Global Information Assurance Certification Paper

GIAC INTRUSION DETECTION CURRICULUM
PRACTICAL ASSIGNMENT

David Whyte

Nov 22, 2000

Assignment 1 – Network Detects

1. Network Detects: Analysis #1

Event Traces

2000/03/14 11:27:21 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.10 16752 00080 www
2000/03/14 11:27:16 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.129 16752 00080 www
2000/03/14 11:27:15 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.165 16752 00080 www
2000/03/14 11:27:15 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.194 16752 00080 www
2000/03/14 11:27:14 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.197 16752 00080 www
2000/03/14 11:27:14 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.200 16752 00080 www
2000/03/14 11:27:14 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.201 16752 00080 www
2000/03/14 11:27:14 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.202 16752 00080 www
2000/03/14 11:27:21 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.2 16752 00080 www
2000/03/14 11:27:13 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.220 16752 00080 www
2000/03/14 11:27:21 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.3 16752 00080 www
2000/03/14 11:27:21 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.7 16752 00080 www
2000/03/14 11:27:21 OUT IN 3045 Queso-Sweep BAD_NET.228.10 MY.NET.196.8 16752 00080 www

Source of traces

The source of the trace is from a customer network.

Detect generated by

The trace was collected by Netranger IDS.

Probability that source address was spoofed

The probability that the address was spoofed is very low. Quesos is a network OS fingerprinting tool and in order for the reconnaissance to be successful the operator would have to receive the network traffic back so the tool could analyze the results. Attacker needs a response

Attack description

Quesos is a tool that can perform OS determination via the response(s) to various combinations of TCP flags sent by the tool. The attack was centered at discovering the particular OS of our web server.

Attack mechanism

The tool sends strange combinations of TCP flags to a host and based on the host response is able to tell with a high degree of accuracy what operating system (and patch # in some cases) it is using. The tool exploits the fact that the RFC for TCP/IP communication may beadhered too by the software developers of the OS stacks but there is still a lot of room for interpretation in the "gray areas". Since there are some flag combinations that are generated by the tool that were never even considered by the developers because they would not occur "naturally" different OSs will respond in different but predictable ways.

Correlation

CVE CAN-1999-0454

Evidence of active targeting

No evidence of active targeting, the scan was done for multiple hosts on the network.

Severity

Severity = (criticality + lethality) – (system countermeasures – network countermeasures)

criticality: 3 scan of a large portion of the entire network
lethality: 1 this type of scan is harmless
countermeasures: 0 systems will respond to most of the traffic if it reaches them thus giving up information
network countermeasures: 5 servers on the network (including web/ftp) are well hardened and have the latest patches and updated when new vulnerabilities arise. There are two types of network based IDS on the network and a host-based IDS on the web/ftp server

(3+1) – (0-5) = -1

Defensive recommendations

Minimal: scans are a fact of life on the Internet, an investigation of what traffic can be dropped at the router is in order (unsolicited ICMP, SYNFIN etc.,). The network itself is well protected and monitored.

Test question

Operating System fingerprinting is a technique by which:

A. sending different TCP flag combinations in packets will illicit observable and unique response(s) that can be attributed to specific operating systems
B. sending different TCP flag combinations in packets will cause response time delays that can be observed and attributed to specific operating systems
C. sending different TCP flag combinations in packets will cause specific packets sequence numbers that can be attributed to specific operating systems
D. sending different TCP flag combinations in packets will cause specific operating systems to crash

Answer: A

2. Network Detects: Analysis #2

Event Traces

2000/03/13 10:31:56 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 13322 00021 ftp
2000/03/13 10:34:34 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 13943 00021 ftp
2000/03/13 10:38:48 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 14524 00021 ftp
2000/03/13 10:40:59 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 15072 00021 ftp
2000/03/13 10:42:10 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 15600 00021 ftp
2000/03/13 10:45:25 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 16161 00021 ftp
2000/03/13 10:47:43 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 16620 00021 ftp
2000/03/13 10:49:53 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 17099 00021 ftp
2000/03/13 10:51:04 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 18589 00021 ftp
2000/03/13 10:56:15 OUT IN 3153 FTP_Improper_Address 199.203.140.6 MY.NET.196.1 18898 00021 ftp

Source of traces

The source of the trace came from a customers network.

Detect generated by

The detect was generated by a Netranger IDS.

Probability that source address was spoofed

The probability that the attack was spoofed is very low. The attack involves legitimately connecting to an ftp server and then trying to connect to other hosts using the ftp server's ip address.

Attack description

A Netranger IDS will trigger alarm 3153 (FTP_Improper_Address) when a port command is issued with an address that is not the same as the requesting host. An attacker tries to establish connections to arbitrary ports on hosts from the ftp server other than the originating client. The attack is called "FTP privileged port bounce".

Attack mechanism

The FTP priveldeged port bounce attack exploits the fact that the PORT command in an active FTP mode can, in some cases establish connections to arbitrary ports on machines other than the originating client. In a normal FTP session a connection is made to the ftp control port (21). Once the control port is established files are transferred using a separate connection which is considered the data connection. The data connection is accomplished by the FTP client sending a PORT command that specifies the ip address and port that it will listen for a TCP connection on. The FTP server then connects to the specified port and transfers the file.

The FTP bounce attack involves the FTP client specifying a different IP address other than its own, and if the FTP server is susceptible, it will make a connect to that IP address and send data to that host. Why? – Because the host that is unfortunate to have the "different ip" address will look like it is under attack by the FTP server. The FTP privileged port bounce attack involves using the legitimate IP of the FTP client but using a privileged port for connection back to the client. This may allow an attacker to attack their own machine via the FTP server.

Correlation

RFC (454)
CVE_1999_0017
CA-97.27.FTP_bounce
CIAC I-018A:FTP bounce vulnerability

Evidence of active targeting

This attack occurred only on the web/ftp server therefore my guess is that it is a targeted attack.

Severity

Severity = (criticality + lethality) – (system countermeasures – network countermeasures)

criticality: 3 if your system can be subverted in this attack your system could be a relay for an attacker
lethality: 2 although your system may only be used as a relay for an attack and dutifully forward traffic it may be subject to active IDS responses from sites your system is targeting. This may cause some instability or loss of service.
system countermeasures:4 the system is not vulnerable to this type of attack and is well patched and hardened.
network countermeasures: 5 servers on the network (including web/ftp) are well hardened and have the latest patches and updated when new vulnerabilities arise. There are two types of network based IDS on the network and a host-based IDS on the web/ftp server.

(3+2) – (4+5) = -4

Defensive recommendations

The use of the PORT command in an active FTP session is RFC compliant but does pose serious security concerns. The defenses are fine, the public web/ftp server has to allow connect to the public for file transfers and the IDS did log the attempts. The server is well patched and maintained and the system logs are looked at daily.

Test question

Why would an ftp bounce attack be useful to an attacker:

A. it would enable an attacker to access to files they do not have the privilege to download
B. it would enable an attacker to mask their ip address with that of an ftp server in attacks
C. it enables an attacker to gain root access to the ftp server
D. it enables an attacker to crash the ftp server

Answer: B

3. Network Detects: Analysis #3

Event Traces

2000-05-09 02:20:41 Duplicate IP address HOME.NET.COMP.7 Old+Ethernet=0800070FF8B2&New+Ethernet=0000947A1061|0800070FF8B2
2000-05-12 05:14:04 Duplicate IP address HOME.NET.COMP.7 Old+Ethernet=0800070FF8B2&New+Ethernet=0000947A1061|0800070FF8B2
2000-05-14 23:54:41 Duplicate IP address HOME.NET.COMP.7 Old+Ethernet=0800070FF8B2&New+Ethernet=0000947A1061|0800070FF8B2

Source of traces

The sources of the trace come from a home Internet account.

Detect generated by

The detect was generated by BlackICE Defender personal firewall.

Probability that source address was spoofed

The probability that it was spoofed is high due to the fact that the source and destination address is the same. HOWEVER, in the defensive recommendations section I believe I have a plausible explanation for this traffic and in fact the source address in the traces are not spoofed.**

Attack description

The Land attack is a denial of service attack. An attacker sends crafted packets that have the SYN flag set and the source address and port are the same as the destination port and address. If a host receives these crafted packets and its particular TCP/IP stack is vulnerable it will cause the machine to crash (blue screen or kernel panic) or hang.

Attack mechanism

The attack exploits a vulnerability in the TCP/IP protocol stacks in some software. A Land attack exploits the fact that a system can be tricked into responding to responding to itself multiple times thus exhausting critical resources and causing the system to crash. If a system is vulnerable (an older OS or unpatched system), an attacker uses a tool (there are several) to craft packets packets that have the SYN flag set and the source address and port are the same as the destination port and address – this will cause the system to crash.

Correlation

CERT:CA-97.28.Teardrop_Land
FreeBSD: SA-98:01
CVE-1999-0016
Xforce:land

Evidence of active targeting

In a Land attack the probability of active targeting is high as it involves crafting packets using the specific ip address of the victim machine.

Severity

Severity = (criticality + lethality) – (system countermeasures – network countermeasures)

criticality: 3 if your system is susceptible to the attack it will crash causing a denial of service – the machine has been targeted
lethality: 3 it is a denial of service attack and will crash the machine, it does not open up the system for unauthorized access.
system countermeasures:4 the system is not vulnerable to this type of attack and is well patched and hardened.
network countermeasures: 4 servers on the network (including web/ftp) are well hardened and have the latest patches and updated when new vulnerabilities arise. There are two types of network based IDS on the network.

(3+3) – (4+4) = -2

Defensive recommendations

Perform egress filtering on your network to stop insiders from spoofing ip addresses thus stopping the land attack. (http://www.sans.org/y2k/egress.htm)

Make sure your systems have the latest patches and your network does not support spoofed packets. I believe, however, it could be a false positive and not evidence of a Land attack. I have had a cable account for some time and the machine runs 24/7 thus it does not release its ip address. It could be a misconfiguration of the DCHP server on Rogers network trying to give out my ip address to another host. Their infrastructure is stretched to the limit with new users and experiences frequent downtime. ☹

Test question

A Land attack occurs when:
A: overlapping packets are sent to a machine causing it to crash
B: fragmented packets are sent to a machine causing it to crash
C: packets with the SYN flag set and the source address and port are the same as the destination port and address are sent to a machine causing it to crash
D: packets with a ttl field of 0 and the same sequence numbers are sent to a machine causing it to crash

Answer: C

4. Network Detects: Analysis #4

Event Traces

2000-10-19 03:39:24 PCAnywhere ping My.HOME.COMP..39 cr806690b.flfrd1.on.wave.home.com port=5632

Source of traces

The sources of the trace come from a home Internet account.

