
64.4.12.163	488	MY.NET.153.110	584
MY.NET.88.165	479	MY.NET.153.165	536
64.4.12.187	479	MY.NET.88.165	466

Analysis and Discussion:

12181 alerts were logged for 104 source and 101 destination addresses. From looking at the data this appears to be standard internet chatting. Of course, without the tcpdump logs it cannot be determined if the payload is of malicious intent. These sessions lasted from a few minutes to a few hours. Much like a conversation between 2 people, multiple packets at a time were exchanged between two addresses.

All of the traffic (except one packet) was between State's address space and the 64.4.12.x domain. A whois on this domain is below:

```
MS Hotmail (NETBLK-HOTMAIL)
  1065 La Avenida
  Mountain View, CA 94043
  US

  Netname: HOTMAIL
  Netblock: 64.4.0.0 - 64.4.63.255

  Coordinator:
    Myers, Michael  (MM520-ARIN)  icon@HOTMAIL.COM
    650-693-7072

  Domain System inverse mapping provided by:

  NS1.HOTMAIL.COM            216.200.206.140
  NS3.HOTMAIL.COM            209.185.130.68

  Record last updated on 09-Jan-2001.
  Database last updated on  14-May-2002 19:59:13 EDT.
```

These alerts appear to be false positives, however, it is recommended snort signatures be added for the latest vulnerability in MSN Chat ActiveX control. Information can be found at http://www.cert.org/advisories/CA-2002-13.html. Because internet chat is allowed at the University, this can become a significant security problem for the State University's network.

INFO Inbound GNUTella Connect request:

Description of Alert:
This alert is triggered when a packet contains the string “GNUTELLA CONNECT”, coming from an external address. GNUtella is peer-to-peer software that allows users to search/share/download files to/from other users across the internet. It is widely utilized to share/download music and multimedia files. An external address is requesting to make a connection to an internal GNUtella p2p client.

Sample traces from alert file:

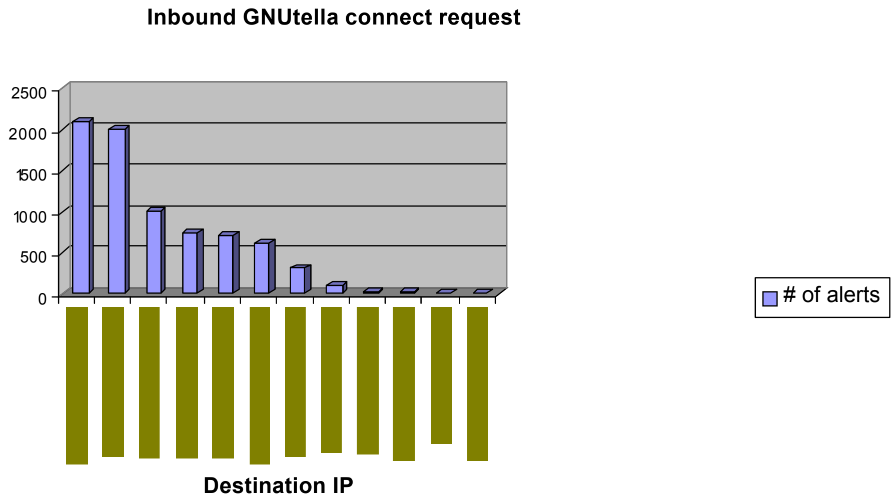
```
03/20-00:03:19.783936  [**] INFO Inbound GNUTella Connect request [**] 208.11.83.130:2026 ->
MY.NET.150.209:6346
03/20-00:03:25.987436  [**] INFO Inbound GNUTella Connect request [**] 172.170.27.13:1851 ->
MY.NET.150.209:6346
03/20-00:03:31.885281  [**] INFO Inbound GNUTella Connect request [**] 172.170.27.13:1851 ->
MY.NET.150.209:6346
03/20-00:04:54.082415  [**] INFO Inbound GNUTella Connect request [**] 80.128.200.29:1392 ->
MY.NET.150.209:6346
03/20-00:05:57.604011  [**] INFO Inbound GNUTella Connect request [**] 24.226.92.69:2064 ->
MY.NET.150.209:6346
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
66.72.181.8	19	MY.NET.153.208	2096
62.31.23.75	17	MY.NET.153.175	2000
172.144.141.182	16	MY.NET.153.145	999
66.69.139.195	13	MY.NET.153.178	729
63.229.205.134	12	MY.NET.153.159	720

Analysis and Discussion:

Of the 7644 alerts logged with this signature, there were 6003 distinct source IPs and only 12 destination IPs. Of the 12 source addresses, 8 were in the 153 subnet. It is obvious from the table above, the Top 5 destination IPs (85.6 % of alerts) were the most requested by the over 6000 external hosts.



This type of traffic is generally not considered malicious, however, it is a major network bandwidth hog. This *will* have a negative impact on network performance. According to Meredith Lynes GSEC paper “Internet File Sharing”,www.giac.org/practical/Meredith_Lynes_GSEC.doc: “Each Gnutella connection uses between 500 and 1000 BPS of bandwidth. In addition each Gnutella client typically broadcasts a ping every minute or so to discover all the other clients on the network. A 2000 client network will produce 4 billion icmp messages per minute. By it's very nature Gnutella may inadvertently produce a Denial of Service.”.

It is recommended this type P2P traffic be monitored and the bandwidth provided be capped. Limiting the bandwidth available to MY.NET.153.208 and MY.NET.153.175 may be a viable option.

spp_http_decode: CGI Null Byte attack detected:

Description of Alert:
Snort’s spp_http_decode preprocessor attempts to assemble http packets before passing it to the snort rule base. The CGI Null Byte option checks for the %00 string in http packets.
Sample traces from alert file:

```
03/21-10:31:03.353202  [**] spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.171:1544 -> 209.10
.239.135:80
03/21-10:31:03.353202  [**] spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.171:1544 -> 209.10
.239.135:80
03/21-10:31:03.353202  [**] spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.171:1544 -> 209.10
.239.135:80
03/21-10:31:03.353202  [**] spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.171:1544 -> 209.10
.239.135:80
03/21-10:31:03.353202  [**] spp_http_decode: CGI Null Byte attack detected [**] MY.NET.153.171:1544 -> 209.10
.239.135:80
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.153.197	2849	209.10.239.135	5896
MY.NET.153.171	2211	66.150.100.30	314
MY.NET.153.184	836	209.143.193.70	148
MY.NET.153.125	314	209.143.193.105	100
MY.NET.153.196	161	216.33.88.53	14

Analysis and discussion:

According to http://archives.neohapsis.com/archives/snort/2000-11/0244.html, the %00 characters are present in url encoded binary data and this causes many false positives for this alert. Of course the only way to check as to whether this is an attack is to check the packet payload. Since tcpdump files are not available, it can't be determined if these alerts are all false positives.