Detect generated by

The detect was generated by BlackICE Defender personal firewall.

Probability that source address was spoofed

The probability that the source address was spoofed is low as this is active reconnaissance to determine if a particular program is running, thus a response is needed.

Attack description

Someone has pinged the system in order to verify if PCAnywhere is currently running on the system.

Attack mechanism

PCAnywhere (Symantec) is a product, which allows for the remote control of a computer. It is a legitimate product, and is used my many system administrators to remotely access their servers. It is also this remote control capability which attracts hackers to it. Once a hacker has located a machine running PCAnywhere, he can crack the password, which is often easy to guess. At this stage the hacker has control of the machine and can not only remove information from the machine, but use it to attack others.

Correlation

CVE-2000-0273
CAN-2000-0300
CAN-2000-0324

Evidence of active targeting

Probably low since no other activity to the ip address was seen by the ip address, it was probably just a reconnaissance attempt and part of a large scale scan.

Severity

Severity = (criticality + lethality) – (system countermeasures – network countermeasures)

criticality: 2 just a scan, no other evidence of targeting
lethality: 1just a scan
system countermeasures: 5 PcAnywhere is not running on the box
network countermeasures: 4 running a personal firewall
(2+1) – (5+4) = -6

Defensive recommendations

If you are using PcAnywhere make sure your passwords are hard to guess.

Test question

It is important for users that use remote access software to:

A: log in frequently so that the remote systems audit files keep an accurate record of where they are
B: make sure to synchronize time manually with the remote server
C: ensure that their passwords are considered strong (i.e. hard to guess or brute force)
D: log out immediately after their session is completed

Answer: C

5. Network Detects: Analysis #5

Event Traces

FWIN,2000/10/11,22:13:06 -5:00 GMT,208.49.12.88:80,MY.HOME.COMP.5:23476,TCP

Source of traces

The sources of the trace come from a home Internet account.

Detect generated by

The detect was generated by a ZoneAlarm personal firewall.

Probability that source address was spoofed

The probability that the source address was spoofed is low as this is active reconnaissance to determine if a particular program is running, thus a response is needed.

Attack description

The attack is a reconnaissance to determine if the machine has been infected with the Donald Dick trojan. The trojan was created in Russia and it enables a remote malicious attacker to have control of your machine.

Attack mechanism

Malicious individuals can scan hundreds/thousands of machines for specific ports that trojan horses are listening on. If a user launches an executable from an email or runs a program they downloaded from the Internet and the site is untrusted they could be infecting themselves with a trojan horse.

Correlation

www.sans.org

Evidence of active targeting

No evidence of active targeting, the scan was probably done for multiple hosts on the Rogers network. No additional traffic was seen from that host in the logs.

Severity

Severity = (criticality + lethality) – (system countermeasures – network countermeasures)

criticality: 2 just a scan, no other evidence of targeting
lethality: 1just a scan
system countermeasures: 4 latest virus scanner with updated .dat files
network countermeasures: 4 running a personal firewall

(2+1) – (4+4) = -5

Defensive recommendations

Install latest virus scanner .dat (this means you need a virus scanner) do not launch any programs or email attachments from untrusted sites.

Test question

If you computer is scanned for a trojan horse it means:
A: you are definitely infected with a trojan horse
B: someone is searching for trojaned computers
C: your machine is probably vulnerable to trojan horses
D: get ready an attack is likely

Answer: B

Assignment – 2 Evaluate an attack

1. Attack tool Identification

Plague v1.0 is a distributed denial of service (DDoS) tool. There are a number of DDoS tools available in the wild today such as:
Trinoo TFN, TFN2K, stacheldraht, Plague, Omega, Trinity, and many more. The tool was downloaded from : http://packetstorm.securify.com/distributed/

2. Description of attack

Plague is a DDoS tool. DDoS tools coordinate several or several hundreds of computers in attacks against its victim(s). The overall goal of the attack is to overwhelm the victim with network traffic (e.g. SYN flood, mstream, etc.,) or strange packets (e.g. targa attack) so the machine will crash or hang. If the attack is large enough it may even overwhelm the network infrastructure the victim resides on (i.e. routers).

The DDoS tools rely on the use of compromised machines owned by unsuspecting users to do the attacking. Typically, a user does not know that their machine has been compromised and is participating in an attack, they simply type away at their email all the while their machine is participating as part of a digital army.

Possible scenario:
A new exploit is discovered and a malicious individual scans the Internet for vulnerable hosts. Once the hosts are identified the malicious actor uses the exploit and compromises machines. The malicious individual then installs the DDoS software on the computers and probably rootkits the machines. A rootkit is used to hide software on the computer from the legitimate user. For instance, the "ls" command is replaced by the malicious individual version of "ls" command which will not show the tools (other commands are typically included in rootkits). Then the malicious individual may even patch the machine to make it not vulnerable to the exploit so that they are the only ones that can exploit the machine. (pride in ownership☺)

Once the DDoS software is installed the compromised machine, in the case of plague, is called a "ghost". The ghost lies dormant waiting for commands from a master (the attacker's machine) on the type of attack and the victim's address.

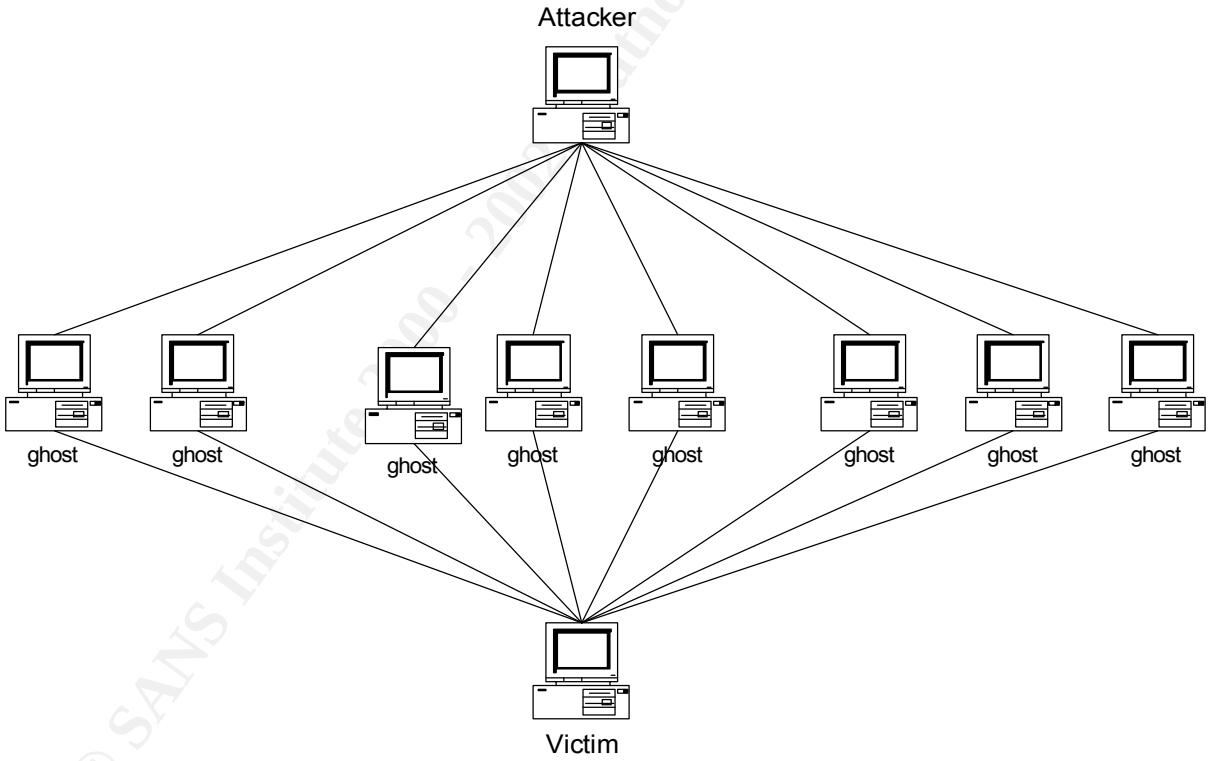
Unless there is some logging done on the network that the masters/ghosts are running on the owners are probably unaware that there machines are being used in a distributed denial of service attack. Even viewing network connections to see if you have any strange processes listening on ports may not be enough – rootkits.

Plague functionality (actual screen shot “help” prints it out”):

plague> help

quit	-	Closes your connection:	*exits the tool*
help	-	Prints out this shit:	*help file (what this is)*
stream	-	<port> <ip of target> <time>:	*will start a stream attack on a specified machine for a specified time*
syn	-	<port> <ip of target> <time>:	*will start a SYN flood on a specified machine for a specified time*
bindshell	-	<ip of miniserver> <port>:	*can bind a root shell to a remote machine on a specified port*
pingall	-	Checks if ghosts are up:	*will ping all hosts in the configuration file server.list*

Plague Architecture



3. Network trace of attack

Snort was used to do the network trace of the attack. Some snippets of the actual entire trace were deleted because of repetition, interesting traces were kept for explanation purposes. Some portions of the packet captures are also bolded to draw attention to them.

Test architecture consists of a master 192.168.1.30, three “ghosts” 192.168.1.10, 192.168.1.40, and 192.168.1.50, and the victim 192.168.1.1.

An actual screen shot of the command line to initiate plague. The “ghosts” that are used by the master are specified in a configuration file called server.list.

The program uses Netcat for its server/client communications. (Netcat can be found at www.l0pht.com) The default login string is ld.so.1 and can be changed during the install of the program.

```
[root@Hood plague]# ./nc 192.168.1.30 3333


Plague by datawar/blazinweed u r 0wn3d

Login: ld.so.1

Excellent!

Try typing help for command list
Idle connection time set correct.
```

Using the pingall command to see what hosts are active:
The pingall command,

```
plague> pingall
192.168.1.10    UP
192.168.1.40    UP
192.168.1.50    UP

Associated network traffic with pingall:

Initializing Network Interface...
snaplen = 1500
Entering readback mode....
Initializing Preprocessors!
Initializing Plug-ins!
Initializating Output Plugins!

++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
```

```
855 Snort rules read...
855 Option Chains linked into 120 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

-*> Snort! <*-
Version 1.6.3-patch2
By Martin Roesch (roesch@clark.net, www.snort.org)
11/17-15:36:43.405414 192.168.1.30:1098 -> 192.168.1.10:6969
TCP TTL:64 TOS:0x0 ID:1029  DF
******S* Seq: 0xA602CD6C   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 43332130 0 NOP WS: 0
0x0000: 00 50 DA CA 44 F0 00 01 02 37 C8 2E 08 00 45 00  .P..D....7....E.
0x0010: 00 3C 04 05 40 00 40 06 B3 3E C0 A8 01 1E C0 A8  .<..@.@..>......
0x0020: 01 0A 04 4A 1B 39 A6 02 CD 6C 00 00 00 00 A0 02  ...J.9...l......
0x0030: 7D 78 7F 6C 00 00 02 04 05 B4 04 02 08 0A 02 95  }x.l............
0x0040: 32 22 00 00 00 00 01 03 03 00                    2".........

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

11/17-15:36:44.411408 192.168.1.30:1098 -> 192.168.1.10:6969
TCP TTL:64 TOS:0x0 ID:1032  DF
***AP*** Seq: 0xA602CD6D   Ack: 0xA5494369   Win: 0x7D78
TCP Options => NOP NOP TS: 43332231 17092837

0x0000: 00 50 DA CA 44 F0 00 01 02 37 C8 2E 08 00 45 00  .P..D....7....E.
0x0010: 00 43 04 08 40 00 40 06 B3 34 C0 A8 01 1E C0 A8  .C..@.@..4......
0x0020: 01 0A 04 4A 1B 39 A6 02 CD 6D A5 49 43 69 80 18  ...J.9...m.ICi..
0x0030: 7D 78 E3 81 00 00 01 01 08 0A 02 95 32 87 01 04  }x..........2...
0x0040: D0 E5 44 20 6C 64 2E 73 6F 2E 31 20 30 20 30 20  ..D ld.so.1 0 0
0x0050: 30                                               0

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

192.168.1.30 is the master talking to one of the ghosts 192.168.10 – passing the default login string ld.so.1

```
11/17-15:36:44.411528 192.168.1.10:6969 -> 192.168.1.30:1098
TCP TTL:64 TOS:0x0 ID:100  DF
***A**** Seq: 0xA5494369   Ack: 0xA602CD7C   Win: 0x7D78
TCP Options => NOP NOP TS: 17092938 43332231
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 44 F0 08 00 45 00  ...7...P..D...E.
0x0010: 00 34 00 64 40 00 40 06 B6 E7 C0 A8 01 0A C0 A8  .4.d@.@.........
0x0020: 01 1E 1B 39 04 4A A5 49 43 69 A6 02 CD 7C 80 10  ...9.J.ICi...|..
0x0030: 7D 78 F2 AB 00 00 01 01 08 0A 01 04 D1 4A 02 95  }x...........J..
```

```
0x0040: 32 87                                           2.

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

11/17-15:36:44.411720 192.168.1.10:6969 -> 192.168.1.30:1098
TCP TTL:64 TOS:0x0 ID:101  DF
***AP*** Seq: 0xA5494369   Ack: 0xA602CD7C   Win: 0x7D78
TCP Options => NOP NOP TS: 17092938 43332231
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 44 F0 08 00 45 00  ...7...P..D...E.
0x0010: 00 39 00 65 40 00 40 06 B6 E1 C0 A8 01 0A C0 A8  .9.e@.@.........
0x0020: 01 1E 1B 39 04 4A A5 49 43 69 A6 02 CD 7C 80 18  ...9.J.ICi...|..
0x0030: 7D 78 54 08 00 00 01 01 08 0A 01 04 D1 4A 02 95  }xT..........J..
0x0040: 32 87 50 4F 4E 47 00                             2.PONG.
```

192.168.1.10 is up and ready for action

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

11/17-15:36:44.412300 192.168.1.30:1099 -> 192.168.1.40:6969
TCP TTL:64 TOS:0x0 ID:1036  DF
******S* Seq: 0xA6367377   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 43332231 0 NOP WS: 0
0x0000: 00 50 DA CA 4C 71 00 01 02 37 C8 2E 08 00 45 00  .P..Lq...7....E.
0x0010: 00 3C 04 0C 40 00 40 06 B3 19 C0 A8 01 1E C0 A8  .<..@.@.........
0x0020: 01 28 04 4B 1B 39 A6 36 73 77 00 00 00 00 A0 02  .(.K.9.6sw......
0x0030: 7D 78 D8 A9 00 00 02 04 05 B4 04 02 08 0A 02 95  }x..............
0x0040: 32 87 00 00 00 00 01 03 03 00                    2.........


11/17-15:36:45.421402 192.168.1.30:1099 -> 192.168.1.40:6969
TCP TTL:64 TOS:0x0 ID:1041  DF
***AP*** Seq: 0xA6367378   Ack: 0xA4A50C26   Win: 0x7D78
TCP Options => NOP NOP TS: 43332332 53856238
0x0000: 00 50 DA CA 4C 71 00 01 02 37 C8 2E 08 00 45 00  .P..Lq...7....E.
0x0010: 00 43 04 11 40 00 40 06 B3 0D C0 A8 01 1E C0 A8  .C..@.@.........
0x0020: 01 28 04 4B 1B 39 A6 36 73 78 A4 A5 0C 26 80 18  .(.K.9.6sx...&..
0x0030: 7D 78 7B 6C 00 00 01 01 08 0A 02 95 32 EC 03 35  }x{l........2..5
0x0040: C7 EE 44 20 6C 64 2E 73 6F 2E 31 20 30 20 30 20  ..D ld.so.1 0 0
0x0050: 30                                               0
```

192.168.1.30 is the master talking to one of the ghosts 192.168.40 – passing the default login string ld.so.1

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

11/17-15:36:45.421472 192.168.1.40:6969 -> 192.168.1.30:1099
TCP TTL:64 TOS:0x0 ID:1979  DF
***A**** Seq: 0xA4A50C26   Ack: 0xA6367387   Win: 0x7D78
TCP Options => NOP NOP TS: 53856338 43332332
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 4C 71 08 00 45 00  ...7...P..Lq..E.
0x0010: 00 34 07 BB 40 00 40 06 AF 72 C0 A8 01 28 C0 A8  .4..@.@..r...(..
0x0020: 01 1E 1B 39 04 4B A4 A5 0C 26 A6 36 73 87 80 10  ...9.K...&.6s...
0x0030: 7D 78 8A 97 00 00 01 01 08 0A 03 35 C8 52 02 95  }x.........5.R..
0x0040: 32 EC                                            2.

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

11/17-15:36:45.421895 192.168.1.40:6969 -> 192.168.1.30:1099
TCP TTL:64 TOS:0x0 ID:1980  DF
***AP*** Seq: 0xA4A50C26   Ack: 0xA6367387   Win: 0x7D78
TCP Options => NOP NOP TS: 53856338 43332332
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 4C 71 08 00 45 00  ...7...P..Lq..E.
0x0010: 00 39 07 BC 40 00 40 06 AF 6C C0 A8 01 28 C0 A8  .9..@.@..l...(..
0x0020: 01 1E 1B 39 04 4B A4 A5 0C 26 A6 36 73 87 80 18  ...9.K...&.6s...
0x0030: 7D 78 EB F3 00 00 01 01 08 0A 03 35 C8 52 02 95  }x.........5.R..
0x0040: 32 EC 50 4F 4E 47 00                             2.PONG.
```

192.168.1.40 is up and ready for action

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


11/17-15:36:45.422299 192.168.1.30:1100 -> 192.168.1.50:6969
TCP TTL:64 TOS:0x0 ID:1044  DF
******S* Seq: 0xA60D097D   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 43332332 0 NOP WS: 0
0x0000: 00 50 DA CA 52 06 00 01 02 37 C8 2E 08 00 45 00  .P..R....7....E.
0x0010: 00 3C 04 14 40 00 40 06 B3 07 C0 A8 01 1E C0 A8  .<..@.@.........
0x0020: 01 32 04 4C 1B 39 A6 0D 09 7D 00 00 00 00 A0 02  .2.L.9...}......
0x0030: 7D 78 42 5D 00 00 02 04 05 B4 04 02 08 0A 02 95  }xB]............
0x0040: 32 EC 00 00 00 00 01 03 03 00                    2.........

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

11/17-15:36:45.422369 192.168.1.30:1099 -> 192.168.1.40:6969
TCP TTL:64 TOS:0x0 ID:1045  DF
***A**** Seq: 0xA6367387   Ack: 0xA4A50C2C   Win: 0x7D78
TCP Options => NOP NOP TS: 43332332 53856338
0x0000: 00 50 DA CA 4C 71 00 01 02 37 C8 2E 08 00 45 00  .P..Lq...7....E.
```

```
0x0010: 00 34 04 15 40 00 40 06 B3 18 C0 A8 01 1E C0 A8  .4..@.@.........
0x0020: 01 28 04 4B 1B 39 A6 36 73 87 A4 A5 0C 2C 80 10  .(.K.9.6s....,..
0x0030: 7D 78 8A 91 00 00 01 01 08 0A 02 95 32 EC 03 35  }x..........2..5
0x0040: C8 52                                            .R

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

11/17-15:36:46.431401 192.168.1.30:1100 -> 192.168.1.50:6969
TCP TTL:64 TOS:0x0 ID:1050  DF
***AP*** Seq: 0xA60D097E   Ack: 0xA5985674   Win: 0x7D78
TCP Options => NOP NOP TS: 43332433 53751283
0x0000: 00 50 DA CA 52 06 00 01 02 37 C8 2E 08 00 45 00  .P..R....7....E.
0x0010: 00 43 04 1A 40 00 40 06 B2 FA C0 A8 01 1E C0 A8  .C..@.@.........
0x0020: 01 32 04 4C 1B 39 A6 0D 09 7E A5 98 56 74 80 18  .2.L.9...~..Vt..
0x0030: 7D 78 33 DB 00 00 01 01 08 0A 02 95 33 51 03 34  }x3.........3Q.4
0x0040: 2D F3 44 20 6C 64 2E 73 6F 2E 31 20 30 20 30 20  -.D ld.so.1 0 0
0x0050: 30                                               0
```