From looking at the 6516 alerts, 5896 (90 %) are for 209.10.239.135. Also, there are only 3 source IPs MY.NET.153.197, 153.171, and 153.184, visiting this web site. A Whois reveals the following:

```
Globix Corporation (NETBLK-GLOBIXBLK3)
  295 Lafayette St- 3rd Fl
  NY, NY 10012
  US

  Netname: GLOBIXBLK3
  Netblock: 209.10.0.0 - 209.11.223.255
  Maintainer: PFMC

  Coordinator:
    Hostmaster, Globix Corporation  (GCH2-ARIN)  arin-admin@GLOBIX.NET
    +1-212-334-8500 (FAX) 212.334.8615

  Domain System inverse mapping provided by:

  Z1.NS.NYC1.GLOBIX.NET       209.10.66.55
  Z1.NS.SJC1.GLOBIX.NET      209.MY.NET4.55
  Z1.NS.LHR1.GLOBIX.NET       212.111.32.38

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

  Record last updated on 09-May-2002.
  Database last updated on  16-May-2002 19:59:02 EDT.
```

More revealing is visiting 209.10.239.135 in your favorite browser will take to "Ifilm The

Internet Movie Guide"

These alerts appear to be false positives. It is recommended to decrease the number of false positives due to this alert, the preprocessor string, in snort.conf , should resemble:

preprocessor http_decode: 80 -unicode –cginull

ICMP Echo Request Nmap or HPING2:

Description of Alert:

This alert flags those ICMP echo request packets from the Nmap scanner or hping2 tool.

Sample traces from alert file:

```
03/21-17:46:06.614847  [**] ICMP Echo Request Nmap or HPING2 [**] MY.NET.152.16 -> MY.NET.11.6
03/21-17:50:15.193904  [**] ICMP Echo Request Nmap or HPING2 [**] MY.NET.152.19 -> MY.NET.11.6
03/21-17:50:56.741272  [**] ICMP Echo Request Nmap or HPING2 [**] MY.NET.152.164 -> MY.NET.11.7
03/21-17:51:49.065594  [**] ICMP Echo Request Nmap or HPING2 [**] MY.NET.152.160 -> MY.NET.11.7
03/21-17:53:13.617633  [**] ICMP Echo Request Nmap or HPING2 [**] MY.NET.152.166 -> MY.NET.11.7
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.253.10	896	MY.NET.11.6	2424
MY.NET.152.172	92	MY.NET.11.7	1821
MY.NET.152.171	89	MY.NET.153.220	13
MY.NET.152.165	87	MY.NET.1.3	6
MY.NET.152.162	86	MY.NET.150.44	5

Analysis and Discussion:

There were 5162 alerts for this signature. 82% of these alerts contained MY.NET.11.6 and 11.7. And all of this traffic is internal to State's network.

Nmap is a port scanner with the ablity to ping sweep entire address ranges. Hping2 is a packet crafting program used to send customized ICMP/UDP/TCP packets (http://www.insecure.org/tools.html). Both of these tools are used for port scanning or network reconnaissance. However, from looking at the data, no traffic is going to or coming from external networks. This rules out port scanning.

These alerts appear to be false positives. One speculation is 11.6 and 11.7 are domain controllers and Microsoft devices from around the network sending echo requests packets to these hosts. Without packet payload it is difficult to determine why this may be a false positive.

High port 65535 udp - possible Red Worm – traffic:

Description of Alert:

Anthony Dell reports in the SANS paper "Adore Worm – Another Mutation", http://rr.sans.org/threats/mutation.php**,** "The Adore worm, originally identified as the Red Worm, is a collection of programs and shell scripts contained in a file called *red.tar*. The

Adore worm attempts to gain unauthorized access to systems that are vulnerable to the LPRng, rpc-statd, and the Berkeley Internet Name Domain (BIND) software exploits."

This alert logs packets where connections are made to UDP port 65535.

Sample traces from alert file:

```
03/20-08:07:42.797091  [**] High port 65535 udp - possible Red Worm - traffic [**] MY.NET.6.50:65535 ->
MY.NE
T.152.14:65535
03/20-08:07:44.483020  [**] High port 65535 udp - possible Red Worm - traffic [**] MY.NET.6.50:65535 ->
MY.NE
T.152.14:65535
03/20-08:07:48.479923  [**] High port 65535 udp - possible Red Worm - traffic [**] MY.NET.6.50:65535 ->
MY.NE
T.152.14:65520
03/20-08:08:19.761885  [**] High port 65535 udp - possible Red Worm - traffic [**] MY.NET.6.52:65535 ->
MY.NE
T.153.169:65535
03/20-08:08:20.956532  [**] High port 65535 udp - possible Red Worm - traffic [**] MY.NET.6.52:65535 ->
MY.NE
T.153.169:65535
```

Top Five Source/Destination Addresses:

Source IP	# of alerts	Dest. IP	# of alerts
MY.NET.6.48	1131	MY.NET.153.153	150
MY.NET.6.52	1129	MY.NET.152.185	168
MY.NET.6.49	1008	MY.NET.153.209	155
MY.NET.6.50	918	MY.NET.153.177	125
MY.NET.6.53	150	MY.NET.153.150	123

Analysis and Discussion:

5016 alerts were logged for this signature. The Top 5 source IPs were responsible for 86.4 % of the alerts. In fact, these alerts accounted for over 95% of alerts for these 5 hosts.

Below are excerpts from the alert files:

```
Mar 20 09:17:28 10.3.6.48:65535 -> 10.3.152.179:65280 UDP
Mar 20 09:17:31 10.3.6.48:65535 -> 10.3.152.179:65535 UDP
Mar 20 09:17:46 10.3.6.48:65535 -> 10.3.152.179:65535 UDP
Mar 20 09:52:22 10.3.6.48:65535 -> 10.3.152.10:65535 UDP

Mar 20 08:59:11 10.3.6.49:65535 -> 10.3.153.148:65280 UDP
Mar 20 09:02:56 10.3.6.49:59583 -> 10.3.153.181:65535 UDP
Mar 20 09:07:24 10.3.6.49:41215 -> 10.3.153.197:65535 UDP
Mar 20 09:07:32 10.3.6.49:55551 -> 10.3.153.197:65535 UDP
Mar 20 09:07:33 10.3.6.49:65535 -> 10.3.153.197:65280 UDP
Mar 20 09:07:34 10.3.6.49:43263 -> 10.3.153.197:65535 UDP
Mar 20 09:07:40 10.3.6.49:65535 -> 10.3.153.197:65535 UDP

Mar 20 08:07:44 10.3.6.50:65535 -> 10.3.152.14:65535 UDP
Mar 20 08:07:48 10.3.6.50:65535 -> 10.3.152.14:65520 UDP
Mar 20 08:13:52 10.3.6.50:0 -> 10.3.153.167:65535 UDP
Mar 20 08:13:55 10.3.6.50:65535 -> 10.3.153.167:65535 UDP
Mar 20 08:14:00 10.3.6.50:65535 -> 10.3.153.167:65535 UDP

Mar 20 08:08:21 10.3.6.52:65535 -> 10.3.153.169:65535 UDP
Mar 20 08:28:24 10.3.6.52:65535 -> 10.3.153.169:65535 UDP
Mar 20 08:29:07 10.3.6.52:16383 -> 10.3.153.169:65535 UDP
Mar 20 08:33:18 10.3.6.52:55551 -> 10.3.153.169:65535 UDP
Mar 20 08:33:24 10.3.6.52:65535 -> 10.3.153.169:65535 UDP

Mar 20 00:00:56 10.3.6.53:65535 -> 10.3.153.204:65535 UDP
Mar 20 08:28:03 10.3.6.53:65535 -> 10.3.152.45:65408 UDP
Mar 20 08:28:19 10.3.6.53:65535 -> 10.3.152.45:65535 UDP
Mar 20 09:10:33 10.3.6.53:65535 -> 10.3.153.160:33732 UDP
Mar 20 09:55:34 10.3.6.53:57599 -> 10.3.153.182:65535 UDP
Mar 20 10:06:41 10.3.6.53:65535 -> 10.3.151.191:65535 UDP
Mar 20 10:37:33 10.3.6.53:65535 -> 10.3.152.167:65535 UDP
```

This pattern suggests these probes generally started between 8 and 9 AM on 3/20/02 for all the top 5 talkers and ended on 3/23/02 between 3:30 and 6:00 PM. Another interesting observance is all these hosts had UDP probes from port 7000 to port 7001.
Probes (taken from scan logs) between ports 7000 and 7001 totaled a staggering 106,311 for the top 5! Ports 7000 and 7001 are for the IBM file sharing protocol afs3.

This is all there is to go on. The Top 5 talkers may by IMB hosts running the afs3 file sharing protocol or Windows hosts running client software (http://www.linux-mag.com/2000-11/dfs_04.html). Is there a connection between afs and these anomalous probes from port 65535 UPD? Hard to say. It has been noted these probes all started and ended about the same time across all 5 hosts. Maybe new software was installed on the hosts and tested for a period of time.

It is highly recommended the Top 5 Source hosts be investigated to get to the bottom of this.

spp_portscan:

Description of Alert
An usually high amount of the alerts were portscans. Portscans are a common occurrence on the Internet. Hackers scan networks to discover open ports and operating system types in an effort to find vulnerable systems.

Sample trace:

```
spp_portscan: End of portscan from MY.NET.60.43: TOTAL time(100s) hosts(106) TCP(0) UDP(147) [**]
spp_portscan: End of portscan from MY.NET.60.43: TOTAL time(100s) hosts(38) TCP(0) UDP(59) [**]
spp_portscan: End of portscan from MY.NET.60.43: TOTAL time(100s) hosts(79) TCP(0) UDP(99) [**]
spp_portscan: End of portscan from MY.NET.60.43: TOTAL time(100s) hosts(92) TCP(0) UDP(127) [**]
```

Top 10 Talkers and Listeners:
The table below details the top source and destination IPs for portscans.

# of ports scanning	Src IP	# of ports scanned	Dst IP
419162	MY.NET.60.43	67426	MY.NET.1.3
378202	MY.NET.11.8	42900	MY.NET.6.45
136664	MY.NET.150.113	42329	MY.NET.11.6
94928	MY.NET.6.45	41758	MY.NET.1.4
86183	MY.NET.6.52	34445	MY.NET.60.43
82864	MY.NET.6.49	33407	MY.NET.11.7
72739	MY.NET.6.48	21865	MY.NET.153.162
66348	MY.NET.6.50	21799	MY.NET.5.55
42668	MY.NET.150.143	20439	MY.NET.152.157
40016	MY.NET.6.53	20355	MY.NET.5.50

Analysis:
From looking at the scan logs we can correlate specific scans:

MY.NET.60.43: This host is shows up a top talker and listener. The vast majority of the traffic is UDP port 123, network time protocol and is the network time server. This host makes up over 19 % of the scans logged.

Subnet 6 hosts have already been discussed.

MY.NET.11.6 and 11.7 are primary domain controllers.

MY.NET.150.143 logged 42668 alerts in a 120 hour period. Most of this traffic was web, but a significant portion was p2p communication. This host needs to be watch as it is generating a lot of traffic and may be a heavy bandwidth consumer.

MY.NET.153.162 is discussed later in this report.

MY.NET.152.157 is getting a lot of UPD traffic to port 7001. This port is for the IBM afs3 distributed file system.

Portscans of Interest

Scan # 1 FTP

On March 20, a portscan was performed on hosts in subnets 5, 88, and 149-153. What is interesting is the source port, except in a few cases, is port 21. Also, it appears selected hosts are scanned twice for dst port 21, once from dst. port 21 and later from an ephemeral port. This appears to be as automated scan and it is possible previous reconnaissance was performed since selected subnets and hosts were scanned.

I mention a speculation here about the high ephemeral src port. Perhaps when the automated script finds an open ftp port, it then telnets into the same host to port 21. By doing this, the ftp version is discovered.

There are multiple vulnerabilities for ftp as mentioned by CERT, http://www.cert.org/advisories/CA-2001-33.html.