192.168.1.30 is the master talking to one of the ghosts 192.168.50 – passing the default login string ld.so.1

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

11/17-15:36:46.431539 192.168.1.50:6969 -> 192.168.1.30:1100
TCP TTL:64 TOS:0x0 ID:636  DF
***A**** Seq: 0xA5985674   Ack: 0xA60D098D   Win: 0x7D78
TCP Options => NOP NOP TS: 53751384 43332433
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 52 06 08 00 45 00  ...7...P..R...E.
0x0010: 00 34 02 7C 40 00 40 06 B4 A7 C0 A8 01 32 C0 A8  .4.|@.@......2..
0x0020: 01 1E 1B 39 04 4C A5 98 56 74 A6 0D 09 8D 80 10  ...9.L..Vt......
0x0030: 7D 78 43 05 00 00 01 01 08 0A 03 34 2E 58 02 95  }xC........4.X..
0x0040: 33 51                                            3Q

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

11/17-15:36:46.431834 192.168.1.50:6969 -> 192.168.1.30:1100
TCP TTL:64 TOS:0x0 ID:637  DF
***AP*** Seq: 0xA5985674   Ack: 0xA60D098D   Win: 0x7D78
TCP Options => NOP NOP TS: 53751384 43332433
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 52 06 08 00 45 00  ...7...P..R...E.
0x0010: 00 39 02 7D 40 00 40 06 B4 A1 C0 A8 01 32 C0 A8  .9.}@.@......2..
0x0020: 01 1E 1B 39 04 4C A5 98 56 74 A6 0D 09 8D 80 18  ...9.L..Vt......
0x0030: 7D 78 A4 61 00 00 01 01 08 0A 03 34 2E 58 02 95  }x.a.......4.X..
0x0040: 33 51 50 4F 4E 47 00                             3QPONG.
```

192.168.1.50 is up and ready for action

The help menu (actual screen shot):

```
plague> help

quit            -       Closes your connection
help            -       Prints out this shit
stream          -       <port> <ip of target> <time>
syn             -       <port> <ip of target> <time>
bindshell       -       <ip of miniserver> <port>
pingall         -       Checks if ghosts are up
```

I am instructing the master to send a syn flood attack to the victim 192.168.1.1 for 2 seconds.

```
plague> syn 2525 192.168.1.1 2
```

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

11/17-15:37:50.910902 192.168.1.30:1103 -> 192.168.1.10:6969
TCP TTL:64 TOS:0x0 ID:1089  DF
***AP*** Seq: 0xAA2A23AF   Ack: 0xA8A3DCF6   Win: 0x7D78
TCP Options => NOP NOP TS: 43338881 17099487
0x0000: 00 50 DA CA 44 F0 00 01 02 37 C8 2E 08 00 45 00  .P..D....7....E.
0x0010: 00 50 04 41 40 00 40 06 B2 EE C0 A8 01 1E C0 A8  .P.A@.@.........
0x0020: 01 0A 04 4F 1B 39 AA 2A 23 AF A8 A3 DC F6 80 18  ...O.9.*#.......
0x0030: 7D 78 AB 9F 00 00 01 01 08 0A 02 95 4C 81 01 04  }x..........L...
0x0040: EA DF 42 20 6C 64 2E 73 6F 2E 31 20 32 35 32 35  ..B ld.so.1 2525
0x0050: 20 31 39 32 2E 31 36 38 2E 31 2E 31 20 32         192.168.1.1 2
```

default login is sent to ghost .10 with the port number (2525)

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

11/17-15:37:50.911017 192.168.1.10:6969 -> 192.168.1.30:1103
TCP TTL:64 TOS:0x0 ID:118  DF
***A**** Seq: 0xA8A3DCF6   Ack: 0xAA2A23CB   Win: 0x7D78
TCP Options => NOP NOP TS: 17099588 43338881
```

```
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 44 F0 08 00 45 00  ...7...P..D...E.
0x0010: 00 34 00 76 40 00 40 06 B6 D5 C0 A8 01 0A C0 A8  .4.v@.@.........
0x0020: 01 1E 1B 39 04 4F A8 A3 DC F6 AA 2A 23 CB 80 10  ...9.O.....*#...
0x0030: 7D 78 C7 54 00 00 01 01 08 0A 01 04 EB 44 02 95  }x.T.........D..
0x0040: 4C 81                                            L.

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

11/17-15:37:50.911316 192.168.1.10:6969 -> 192.168.1.30:1103
TCP TTL:64 TOS:0x0 ID:119  DF
***AP*** Seq: 0xA8A3DCF6   Ack: 0xAA2A23CB   Win: 0x7D78
TCP Options => NOP NOP TS: 17099588 43338881
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 44 F0 08 00 45 00  ...7...P..D...E.
0x0010: 00 47 00 77 40 00 40 06 B6 C1 C0 A8 01 0A C0 A8  .G.w@.@.........
0x0020: 01 1E 1B 39 04 4F A8 A3 DC F6 AA 2A 23 CB 80 18  ...9.O.....*#...
0x0030: 7D 78 B0 16 00 00 01 01 08 0A 01 04 EB 44 02 95  }x...........D..
0x0040: 4C 81 07 0A 66 6C 6F 6F 64 69 6E 67 20 74 61 72  L...flooding tar
0x0050: 67 65 74 20 0A                                   get .
```

.10 will now start flooding the target .1 with a syn flood coming from spoofed ip addresses

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

11/17-15:37:50.911432 192.168.1.30:1103 -> 192.168.1.10:6969
TCP TTL:64 TOS:0x0 ID:1090  DF
***A**** Seq: 0xAA2A23CB   Ack: 0xA8A3DD09   Win: 0x7D78
TCP Options => NOP NOP TS: 43338881 17099588
0x0000: 00 50 DA CA 44 F0 00 01 02 37 C8 2E 08 00 45 00  .P..D....7....E.
0x0010: 00 34 04 42 40 00 40 06 B3 09 C0 A8 01 1E C0 A8  .4.B@.@.........
0x0020: 01 0A 04 4F 1B 39 AA 2A 23 CB A8 A3 DD 09 80 10  ...O.9.*#.......
0x0030: 7D 78 C7 41 00 00 01 01 08 0A 02 95 4C 81 01 04  }x.A........L...
0x0040: EB 44                                            .D

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

11/17-15:37:50.911570 192.168.1.30:1104 -> 192.168.1.40:6969
TCP TTL:64 TOS:0x0 ID:1091  DF
******S* Seq: 0xAA37FF42   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 43338881 0 NOP WS: 0
0x0000: 00 50 DA CA 4C 71 00 01 02 37 C8 2E 08 00 45 00  .P..Lq...7....E.
0x0010: 00 3C 04 43 40 00 40 06 B2 E2 C0 A8 01 1E C0 A8  .<.C@.@.........
0x0020: 01 28 04 50 1B 39 AA 37 FF 42 00 00 00 00 A0 02  .(.P.9.7.B......
0x0030: 7D 78 2E DE 00 00 02 04 05 B4 04 02 08 0A 02 95  }x..............
0x0040: 4C 81 00 00 00 00 01 03 03 00                    L.........

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

```
11/17-15:37:50.911641 192.168.1.40:6969 -> 192.168.1.30:1104
TCP TTL:64 TOS:0x0 ID:1982  DF
***A**S* Seq: 0xA8663D12   Ack: 0xAA37FF43   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 53862887 43338881 NOP WS: 0
0x0000: 00 01 02 37 C8 2E 00 50 DA CA 4C 71 08 00 45 00  ...7...P..Lq..E.
0x0010: 00 3C 07 BE 40 00 40 06 AF 67 C0 A8 01 28 C0 A8  .<..@.@..g...(..
0x0020: 01 1E 1B 39 04 50 A8 66 3D 12 AA 37 FF 43 A0 12  ...9.P.f=..7.C..
0x0030: 7D 78 64 37 00 00 02 04 05 B4 04 02 08 0A 03 35  }xd7...........5
0x0040: E1 E7 02 95 4C 81 01 03 03 00                    ....L.....
```

.40 joins in on the attack talking to the master .30

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

11/17-15:37:50.911897 192.168.1.30:1104 -> 192.168.1.40:6969
TCP TTL:64 TOS:0x0 ID:1092  DF
***A**** Seq: 0xAA37FF43   Ack: 0xA8663D13   Win: 0x7D78
TCP Options => NOP NOP TS: 43338881 53862887
0x0000: 00 50 DA CA 4C 71 00 01 02 37 C8 2E 08 00 45 00  .P..Lq...7....E.
0x0010: 00 34 04 44 40 00 40 06 B2 E9 C0 A8 01 1E C0 A8  .4.D@.@.........
0x0020: 01 28 04 50 1B 39 AA 37 FF 43 A8 66 3D 13 80 10  .(.P.9.7.C.f=...
0x0030: 7D 78 92 FC 00 00 01 01 08 0A 02 95 4C 81 03 35  }x..........L..5
0x0040: E1 E7                                            ..

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

the flooding of .1 begins – spoofed addresses

```
11/17-15:37:50.918298 57.106.228.45:0 -> 192.168.1.1:0
TCP TTL:40 TOS:0x0 ID:2450
0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 09 92 00 00 28 06 A9 FD 39 6A E4 2D C0 A8  .(....(...9j.-..
0x0020: 01 01 B4 9D 00 01 B5 D1 C7 63 20 5C 06 6D 00 02  .........c \.m..
0x0030: FF FF 12 11 00 00 00 00 00 00 00 00              ............

0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 09 92 00 00 28 06 A9 FD 39 6A E4 2D C0 A8  .(....(...9j.-..
0x0020: 01 01 B4 9D 00 01 B5 D1 C7 63 20 5C 06 6D 00 02  .........c \.m..
0x0030: FF FF 12 11 00 00 00 00 00 00 00 00              ............