```
Mar 20 02:24:22 64.152.183.174:21 -> MY.NET.5.25:21 SYNFIN ******SF
Mar 20 02:24:22 64.152.183.174:21 -> MY.NET.5.37:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.79:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:57219 -> MY.NET.5.79:21 SYN ******S*
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.83:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.85:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:57221 -> MY.NET.5.85:21 SYN ******S*
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.87:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.90:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.92:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:57222 -> MY.NET.5.92:21 SYN ******S*
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.95:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:57225 -> MY.NET.5.95:21 SYN ******S*
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.96:21 SYNFIN ******SF
Mar 20 02:24:23 64.152.183.174:21 -> MY.NET.5.97:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.101:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.102:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.103:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.104:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.105:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.106:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.108:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.109:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.127:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.128:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.137:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.141:21 SYNFIN ******SF
Mar 20 02:24:24 64.152.183.174:21 -> MY.NET.5.143:21 SYNFIN ******SF
Mar 20 02:24:26 64.152.183.174:21 -> MY.NET.5.204:21 SYNFIN ******SF
Mar 20 02:24:26 64.152.183.174:21 -> MY.NET.5.244:21 SYNFIN ******SF
Mar 20 02:31:27 64.152.183.174:21 -> MY.NET.88.130:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.131:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.142:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.145:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.146:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.148:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.149:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.151:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.152:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.153:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.154:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.156:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.158:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.159:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.161:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.162:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.163:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.164:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.169:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.170:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.175:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.178:21 SYNFIN ******SF
Mar 20 02:31:28 64.152.183.174:21 -> MY.NET.88.181:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.182:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.183:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.185:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.187:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:57363 -> MY.NET.88.187:21 SYN ******S*
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.188:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.189:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.192:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.198:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.203:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.207:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.216:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.217:21 SYNFIN ******SF
Mar 20 02:31:29 64.152.183.174:21 -> MY.NET.88.230:21 SYNFIN ******SF
Mar 20 02:31:30 64.152.183.174:21 -> MY.NET.88.245:21 SYNFIN ******SF
Mar 20 02:31:30 64.152.183.174:21 -> MY.NET.88.246:21 SYNFIN ******SF
Mar 20 02:36:36 64.152.183.174:21 -> MY.NET.149.17:21 SYNFIN ******SF
Mar 20 02:36:36 64.152.183.174:21 -> MY.NET.149.21:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.28:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.32:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.45:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.55:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.59:21 SYNFIN ******SF
Mar 20 02:36:37 64.152.183.174:21 -> MY.NET.149.60:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:21 -> MY.NET.150.2:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:21 -> MY.NET.150.3:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:21 -> MY.NET.150.6:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:21 -> MY.NET.150.14:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:21 -> MY.NET.150.16:21 SYNFIN ******SF
Mar 20 02:36:41 64.152.183.174:57577 -> MY.NET.150.16:21 SYN ******S*
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.24:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.41:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:57579 -> MY.NET.150.41:21 SYN ******S*
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.42:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.45:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.46:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.51:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.52:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.54:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.55:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:21 -> MY.NET.150.59:21 SYNFIN ******SF
Mar 20 02:36:42 64.152.183.174:57581 -> MY.NET.150.59:21 SYN ******S*
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.72:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.83:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:57583 -> MY.NET.150.83:21 SYN ******S*
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.84:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:57585 -> MY.NET.150.84:21 SYN ******S*
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.85:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.86:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.97:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.99:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.101:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:57587 -> MY.NET.150.101:21 SYN ******S*
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.103:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.104:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.106:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.107:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:57589 -> MY.NET.150.107:21 SYN ******S*
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.113:21 SYNFIN ******SF
Mar 20 02:36:43 64.152.183.174:21 -> MY.NET.150.114:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.132:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.133:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.139:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.142:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.143:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:57592 -> MY.NET.150.143:21 SYN ******S*
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.147:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:57595 -> MY.NET.150.147:21 SYN ******S*
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.160:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.165:21 SYNFIN ******SF
Mar 20 02:36:44 64.152.183.174:21 -> MY.NET.150.170:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.172:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.185:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.194:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.195:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:57597 -> MY.NET.150.195:21 SYN ******S*
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.197:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:57599 -> MY.NET.150.197:21 SYN ******S*
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.198:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.207:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.209:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.210:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.215:21 SYNFIN ******SF
Mar 20 02:36:45 64.152.183.174:21 -> MY.NET.150.220:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:57601 -> MY.NET.150.220:21 SYN ******S*
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.224:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.226:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:57603 -> MY.NET.150.226:21 SYN ******S*
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.231:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:57605 -> MY.NET.150.231:21 SYN ******S*
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.235:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.237:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.244:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.246:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.248:21 SYNFIN ******SF
Mar 20 02:36:46 64.152.183.174:21 -> MY.NET.150.250:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.17:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.18:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.28:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.31:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.53:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.63:21 SYNFIN ******SF
Mar 20 02:36:47 64.152.183.174:21 -> MY.NET.151.64:21 SYNFIN ******SF
Mar 20 02:36:44 MY.NET.150.139:21 -> 64.152.183.174:21 INVALIDACK ***A**SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.72:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.73:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.78:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.79:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.86:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.90:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.92:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.93:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.107:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.108:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.110:21 SYNFIN ******SF
Mar 20 02:36:48 64.152.183.174:21 -> MY.NET.151.114:21 SYNFIN ******SF
Mar 20 02:36:49 64.152.183.174:21 -> MY.NET.151.122:21 SYNFIN ******SF
Mar 20 02:36:49 64.152.183.174:21 -> MY.NET.151.124:21 SYNFIN ******SF
Mar 20 02:36:49 64.152.183.174:21 -> MY.NET.151.129:21 SYNFIN ******SF
Mar 20 02:36:49 64.152.183.174:21 -> MY.NET.151.132:21 SYNFIN ******SF
Mar 20 02:36:50 64.152.183.174:21 -> MY.NET.151.190:21 SYNFIN ******SF
Mar 20 02:36:50 64.152.183.174:21 -> MY.NET.151.191:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.10:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.11:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.12:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.13:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.14:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.16:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.17:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.18:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.19:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.20:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.21:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.30:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.44:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.45:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.46:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.47:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.48:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.49:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.52:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.53:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.54:21 SYNFIN ******SF
Mar 20 02:36:52 64.152.183.174:21 -> MY.NET.152.55:21 SYNFIN ******SF
Mar 20 02:36:53 64.152.183.174:21 -> MY.NET.152.65:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.120:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.123:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.124:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.125:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.127:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.139:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.140:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.141:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.142:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.143:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.144:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.145:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.147:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.148:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.149:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.150:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.151:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.152:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.157:21 SYNFIN ******SF
Mar 20 02:36:54 64.152.183.174:21 -> MY.NET.152.159:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.160:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.161:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.162:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.163:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.166:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.167:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.169:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.170:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.171:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.174:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.176:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.177:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.178:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.180:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.181:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.182:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.183:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.184:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.185:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.186:21 SYNFIN ******SF
Mar 20 02:36:55 64.152.183.174:21 -> MY.NET.152.188:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.212:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.213:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.214:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.215:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.216:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.244:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.245:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.246:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.247:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.248:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.250:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.251:21 SYNFIN ******SF
Mar 20 02:36:56 64.152.183.174:21 -> MY.NET.152.252:21 SYNFIN ******SF
Mar 20 02:36:57 64.152.183.174:21 -> MY.NET.153.45:21 SYNFIN ******SF
Mar 20 02:36:57 64.152.183.174:21 -> MY.NET.153.46:21 SYNFIN ******SF
Mar 20 02:36:58 64.152.183.174:21 -> MY.NET.153.71:21 SYNFIN ******SF
Mar 20 02:36:58 64.152.183.174:21 -> MY.NET.153.105:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.106:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.107:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.108:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.109:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.111:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.112:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.113:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.114:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.115:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.117:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.118:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.119:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.120:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.121:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.123:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.124:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.125:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.126:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.127:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.135:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.136:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.137:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.140:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.141:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.142:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.143:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.144:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.145:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.146:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.147:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.148:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.149:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.152:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.153:21 SYNFIN ******SF
Mar 20 02:36:59 64.152.183.174:21 -> MY.NET.153.154:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.157:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.159:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.160:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.162:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.163:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.165:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.166:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.167:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.169:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.170:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.173:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.174:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.175:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.176:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.177:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.179:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.180:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.181:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.184:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.185:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.186:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.187:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.188:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.189:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.190:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.191:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.193:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.194:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.195:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.196:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.197:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.198:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.199:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.200:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.203:21 SYNFIN ******SF
Mar 20 02:37:00 64.152.183.174:21 -> MY.NET.153.204:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.205:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.206:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.207:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.208:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.209:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.211:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.219:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:21 -> MY.NET.153.220:21 SYNFIN ******SF
Mar 20 02:37:01 64.152.183.174:57607 -> MY.NET.153.220:21 SYN ******S*
```

A Whois on 64.152.183.174 reveals the following:

```
iNYC (NETBLK-LVLT-SWIP-INYC-3)
  3040 Nostrand Ave.
  Marine Park, NY 11229
  US

  Netname: LVLT-SWIP-INYC-3
  Netblock: 64.152.176.0 - 64.152.183.255
  Maintainer: INYC

  Coordinator:
    Bradley, Christopher  (CB832-ARIN)  netadmin@inyc.com
    718-677-4111

  Domain System inverse mapping provided by:
```

```
DNS1.INYC.COM             63.211.38.10
DNS2.INYC.COM             63.211.38.11

Record last updated on 24-Oct-2000.
Database last updated on  16-May-2002 19:59:02 EDT.
```

It is recommended the user community be notified about ftp vulnerabilities and the fact that scanning for ftp is taking place. Many hackers are looking for anonymous accounts to dump warez. An inventory of FTP servers is recommended so to discover vulnerable versions.

Robert Schmaling GIAC practical recommends removing anonymous accounts . If anonymous ftp is allowed, ensure ACL's are properly set for directories.

Scan #2 Port 8888

MY.NET.153.113 is scanning for port 8888. The target addresses appear to be random. The only know service running on 8888 is Sun Answerbook (http) and News Edge Server. A search on CERT revealed no exploits for Answerbook , Newsedge or port 8888.

```
Mar 20 11:35:40 MY.NET.153.168:1247 -> 211.233.43.147:8888 SYN ******S*
Mar 20 15:00:27 MY.NET.150.103:4469 -> 216.187.118.222:8888 SYN ******S*
Mar 20 16:21:23 MY.NET.150.113:3710 -> 12.45.95.213:8888 SYN ******S*
Mar 20 16:21:24 MY.NET.150.113:3714 -> 4.61.189.132:8888 SYN ******S*
Mar 20 16:21:24 MY.NET.150.113:3716 -> 24.125.48.24:8888 SYN ******S*
Mar 20 16:21:28 MY.NET.150.113:3712 -> 80.116.199.81:8888 SYN ******S*
Mar 20 16:21:42 MY.NET.150.113:3722 -> 62.163.4.241:8888 SYN ******S*
Mar 20 16:21:41 MY.NET.150.113:3724 -> 80.135.93.193:8888 SYN ******S*
Mar 20 16:21:44 MY.NET.150.113:3725 -> 161.184.66.95:8888 SYN ******S*
Mar 20 16:21:44 MY.NET.150.113:3727 -> 62.211.22.123:8888 SYN ******S*
Mar 20 16:21:42 MY.NET.150.113:3728 -> 62.211.200.73:8888 SYN ******S*
Mar 20 16:21:42 MY.NET.150.113:3729 -> 63.149.6.91:8888 SYN ******S*
Mar 20 16:21:45 MY.NET.150.113:3729 -> 63.149.6.91:8888 SYN ******S*
Mar 20 16:21:50 MY.NET.150.113:3725 -> 161.184.66.95:8888 SYN ******S*
Mar 20 16:21:50 MY.NET.150.113:3727 -> 62.211.22.123:8888 SYN ******S*
Mar 20 16:21:51 MY.NET.150.113:3729 -> 63.149.6.91:8888 SYN ******S*
Mar 20 16:21:56 MY.NET.150.113:3736 -> 63.64.164.91:8888 SYN ******S*
Mar 20 16:21:54 MY.NET.150.113:3731 -> 212.58.188.146:8888 SYN ******S*
Mar 20 16:21:54 MY.NET.150.113:3737 -> 64.163.149.3:8888 SYN ******S*
Mar 20 16:21:56 MY.NET.150.113:3738 -> 62.211.45.118:8888 SYN ******S*
Mar 20 16:21:57 MY.NET.150.113:3738 -> 62.211.45.118:8888 SYN ******S*
Mar 20 16:22:00 MY.NET.150.113:3731 -> 212.58.188.146:8888 SYN ******S*
Mar 20 16:22:02 MY.NET.150.113:3736 -> 63.64.164.91:8888 SYN ******S*
Mar 20 16:22:16 MY.NET.150.113:3741 -> 217.39.139.173:8888 SYN ******S*
Mar 20 16:22:16 MY.NET.150.113:3743 -> 212.187.47.3:8888 SYN ******S*
Mar 20 16:22:18 MY.NET.150.113:3747 -> 63.64.164.91:8888 SYN ******S*
Mar 20 16:22:15 MY.NET.150.113:3748 -> 213.254.1.227:8888 SYN ******S*
Mar 20 16:22:15 MY.NET.150.113:3742 -> 204.96.98.13:8888 SYN ******S*
Mar 20 16:22:15 MY.NET.150.113:3749 -> 68.3.168.22:8888 SYN ******S*
Mar 20 16:22:18 MY.NET.150.113:3746 -> 62.211.28.35:8888 SYN ******S*
Mar 20 16:22:24 MY.NET.150.113:3746 -> 62.211.28.35:8888 SYN ******S*
Mar 20 16:22:48 MY.NET.150.113:3751 -> 67.81.94.246:8888 SYN ******S*
Mar 20 16:22:48 MY.NET.150.113:3753 -> 62.163.224.120:8888 SYN ******S*
Mar 20 16:22:52 MY.NET.150.113:3755 -> 216.175.64.208:8888 SYN ******S*
Mar 20 16:22:52 MY.NET.150.113:3756 -> 213.254.1.229:8888 SYN ******S*
Mar 20 16:22:56 MY.NET.150.113:3757 -> 62.211.17.210:8888 SYN ******S*
Mar 20 16:22:54 MY.NET.150.113:3758 -> 67.80.157.166:8888 SYN ******S*
Mar 20 16:23:00 MY.NET.150.113:3759 -> 212.241.132.51:8888 SYN ******S*
Mar 20 16:23:00 MY.NET.150.113:3760 -> 172.173.56.80:8888 SYN ******S*
Mar 20 16:23:00 MY.NET.150.113:3761 -> 12.250.207.35:8888 SYN ******S*
Mar 20 16:23:00 MY.NET.150.113:3762 -> 24.42.82.21:8888 SYN ******S*
Mar 20 16:23:03 MY.NET.150.113:3761 -> 12.250.207.35:8888 SYN ******S*
Mar 20 16:23:09 MY.NET.150.113:3762 -> 24.42.82.21:8888 SYN ******S*
Mar 20 16:23:16 MY.NET.150.113:3764 -> 62.64.223.135:8888 SYN ******S*
Mar 20 16:23:17 MY.NET.150.113:3764 -> 62.64.223.135:8888 SYN ******S*
Mar 20 16:23:17 MY.NET.150.113:3763 -> 213.254.1.230:8888 SYN ******S*
Mar 20 16:23:31 MY.NET.150.113:3766 -> 141.154.115.222:8888 SYN ******S*
Mar 20 16:23:35 MY.NET.150.113:3768 -> 210.54.37.137:8888 SYN ******S*
Mar 20 16:23:35 MY.NET.150.113:3769 -> 12.45.95.213:8888 SYN ******S*
Mar 20 16:23:34 MY.NET.150.113:3770 -> 213.93.78.164:8888 SYN ******S*
Mar 20 16:23:35 MY.NET.150.113:3767 -> 134.87.210.254:8888 SYN ******S*
Mar 20 16:23:40 MY.NET.150.113:3767 -> 134.87.210.254:8888 SYN ******S*
Mar 20 16:23:49 MY.NET.150.113:3771 -> 4.61.189.132:8888 SYN ******S*
Mar 20 16:23:49 MY.NET.150.113:3773 -> 24.125.48.24:8888 SYN ******S*
Mar 20 16:23:50 MY.NET.150.113:3774 -> 209.144.52.24:8888 SYN ******S*
Mar 20 16:23:51 MY.NET.150.113:3776 -> 62.163.4.241:8888 SYN ******S*
Mar 20 16:24:57 MY.NET.150.113:3788 -> 64.163.149.3:8888 SYN ******S*
Mar 20 16:24:58 MY.NET.150.113:3784 -> 62.211.22.123:8888 SYN ******S*
Mar 20 16:25:19 MY.NET.150.113:3841 -> 204.96.98.13:8888 SYN ******S*
Mar 20 16:25:47 MY.NET.150.113:3856 -> 217.39.139.173:8888 SYN ******S*
Mar 20 16:25:49 MY.NET.150.113:3860 -> 213.254.1.227:8888 SYN ******S*
Mar 20 16:25:50 MY.NET.150.113:3862 -> 67.81.94.246:8888 SYN ******S*
Mar 20 16:25:50 MY.NET.150.113:3864 -> 213.254.1.228:8888 SYN ******S*
Mar 20 16:25:51 MY.NET.150.113:3866 -> 172.173.56.80:8888 SYN ******S*
Mar 20 16:25:50 MY.NET.150.113:3858 -> 212.187.47.3:8888 SYN ******S*
Mar 20 16:25:52 MY.NET.150.113:3857 -> 63.149.6.91:8888 SYN ******S*
Mar 20 16:25:53 MY.NET.150.113:3856 -> 217.39.139.173:8888 SYN ******S*
Mar 20 16:25:58 MY.NET.150.113:3857 -> 63.149.6.91:8888 SYN ******S*
Mar 20 16:25:58 MY.NET.150.113:3859 -> 62.211.28.35:8888 SYN ******S*
Mar 20 16:26:07 MY.NET.150.113:3869 -> 216.175.64.208:8888 SYN ******S*
Mar 20 16:26:08 MY.NET.150.113:3867 -> 213.254.1.229:8888 SYN ******S*
Mar 20 16:26:21 MY.NET.150.113:3871 -> 24.42.82.21:8888 SYN ******S*
Mar 20 16:26:24 MY.NET.150.113:3872 -> 141.154.115.222:8888 SYN ******S*
Mar 20 16:26:22 MY.NET.150.113:3873 -> 213.254.1.230:8888 SYN ******S*
Mar 20 16:26:24 MY.NET.150.113:3870 -> 12.250.207.35:8888 SYN ******S*
Mar 20 16:26:24 MY.NET.150.113:3871 -> 24.42.82.21:8888 SYN ******S*
Mar 20 16:26:30 MY.NET.150.113:3871 -> 24.42.82.21:8888 SYN ******S*
Mar 20 16:26:30 MY.NET.150.113:3872 -> 141.154.115.222:8888 SYN ******S*
Mar 20 16:26:33 MY.NET.150.113:3875 -> 212.241.132.51:8888 SYN ******S*
Mar 20 16:26:34 MY.NET.150.113:3875 -> 212.241.132.51:8888 SYN ******S*
Mar 20 16:26:50 MY.NET.150.113:3876 -> 210.54.37.137:8888 SYN ******S*
Mar 20 16:26:49 MY.NET.150.113:3877 -> 62.64.223.135:8888 SYN ******S*
Mar 20 16:27:19 MY.NET.150.113:3966 -> 216.65.107.35:8888 SYN ******S*
Mar 20 16:27:20 MY.NET.150.113:3967 -> 64.71.163.205:8888 SYN ******S*
Mar 20 16:27:24 MY.NET.150.113:3974 -> 212.50.181.220:8888 SYN ******S*
Mar 20 16:27:25 MY.NET.150.113:3975 -> 212.50.169.126:8888 SYN ******S*
Mar 20 16:27:27 MY.NET.150.113:3973 -> 80.195.58.73:8888 SYN ******S*
Mar 20 16:27:28 MY.NET.150.113:3968 -> 134.87.210.254:8888 SYN ******S*
Mar 20 16:27:28 MY.NET.150.113:3966 -> 216.65.107.35:8888 SYN ******S*
Mar 20 16:27:33 MY.NET.150.113:3973 -> 80.195.58.73:8888 SYN ******S*
Mar 20 16:27:36 MY.NET.150.113:3976 -> 213.93.78.164:8888 SYN ******S*
Mar 20 16:27:52 MY.NET.150.113:3978 -> 4.61.189.132:8888 SYN ******S*
```

This host needs to be check out ASAP. This could indicate scanning for a Trojan or BOTs. In any case, the owner needs to be contacted and the host analyzed.

Scan # 3 Ports 8080, 8000, 3128

A total of 1080 hosts were scanned for ports 8080, 8000, and 3128 by 61.132.208.63.

```
Mar 21 05:51:17 61.132.208.63:1723 -> MY.NET.5.37:8080 SYN ******S*
Mar 21 05:51:17 61.132.208.63:1724 -> MY.NET.5.37:8000 SYN ******S*
Mar 21 05:51:17 61.132.208.63:1725 -> MY.NET.5.37:3128 SYN ******S*
Mar 21 05:51:16 61.132.208.63:1726 -> MY.NET.5.38:8080 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1863 -> MY.NET.5.83:8080 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1864 -> MY.NET.5.83:8000 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1865 -> MY.NET.5.83:3128 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1851 -> MY.NET.5.79:8080 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1852 -> MY.NET.5.79:8000 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1853 -> MY.NET.5.79:3128 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1873 -> MY.NET.5.85:8080 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1874 -> MY.NET.5.85:8000 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1875 -> MY.NET.5.85:3128 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1896 -> MY.NET.5.92:8080 SYN ******S*
Mar 21 05:51:20 61.132.208.63:1897 -> MY.NET.5.92:8000 SYN ******S*
Mar 21 05:51:21 61.132.208.63:1898 -> MY.NET.5.92:3128 SYN ******S*
…
Mar 21 06:39:26 61.132.208.63:1575 -> MY.NET.153.202:8000 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1597 -> MY.NET.153.209:3128 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1595 -> MY.NET.153.209:8080 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1596 -> MY.NET.153.209:8000 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1592 -> MY.NET.153.208:8080 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1593 -> MY.NET.153.208:8000 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1594 -> MY.NET.153.208:3128 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1570 -> MY.NET.153.200:3128 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1568 -> MY.NET.153.200:8080 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1569 -> MY.NET.153.200:8000 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1591 -> MY.NET.153.207:3128 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1589 -> MY.NET.153.207:8080 SYN ******S*
Mar 21 06:39:26 61.132.208.63:1590 -> MY.NET.153.207:8000 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1629 -> MY.NET.153.220:8080 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1631 -> MY.NET.153.220:3128 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1630 -> MY.NET.153.220:8000 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1626 -> MY.NET.153.219:8080 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1627 -> MY.NET.153.219:8000 SYN ******S*
Mar 21 06:39:27 61.132.208.63:1628 -> MY.NET.153.219:3128 SYN ******S*
```

Whois:

```
[whois.apnic.net]

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

inetnum:     61.132.128.0 - 61.132.255.255
netname:     CHINANET-AH
```

```
descr:      CHINANET Anhui province network
descr:      Data Communication Division
descr:      China Telecom
country:    CN
admin-c:    CH93-AP
tech-c:     JW89-AP
mnt-by:     MAINT-CHINANET
mnt-lower:  MAINT-CHINANET-AH
changed:    hostmaster@ns.chinanet.cn.net 20000701
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:     Jinneng Wang
address:    17/F, Postal Building No.120 Changjiang
address:    Middle Road, Hefei, Anhui, China
country:    CN
phone:      +86-551-2659073
fax-no:     +86-551-2659287
e-mail:     wang@mail.hf.ah.cninfo.net
nic-hdl:    JW89-AP
mnt-by:     MAINT-NEW
changed:    wang@mail.hf.ah.cninfo.net 19990818
source:     APNIC
```

Port 8080 and 3128 is associated with the RingZero Trojan, along with other Trojans. Recommend a network scan of these ports to determine if they are open and investigation on any hosts with these ports open.

OOS Scans:

While reviewing the OOS scan files, it appears the ftp scan from 64.152.183.174 was also logged and provides a means of correlation to the portscan files.

```
03/20-02:24:22.715554 64.152.183.174:21 -> MY.NET.5.25:21
03/20-02:24:22.946421 64.152.183.174:21 -> MY.NET.5.37:21
03/20-02:24:23.785978 64.152.183.174:21 -> MY.NET.5.79:21
```

```
03/20-02:24:23.882917 64.152.183.174:21 -> MY.NET.5.83:21
03/20-02:24:23.929229 64.152.183.174:21 -> MY.NET.5.85:21
03/20-02:24:23.954910 64.152.183.174:21 -> MY.NET.5.87:21
03/20-02:24:23.992367 64.152.183.174:21 -> MY.NET.5.90:21
03/20-02:24:24.023656 64.152.183.174:21 -> MY.NET.5.92:21
03/20-02:24:24.119744 64.152.183.174:21 -> MY.NET.5.95:21
…
```

Of the 348 packets logged, 316 were from the portscan from 64.152.183.174.

There were also packets from 213.107.228.218 to MY.NET.88.162. A Google search on port 21536 indicates that a corrupt Nortel network device removes the TCP header, but leaves the data. Quoting http://www.incidents.org/archives/intrusions/msg00156.html , "the first 4 bytes of the data portion in hex are 47 45 54 20 = "GET ". However, these 4 bytes are where the TCP source and destination port should be, so they get interpreted as tcp source port 4745 = 18245, dest port 5420= 21536.
My network logs show a client connecting to our website, sending a corrupt packet with the TCP header "missing", with "GET " 18245 > 21536. The next packet they send is a proper request "GET" directed at tcp port 80 of our web server. I'd expect you'd see something similar. "

Sample trace below:

```
03/21-18:11:11.788739 213.107.228.218:18245 -> MY.NET.88.162:21536
TCP TTL:109 TOS:0x0 ID:18424  DF
**SFR*AU Seq: 0x2F2E6861   Ack: 0x73683D33   Win: 0x3838
30 37 38 38 31 66 63 38 34 35 34 65 66 36 30 38  07881fc8454ef608
66 35 35 33 32 32                                f55322

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/21-18:12:33.309741 213.107.228.218:18245 -> MY.NET.88.162:21536
TCP TTL:109 TOS:0x0 ID:18611  DF
**SFR*AU Seq: 0x2F2E6861   Ack: 0x73683D33   Win: 0x3838
30 37 38 38 31 66 63 38 34 35 34 65 66 36 30 38  07881fc8454ef608
66 35 35 33 32 32                                f55322

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/21-18:14:19.480208 213.107.228.218:18245 -> MY.NET.88.162:21536
TCP TTL:109 TOS:0x0 ID:18952  DF
**SFR*AU Seq: 0x2F2E6861   Ack: 0x73683D33   Win: 0x3838
30 37 38 38 31 66 63 38 34 35 34 65 66 36 30 38  07881fc8454ef608
66 35 35 33 32 32                                f55322
```

The remainder of the traffic was GNUtella and Kazaa packets

Defensive Recommendations:

Many specific recommendations have been suggested in the body of this paper. Below are general recommendations for the State University Network.

- Install a firewall at the Border. Even though university networks are open, a firewall will greatly increase the security posture. There are many ports that can be blocked without adversely affecting the open network policy. Specifically Trojan ports, finger, echo, chargen, NETBIOS, etc, need to be blocked. Also, if there is a problem with a specific internal/external host, that IP can be blocked at the firewall.

- Designate “approved” DNS, Mail, public FTP servers. Have only approved servers for these services and allow traffic only to these designated IPs through the firewall.
- Perform regular port scans for open trojan ports, open FTP servers, mail relays, etc. Investigate hosts with vulnerable open ports and institute corrective action.
- Generate a list of Top Talkers and note anomalies. Consider limiting band for top talkers, especially those P2P hosts.
- Tweak snort rules to decrease amount of false positives. Write pass rules for trusted hosts that generate false positive alerts.
- Educate university community on best security practices. Because lack of IT resources, many users are left to secure their own systems. Security education in the form of a security Web Page, email alerts on current vulnerabilities, understanding basic system admin is critical. Get the word out on security to the masses.

Analysis Process:

All alert and scan files were merged into a single alert and single scan file.

Snortsnarf was used to process the alert files and generate a list of Top Talkers and segregate the snort alerts, by type.

Scan file was sorted by source and destination IP via sort, cut, and uniq commands. File then imported into Excel spreadsheet for further manipulation to find evidence of port scans and top scanning and scanned IPs.

Excel used to generate link graphs and general data manipulation.

References:

II. “Vulnerability Note VU#382365”. Doc. Rev. 38. 12 Dec. 2000.
URL: http://www.kb.cert.org/vuls/id/382365 (17 May 17, 2002).

III. Graham, Robert. “FAQ: Firewall Forensics (What am I seeing?)”.
URL: http://www.robertgraham.com/pubs/firewall-seen.html - netbios (17 May 2002).

Kipp, James. “Using Snort as an IDS and Network Monitor in Linux”. 13 June 2001.
URL:http://rr.sans.org/intrusion/monitor.php. (17 May 2002).

Brannan, Andrew. “Unicode Vulnerability – How & Why?” 7 August 2001.

URL: http://rr.sans.org/threats/unicode.php (17 May 2002).

Incidents.org. 14 June 2001.
URL: http://www.incidents.org/archives/intrusions/msg04079.html. (17 May 2002)

Fiddler, Matthew. GCIA Practical. URL:
http://www.giac.org/practical/Matthew_Fiddler_GCIA.doc . (17 May 2002)

Romanski, James. "Using DNMP for Reconnaissance". 12 August 2000.
URL: http://www.sans.org/newlook/resources/IDFAQ/SNMP.htm . (17 May 2002)

Whitehats.com. URL:
http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids311&view=event. (17 May 2002).

Whitehats.com. URL: http://www.whitehats.com/IDS/247 . (17 May 2002).

Chapman, Todd. GCIA Practical. URL:
www.giac.org/practical/Todd_Chapman_GCIA.doc. (17 May 2002)

Microsoft. "Firewalls and Ports Used by Windows Media Services (Q189416)".
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q189416. (17 May 2002).

Widom, Jeffrey. "Confidentiality: Can anyone read this message?" – GSEC Practical. 13 August 2001. URL:
http://www.giac.org/practical/jeffrey_widom_GSEC.doc. (17 May 2002).

CERT. "CERT® Advisory CA-2002-13 Buffer Overflow in Microsoft's MSN Chat ActiveX Control". 10 May 2002. URL: http://www.cert.org/advisories/CA-2002-13.html. (17 May 2002).

Lynes, Meredith. GSEC paper "Internet File Sharing", 19 June 2000. URL:
www.giac.org/practical/Meredith_Lynes_GSEC.doc . (17 May 2002).

Neohapsis.com. 20 November 2000. URL:
http://archives.neohapsis.com/archives/snort/2000-11/0244.html. (17 May 2002).

Insecure.org. "Top 50 Security Tools". 22 March 2002. URL:
http://www.insecure.org/tools.html. (17 May 2002).

Dell, Anthony. "Adore Worm – Another Mutation". 6 April 2001. URL:
http://rr.sans.org/threats/mutation.php. (17 May 2002).

Linux Magazine. "Distributed Filesystems for Linux", November 2000. URL:

http://www.linux-mag.com/2000-11/dfs_04.html. (17 May 2002).

IV. CERT. "CERT® Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPD". 15 Feburary 2002. URL: http://www.cert.org/advisories/CA-2001-33.html . (17 May 2002).

Schmaling, Robert. GCIA Practical. 3 October 2001. URL: http://www.giac.org/practical/Robert_Schmaling_GCIA.zip. (17 May 2002).

Incidents.org. 10 May 2001. URL: http://www.incidents.org/archives/intrusions/msg00156.html. (17 May 2002).