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

11/17-15:37:50.928293 17.134.247.16:0 -> 192.168.1.1:0
TCP TTL:40 TOS:0x0 ID:21229
0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 52 ED 00 00 28 06 75 A3 11 86 F7 10 C0 A8  .(R...(.u.......
```

```
0x0020: 01 01 A4 5F 00 02 4F 21 84 7C 0C C6 17 1A 00 02  ..._..O!.|......
0x0030: FF FF 52 0D 00 00 00 00 00 00 00 00              ..R.........

0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 52 ED 00 00 28 06 75 A3 11 86 F7 10 C0 A8  .(R...(.u.......
0x0020: 01 01 A4 5F 00 02 4F 21 84 7C 0C C6 17 1A 00 02  ..._..O!.|......
0x0030: FF FF 52 0D 00 00 00 00 00 00 00 00              ..R.........


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

11/17-15:37:50.968292 179.18.105.14:0 -> 192.168.1.1:0
TCP TTL:40 TOS:0x0 ID:35313
0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 89 F1 00 00 28 06 2B 15 B3 12 69 0E C0 A8  .(....(.+...i...
0x0020: 01 01 E6 0A 00 06 B7 BB 15 45 69 0B AE 7A 00 02  .........Ei..z..
0x0030: FF FF 78 7D 00 00 00 00 00 00 00 00              ..x}........

0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 89 F1 00 00 28 06 2B 15 B3 12 69 0E C0 A8  .(....(.+...i...
0x0020: 01 01 E6 0A 00 06 B7 BB 15 45 69 0B AE 7A 00 02  .........Ei..z..
0x0030: FF FF 78 7D 00 00 00 00 00 00 00 00              ..x}........

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

11/17-15:37:50.978293 43.89.68.2:0 -> 192.168.1.1:0
TCP TTL:40 TOS:0x0 ID:61733
0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 F1 25 00 00 28 06 70 A6 2B 59 44 02 C0 A8  .(.%..(.p.+YD...
0x0020: 01 01 73 9D 00 07 DF F6 FB 23 A6 F7 C1 56 00 02  ..s......#...V..
0x0030: FF FF D0 72 00 00 00 00 00 00 00 00              ...r........

0x0000: 00 50 DA CA 55 83 00 50 DA CA 44 F0 08 00 45 00  .P..U..P..D...E.
0x0010: 00 28 F1 25 00 00 28 06 70 A6 2B 59 44 02 C0 A8  .(.%..(.p.+YD...
0x0020: 01 01 73 9D 00 07 DF F6 FB 23 A6 F7 C1 56 00 02  ..s......#...V..
0x0030: FF FF D0 72 00 00 00 00 00 00 00 00              ...r........
```

Exiting the program:

```
plague> quit
bye!
```

Defensive Recommendations

Consult the references below. Make sure your machines are hardened and have the latest patches applied. Invest in a personal firewall and a goodvirus scanner this will help prevent your machine being compromised and added to a digital army. If egress and ingress filtering is done by routers this would help eliminate spoofing of ip addresses and contribute greatly to stooping these attacks.

References

1. Resisting the Effects of Distributed Denial of Service Attacks**,** Version 1.10, http://www.sans.org/y2k/resist.htm
2. Help Defeat Denial of Service Attacks: Step-by-Step , Revision: 1.41, http://www.sans.org/dosstep/index.htm
3. Dave Dittrich's homepage, on DdoS, http://www.washington.edu/People/dad/

Assignment #3 "Analyze This"

The following table is data collected from the available logs for the network. The information was incomplete and we had no information about the topology of the network. Analysis was a daunting task. The table below is the raw data used to make the 4 charts which immediately follow. The data sets and associated charts are:

1. Chart 1: top 11 source addresses for number of scans
2. Chart 2: top 11 destination addresses for number of scans
3. Chart 3: top 11 destination addresses for number of alerts
4. Chart 4: top 11 source addresses for number of alerts

This data was the starting part of the analysis, please refer to Assignment #4 of this practical for a rationale.

Chart #1 data		**Chart #2 data**		**Chart #3 data**		**Chart #4 data**	
Ip address	# of scans	Ip Address	# of scans	Ip address	# of alarms	Ip address	# of alerts
195.114.226.41	42652	MY.NET.97.199	27513	MY.NET.253.43	5419	159.226.63.190	10920
24.180.134.156	31901	MY.NET.213.78	5815	MY.NET.253.42	4416	210.61.144.125	4784
210.125.174.11	27125	MY.NET.208.58	3759	MY.NET.253.41	4287	168.187.26.157	4290
35.10.82.111	25469	MY.NET.204.126	3541	MY.NET.6.7	2577	159.226.45.108	2346
206.186.79.9	22156	MY.NET.208.238	2072	MY.NET.162.199	1746	159.226.114.129	1746
24.17.189.83	20155	MY.NET.213.10	1631	MY.NET.157.200	1615	212.179.58.174	1615
212.141.100.97	19968	MY.NET.204.166	1284	MY.NET.101.192	1202	159.226.45.3	1558
63.248.55.245	17566	MY.NET.60.8	1074	MY.NET.217.42	1054	159.226.63.200	1556
129.186.93.133	4663	MY.NET.217.10	996	MY.NET.221.94	612	212.179.66.2	1144
194.165.230.250	3300	MY.NET.208.66	785	MY.NET.53.28	542	205.188.179.33	1054
210.55.227.138	3234	MY.NET.208.166	766	MY.NET.100.230	535	213.25.136.60	663

Chart -1 Scans generated by source address

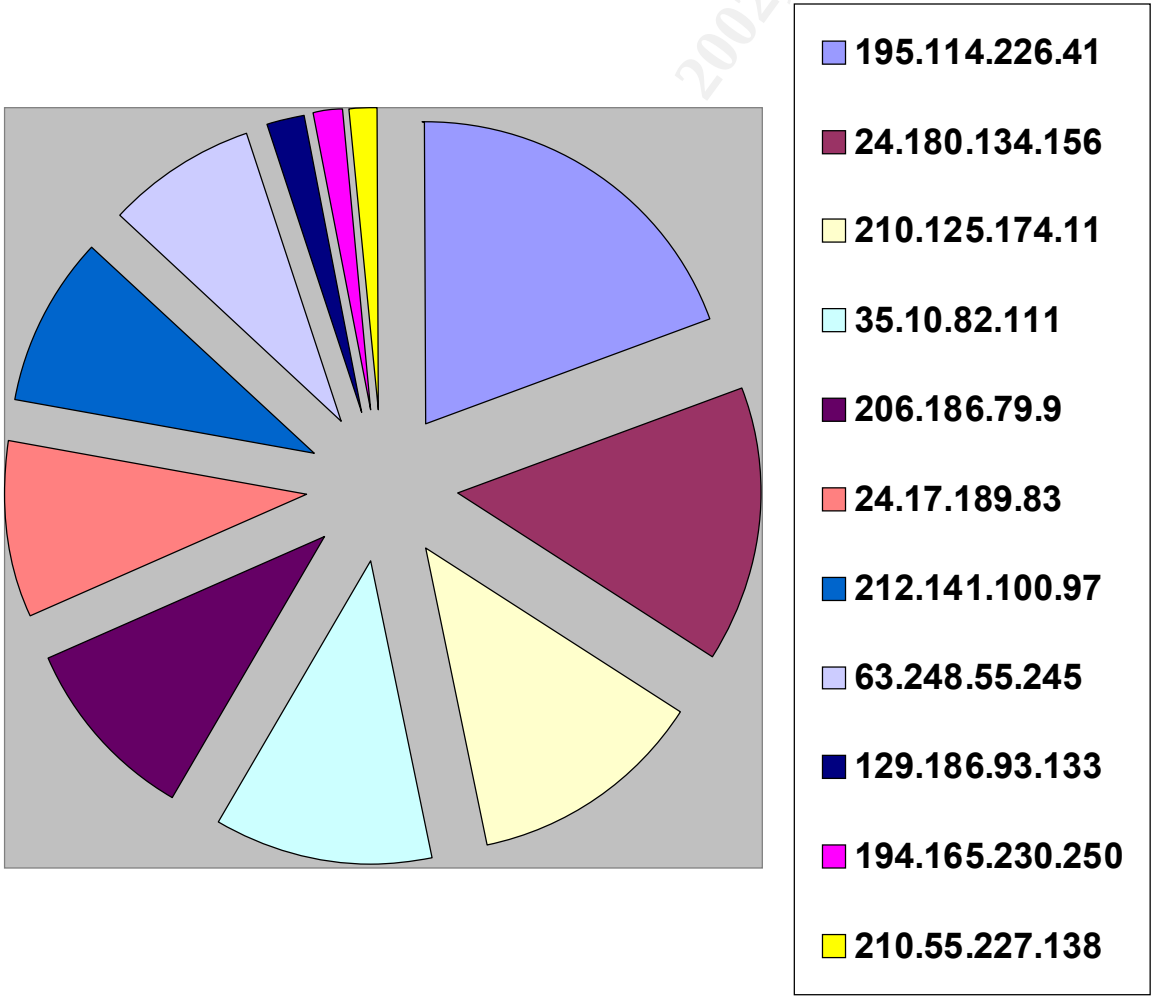


Chart -2 Scans generated by destination address

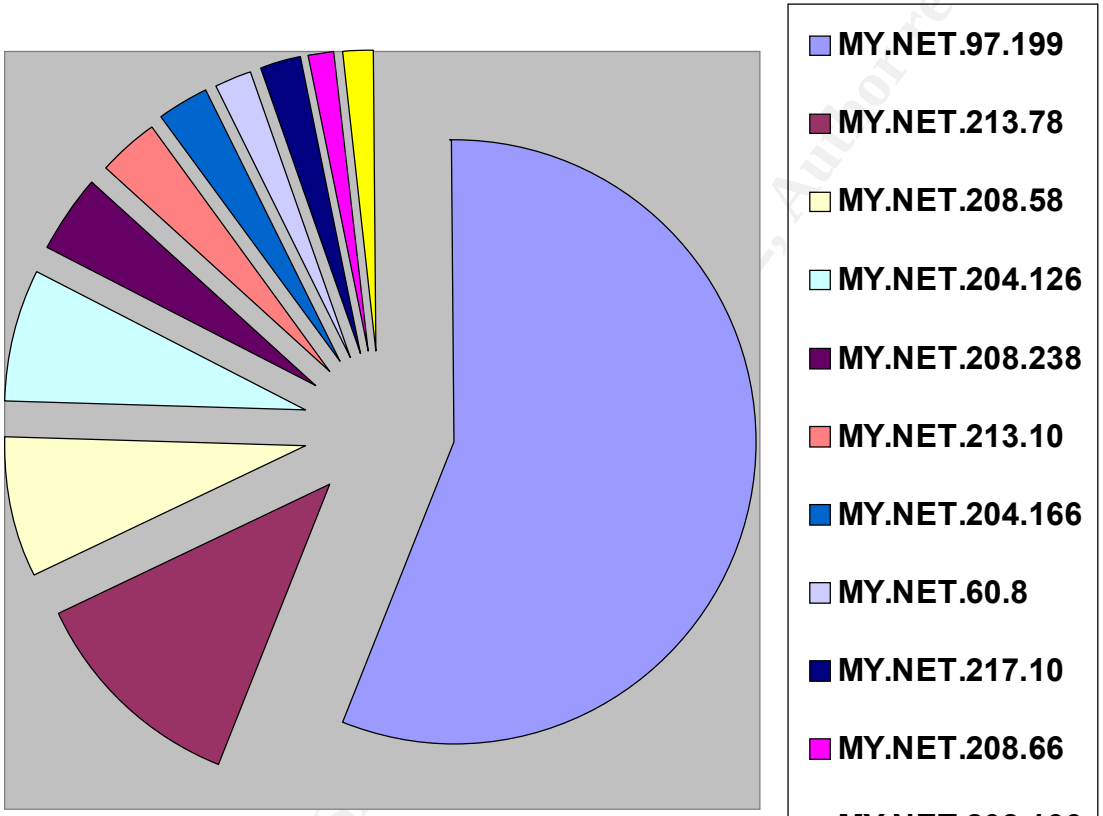


Chart -3 Alerts generated by destination address

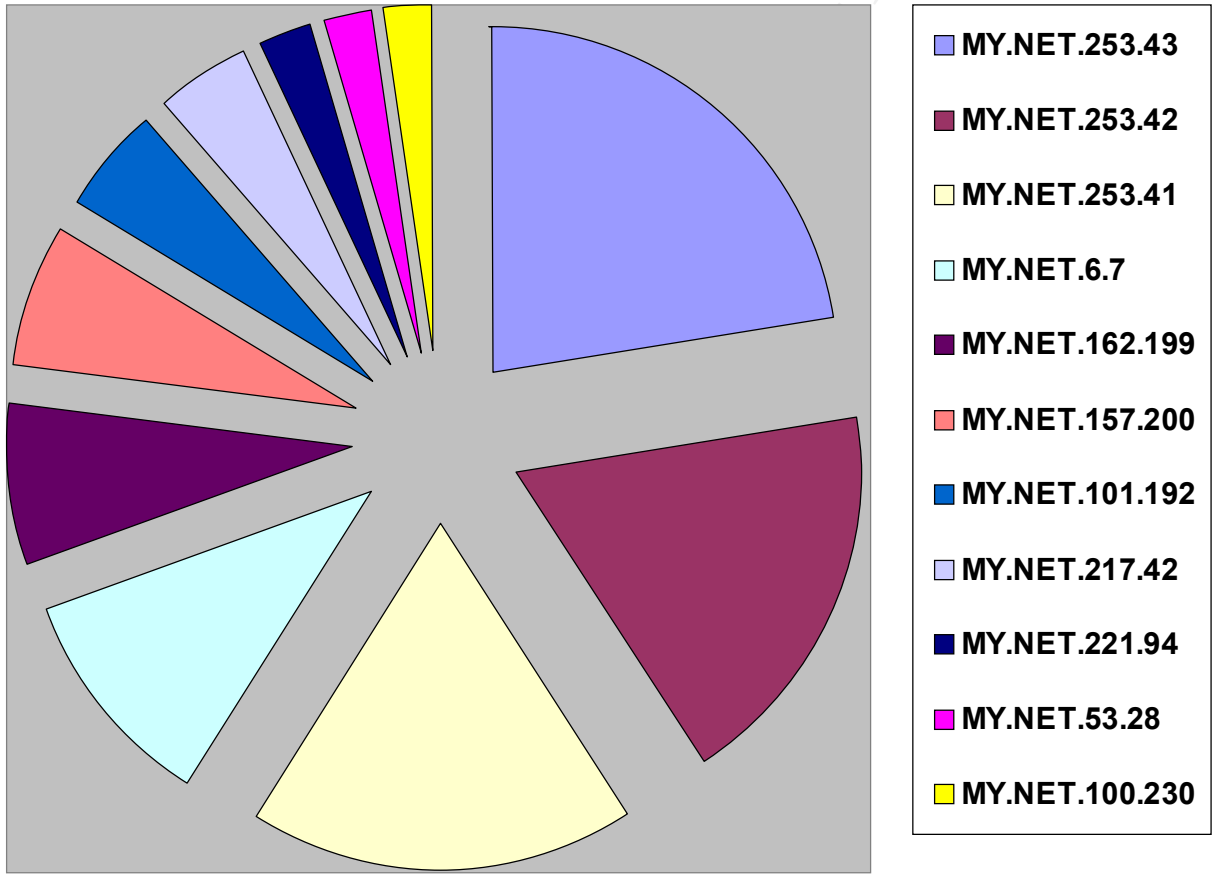
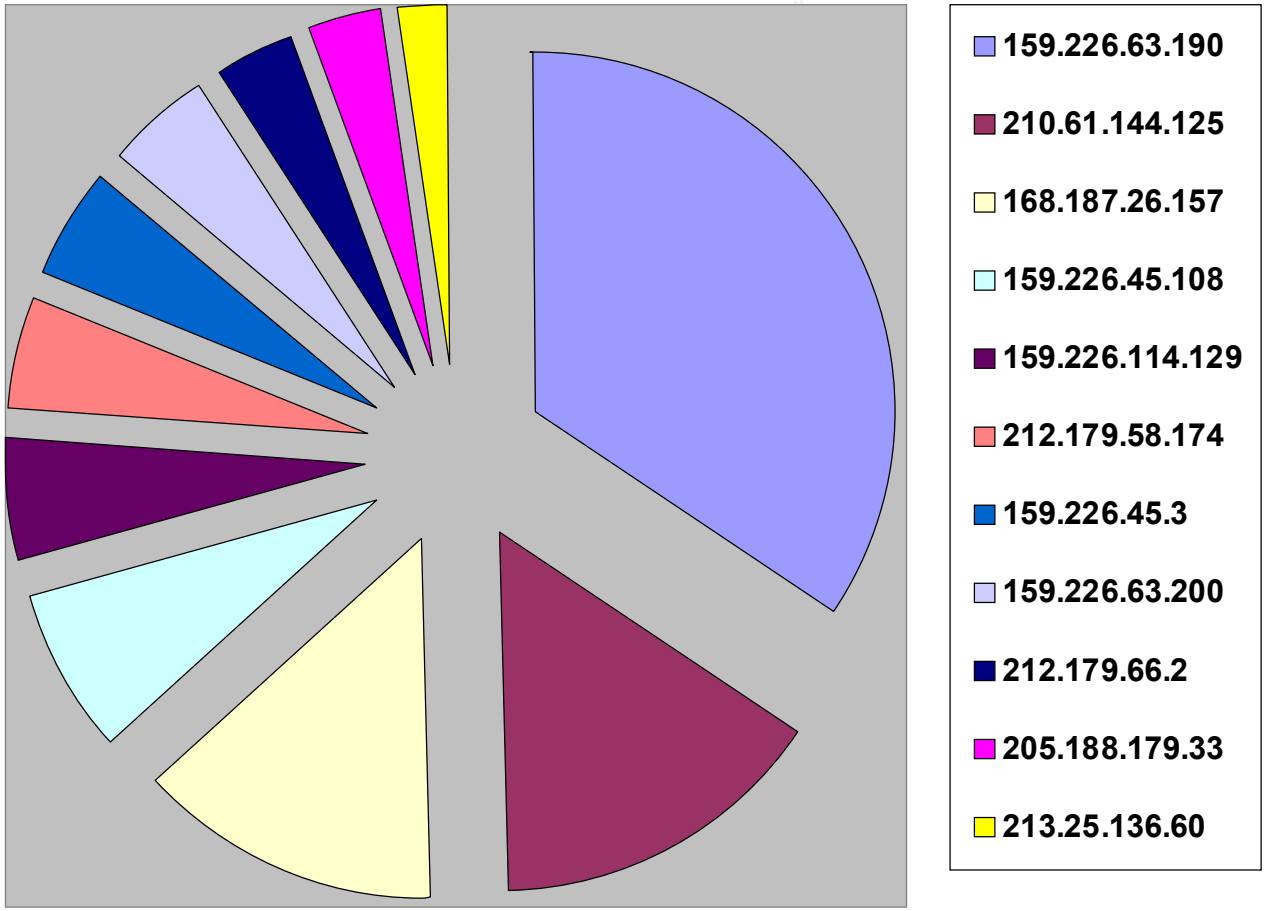


Chart - 4 Alerts generated by source address



Security issues of concern in priority

1. Internal host scanning

Event description

An internal host on the network is scanning other hosts on the network. This may be an indication that an internal host is comprimised and being used as a scanner or it could be a sign of a malicious insider.

Suggested security action

I would immediately check this machine for compromise or malicious insider use.

IP Address	Activity	Plausible explanation	Severity
MY.NET.1.3 TOTAL HOSTS:1916 TCP:0 UDP:2206	An internal machine scanning other internal hosts	The machine may be compromised or at the very least running unauthorized or misconfigured software.	HIGH

Sample of Traffic:

```
09/03-09:16:06.629274  [**] spp_portscan: PORTSCAN DETECTED from MY.NET.1.3 (THRESHOLD 7 connections in 2 seconds) [**]
09/03-09:16:06.755697  [**] spp_portscan: portscan status from MY.NET.1.3: 23 connections across 22 hosts: TCP(0), UDP(23) [**]
09/03-09:16:06.868520  [**] spp_portscan: portscan status from MY.NET.1.3: 18 connections across 15 hosts: TCP(0), UDP(18) [**]
09/03-09:16:23.712264  [**] spp_portscan: portscan status from MY.NET.1.3: 12 connections across 11 hosts: TCP(0), UDP(12) [**]
09/03-09:16:26.083873  [**] spp_portscan: End of portscan from MY.NET.1.3 (TOTAL HOSTS:1916 TCP:0 UDP:2206) [**]
```

Correlation: N/A

2. WatchList Activity

The watchlist networks identified

Two address ranges were specified in the watchlist that records network activity coming from those ip address within the range. There was a lot of traffic to the network from hosts within this address range. A sample of the traffic can be found in Section 2 WatchList traffic. Watchlist traffic is of considerable interest as the network security posture is to log the connections into the network. Obviously taking the effort to log the network access attempts from these address spaces means that any traffic should be given more scrutiny than normal.

- 159.226.x.x: The Computer Network Center Chinese Academy of Sciences. There was a lot of telnet (port23) and mail traffic (port 25)

between hosts within the watchlist and the internal network. It is possible mail was sent and telnet sessions were established.

DNS – lookup: The Computer Network Center Chinese Academy of Sciences (NET-NCFC) P.O. Box 2704-10, Institute of Computing Technology Chinese Academy of Sciences Beijing 100080, China.

Additional mention of this particular ip address can be found at: http://www.sans.org/y2k/022200.htm

- 212.179.x.x: Bezeq International, Israel. There was some mail activity and a lot of napster activity. If the hosts within this address range warrant close inspection because of their addition to the watchlist then I would revisit the napster policies on the network or perhaps visit the hosts in the internal network invovled in the napster traffic. Napster is known to have some security issues. (see CVE… CAN-2000-0281, CAN-2000-0412)

DNS lookup: Bezeq International address: 40 Hashacham St. address: Petach Tikvah Israel

What did they do?

Referring to the Alerts by Source Address chart 6 of the top 11 addresses are contained within the watchlists with 159.226.x.x being the prime offender. If you correlate this with the Alerts by Destination Address chart the three top destination addresses were MY.NET.253.41, MY.NET.253.42, and MY.NET.253.43. All these internal hosts were targeted on port 25 by hosts on the watchlists networks, with 159.226.x.x generating the majority of the alerts.

Suggested security action

These hosts are probably mailservers and the log files should be checked immediately.

IP Address	Activity	Plausible explanation	Severity

Watchlist 000222 NET-NCFC [**] 159.226.x.x	A lot of traffic to port 25 and 23 , mail and telnet – this ip is on the watchlist	Could be mail and/or telnet attempts – cannot determine because traffic flow is unidirectional	HIGH – assumed because of watchlist

Sample of Traffic:

```
09/05-04:33:27.292559  [**] Watchlist 000222 NET-NCFC [**] 159.226.5.77:1232 -> MY.NET.253.43:25
09/11-03:32:24.827696  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4016 -> MY.NET.253.43:25
09/13-07:04:30.320543  [**] Watchlist 000222 NET-NCFC [**] 159.226.5.94:3982 -> MY.NET.253.43:25
09/13-07:04:30.325625  [**] Watchlist 000222 NET-NCFC [**] 159.226.5.94:3982 -> MY.NET.253.43:25
08/17-01:38:04.537509  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.190:1094 -> MY.NET.253.43:25
08/17-06:39:50.388789  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.190:1719 -> MY.NET.253.42:25
09/08-07:15:18.160830  [**] Watchlist 000222 NET-NCFC [**] 159.226.21.3:22989 -> MY.NET.253.42:25
09/08-07:15:18.888527  [**] Watchlist 000222 NET-NCFC [**] 159.226.21.3:22989 -> MY.NET.253.42:25
08/11-11:44:07.487451  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1848 -> MY.NET.253.42:25
08/15-18:37:37.788602  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.190:1792 -> MY.NET.253.41:25
09/13-21:17:55.685863  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4487 -> MY.NET.253.41:25
09/13-21:17:56.543530  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4487 -> MY.NET.253.41:25
08/17-02:34:13.979513  [**] Watchlist 000222 NET-NCFC [**] 159.226.66.130:1279 -> MY.NET.253.41:25
08/11-11:57:40.658687  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1922 -> MY.NET.253.41:25
08/16-20:43:23.793259  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4628 -> MY.NET.6.7:23
08/16-20:43:24.581289  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4628 -> MY.NET.6.7:23
09/11-04:58:16.400806  [**] Watchlist 000222 NET-NCFC [**] 159.226.64.61:51343 -> MY.NET.6.7:25
08/11-01:54:49.408437  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1051 -> MY.NET.6.7:23
09/11-03:30:47.857584  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4016 -> MY.NET.253.43:25
09/11-11:06:50.919149  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:23 -> MY.NET.163.32:1060
08/16-03:09:37.890806  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1098 -> MY.NET.100.230:113
08/16-03:58:29.254058  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1138 -> MY.NET.100.230:113
08/11-01:53:16.813427  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1628 -> MY.NET.253.42:25
08/11-01:53:16.813494  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.200:1628 -> MY.NET.253.42:25

08/11-01:51:06.064671  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1051 -> MY.NET.6.7:23

08/11-02:24:41.440131  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1054 -> MY.NET.60.8:23
08/11-02:24:42.308394  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1054 -> MY.NET.60.8:23
---most to .7
08/11-03:01:50.262517  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1057 -> MY.NET.6.7:23
08/11-03:01:53.618330  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1057 -> MY.NET.6.7:23
 ---IP 159.226.114.129
08/20-15:12:50.398838  [**] Watchlist 000222 NET-NCFC [**] 159.226.114.129:21 -> MY.NET.162.199:1095

08/20-15:13:34.060894  [**] Watchlist 000222 NET-NCFC [**] 159.226.114.129:37268 -> MY.NET.162.199:1097
```

Correlation: see description at beginning.

IP Address	Activity	Plausible explanation	Severity
Watchlist 000220 IL-ISDNNET-990517 [**] 212.x.7.x	Mail and napster attempts.	Sharing music files/possible vulnerability exploitation, mail attempts.	HIGH – assumed because of watchlist

Sample of Traffic:

```
09/14-10:45:37.434897  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.7.36:1192 -> MY.NET.253.43:25
09/14-10:45:40.888639  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.7.36:1192 -> MY.NET.253.43:25

09/14-07:45:21.201421  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.174:2173 -> MY.NET.157.200:6699
09/14-07:45:21.331348  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.174:2173 -> MY.NET.157.200:6699

09/09-10:45:34.320507  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:22756 -> MY.NET.221.94:6699
09/09-10:45:34.504077  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:22756 -> MY.NET.221.94:6699


08/20-09:05:48.446745  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.29.150:1098 -> MY.NET.53.28:4407
08/20-09:05:48.496787  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.29.150:1098 -> MY.NET.53.28:4407
09/09-10:45:33.326028  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:22756 -> MY.NET.221.94:6699
09/09-10:45:34.320507  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:22756 -> MY.NET.221.94:6699
08/17-12:45:53.433672  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:4807 -> MY.NET.181.87:6699
08/17-12:45:54.068768  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.66.2:4807 -> MY.NET.181.87:6699

09/14-07:45:21.637923  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.174:2173 -> MY.NET.157.200:6699
09/14-07:45:22.427696  [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.58.174:2173 -> MY.NET.157.200:6699
1615 napster attempts
```

Correlation: see description at beginning.

3. SNMP community string

Event description

The traffic indicates that internal machines are using the default community string to communicate. This is an insecure configuration.

Suggested security action

The default community string "public" should be renamed to a hard to guess password.

IP Address	Activity	Plausible explanation	Severity
MY.NET.98.181	SNMP public accesses	Someone is trying to take advantage of the default "public" community string. Internal traffic indicates that default community string "public" has not been renamed. – Internal users may be able to map the network.	HIGH

Sample of Traffic:

```
09/02-07:59:57.907710  [**] SNMP public access [**] MY.NET.98.181:1205 -> MY.NET.101.192:161
09/02-07:59:58.103467  [**] SNMP public access [**] MY.NET.98.181:1206 -> MY.NET.101.192:161
09/02-08:03:23.255707  [**] SMB Name Wildcard [**] MY.NET.101.160:137 -> MY.NET.101.192:137
09/02-08:03:24.761865  [**] SMB Name Wildcard [**] MY.NET.101.160:137 -> MY.NET.101.192:137

09/10-17:11:57.000739  [**] SNMP public access [**] MY.NET.98.172:1519 -> MY.NET.101.192:161
09/10-17:11:57.015726  [**] SNMP public access [**] MY.NET.98.172:1520 -> MY.NET.101.192:161
08/15-20:00:08.300206  [**] SNMP public access [**] MY.NET.97.154:1062 -> MY.NET.101.192:161
08/15-20:00:08.621159  [**] SNMP public access [**] MY.NET.97.154:1063 -> MY.NET.101.192:161
09/11-19:37:51.662281  [**] SNMP public access [**] MY.NET.97.217:1380 -> MY.NET.101.192:161
09/11-21:00:02.792773  [**] SNMP public access [**] MY.NET.97.217:1618 -> MY.NET.101.192:161
09/13-19:20:12.022455  [**] SNMP public access [**] MY.NET.98.171:1439 -> MY.NET.101.192:161
```

Correlation: CAN-1999-0519 An SNMP community name can be guessed. CAN-1999-0517 a community name is default, null or missing.

4. Active Reconnaissance

Event description

24.180.134.156 has the honor to be #2 in the amount of scans generated by source address. This machine is actively scanning the network using a variety of mapping techniques. Xmas (all flags set) tree scans, SYN scans, UDP, they are probably using the nmap tool to accomplish this scanning. (see entry in traffic below for conformation.)

Suggested security action

Contact 24.180.134.156's ISP and report the activity, hopefully their account will be revoked.

IP Address	Activity	Plausible explanation	Severity
24.180.134.156	Active mapping of the network to determine hosts and Oss.	Reconnaissance for a future attack.	MED – due to number of scans

Sample of Traffic:

```
Sep 11 04:48:03 24.180.134.156:3089 -> MY.NET.208.1:757 SYN **S*****
Sep 11 04:48:03 24.180.134.156:3091 -> MY.NET.208.1:4333 SYN **S*****
Sep 11 05:19:09 24.180.134.156:50109 -> MY.NET.208.245:23 SYN 2*S***** RESERVEDBITS
Sep 11 05:19:13 24.180.134.156:50108 -> MY.NET.208.245:23 SYN **S*****
Sep 11 05:08:22 24.180.134.156:50109 -> MY.NET.208.146:77 SYN 2*S***** RESERVEDBITS
Sep 11 05:08:27 24.180.134.156:50115 -> MY.NET.208.146:40548 XMAS ***F*P*U
Sep 11 05:09:00 24.180.134.156:50110 -> MY.NET.208.153:23 NULL ********
Sep 11 05:09:00 24.180.134.156:50111 -> MY.NET.208.153:23 NMAPID **SF*P*U
Sep 11 05:09:00 24.180.134.156:50113 -> MY.NET.208.153:34532 SYN **S*****
Sep 11 05:09:00 24.180.134.156:50115 -> MY.NET.208.153:34532 XMAS ***F*P*U
Sep 11 05:09:00 24.180.134.156:50102 -> MY.NET.208.153:34532 UDP
```

Correlation: DNS lookup: DNS lookup: @Home Network (NETBLK-BLTMMD1-MD-1) 425 Broadway Redwood City, CA 94063 US

5. WinGate activity

Event description

168.187.26.157 is scanning for WinGate on a number of hosts on the network. Windows is a popular firewall/proxy for Windows based machines. The service has some security issues (see correlation in table below) and can be used to anonymize network traffic – an attractive feature for malicious individuals.

Suggested security action

Revisit site security policy in regards to the use of WinGate, check internal machines for signs of compromise.

IP Address	Activity	Plausible explanation	Severity
168.187.26.157	WinGate 1080 Attempt	Most scans for port 1080 are for WinGate which is a popular firewall/proxy for Windows.	MED

Sample of Traffic:

```
09/11-19:15:07.528933  [**] WinGate 1080 Attempt [**] 168.187.26.157:4737 -> MY.NET.53.220:1080
09/11-19:15:07.611279  [**] WinGate 1080 Attempt [**] 168.187.26.157:4770 -> MY.NET.54.10:1080
09/11-19:15:07.956904  [**] WinGate 1080 Attempt [**] 168.187.26.157:4749 -> MY.NET.53.223:1080
```

Correlation: DNS lookup: Kuwait Ministry of Communications (NET-MOC-KW) PO Box No 31811111 KW, CVE-1999-0291 if no password is specified a remote attacker can redirect connections without authentication., CVE-1999-0441, CVE-1999-0494

6. SMB Name Wildcard

IP Address	Activity	Plausible explanation	Severity
131.118.254.222	SMB information is being passed between external hosts and host on the internal network.	SMB name wildcard is indicative of an information gathering activity.	LOW

Sample of Traffic:

```
08/11-16:15:33.790499  [**] SMB Name Wildcard [**] 131.118.254.222:137 -> MY.NET.6.7:137
08/11-16:15:35.294638  [**] SMB Name Wildcard [**] 131.118.254.222:137 -> MY.NET.6.7:137
```

Correlation: DNS lookup: University of Maryland (NET-MINCNET) System Administration 3300 Metzerott Road Adelphi, MD 20783

7. External RPC call

IP Address	Activity	Plausible explanation	Severity
141.223.124.31 209.160.238.215 161.31.208.237	Connection attempts to the portmapper service.	This is a reconnaissance attempt to determine the ports that various NFS services may be running on.	MED

Sample of Traffic:

```
08/19-01:46:08.843875  [**] External RPC call [**] 141.223.124.31:875 -> MY.NET.6.15:111
08/19-01:46:08.843875  [**] External RPC call [**] 141.223.124.31:875 -> MY.NET.6.15:111
08/19-10:11:34.624625  [**] External RPC call [**] 209.160.238.215:2572 -> MY.NET.6.15:111
08/19-10:11:34.624625  [**] External RPC call [**] 209.160.238.215:2572 -> MY.NET.6.15:111
09/10-03:15:33.932802  [**] External RPC call [**] 161.31.208.237:874 -> MY.NET.6.15:111
09/10-03:15:33.932802  [**] External RPC call [**] 161.31.208.237:874 -> MY.NET.6.15:111
```

Correlation DNS lookups:

141.223.124.31 Pohang Institute of Science and Technology (NET-PIST) Computer Center POSTECH P.O. Box 125 Pohang, 790-330 REPUBLIC OF KOREA

209.160.238.215 Brooks Fiber Properties, Inc. (NETBLK-NETBLK-BROOKS) 10316 Placer Lane, Sacramento, CA 95827 US

161.31.208.237 University of Central Arkansas (NET-UCANET) Box 4932 Conway, AR 72035 US

8. ALERTS

A selection of the alerts generated by the network IDS are contained within this section. A description of the alert can be found contained within the respective tables.

Tinyfrag

IP Address	Activity	Plausible explanation	Severity
24.68.58.96	A tiny fragments alarm is generated when TCP traffic was fragmented smaller than is normally done by network infrastructure (e.g. OS, routers).	Tiny framgments or TCP fragmentation is a way to defeat firewalls and intrusion detection systems that do not reassemble packets as part of their detection of malicious activity or forwarding policies.	MED

Sample of Traffic:

```
09/11-13:21:13.480527  [**] Tiny Fragments - Possible Hostile Activity [**] 24.68.58.96 -> MY.NET.217.82
09/11-13:21:13.480527  [**] Tiny Fragments - Possible Hostile Activity [**] 24.68.58.96 -> MY.NET.217.82
```

Correlation DNS lookup: Shaw Fiberlink ltd. (NETBLK-FIBERLINK-CABLE) 630 3rd Avenue SW, Suite 900 Calgary AB, 4L4 C

Queso

IP Address	Activity	Plausible explanation	Severity
24.3.161.193 64.80.63.121 147.126.59.89	Queso is a operating system mapping tool. Queso may have been deployed against the network.	The tool sends strange combinations of TCP flags to a host and based on the host response is able to tell with a high degree of accuracy what operating system (and patch # in some cases) it is using. The tool exploits the fact that the RFC for TCP/IP communication may be adhered too by the software developers of the OS stacks but there is still a lot of room for interpretation in the "gray areas". Since there are some flag combinations that are generated by the tool that were never even considered by the developers because they would not occur "naturally" different OSs will respond in different but predictable ways.	MED

Sample of Traffic:

```
09/05-09:00:54.631991  [**] Queso fingerprint [**] 24.3.161.193:32814 -> MY.NET.145.9:110
09/05-09:00:54.631991  [**] Queso fingerprint [**] 24.3.161.193:32814 -> MY.NET.145.9:110
09/07-19:27:42.236314  [**] Queso fingerprint [**] 64.80.63.121:4114 -> MY.NET.204.214:6355
09/07-19:27:42.236314  [**] Queso fingerprint [**] 64.80.63.121:4114 -> MY.NET.204.214:6355
09/06-09:31:55.767609  [**] Queso fingerprint [**] 147.126.59.89:37262 -> MY.NET.253.24:113
09/06-09:31:55.767609  [**] Queso fingerprint [**] 147.126.59.89:37262 -> MY.NET.253.24:113
```

Correlation:
DNS lookups:
24.3.161.193 @Home Network (NETBLK-NJ-COMCAST-UNION-1) 425 Broadway Redwood City, CA 94063 US

64.80.63.121 PaeTec Communications, Inc. (NETBLK-PAETECCOMM) 290 Woodcliff Dr. Fairport, NY 14450 US

147.126.59.89 Loyola University Chicago (NET-LUC) Building 201, Second Floor 8601 W. Roosevelt Road Forest Park, IL 60130 US

wuftpd

IP Address	Activity	Plausible explanation	Severity
24.17.189.83	The wu-ftpd exploit is a buffer overflow that allows a remote user to gain access to a machine with the vulnerable ftp software.	Someone is deploying the exploit against hosts hoping they are running the vulnerable software so they can gain rout access.	MED

Sample of Traffic:

```
09/08-05:59:01.961301  [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**] 24.17.189.83:2362 -> MY.NET.202.202:21
09/08-05:59:01.961301  [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**] 24.17.189.83:2362 -> MY.NET.202.202:21
```

Correlation DNS lookup:
24.17.189.83 @Home Network (NETBLK-BB1-RDC1-TX-10) 425 Broadway Redwood City, CA 94063 US

Null scan

IP Address	Activity	Plausible explanation	Severity
207.151.147.201 24.200.201.223	Someone is scanning the network with packets that have no TCP flags set	A stealth scan of the network	LOW

Sample of Traffic:

```
08/16-01:42:51.231463  [**] Null scan! [**] 207.151.147.201:58190 -> MY.NET.60.8:21
08/16-19:17:36.848025  [**] Null scan! [**] 24.200.201.223:1635 -> MY.NET.162.183:6346
```

Correlation DNS lookup:
207.151.147.201 Los Nettos (NETBLK-LOS-NETTOS-BLK3) USC Information Sciences Institute PO 11565 Marina del Rey, CA 90295 US

24.200.201.223 Videotron Ltee (NETBLK-VL-D-MF-18C8C900) 2000 Rue Berri Montreal, QC H2L 4V7 Canada

9. *Miscellaneous scans*

IP Address	Activity	Plausible explanation	Severity
205.188.179.33	Sun RPC high port traffic – or probably ICQ traffic	Since a source port of 4000 this is probably ICQ traffic	LOW

Sample of Traffic:

```
08/16-08:51:03.100441  [**] Attempted Sun RPC high port access [**] 205.188.179.33:4000 -> MY.NET.217.42:32771
08/16-08:53:03.035231  [**] Attempted Sun RPC high port access [**] 205.188.179.33:4000 -> MY.NET.217.42:32771
```

Correlation: http://www.hypertony.co.uk/portscan/ps1.htm Mention at this site about this ip address scanning, but info. could not be copied to a text format. Please consult the above hyperlink for further examples.

IP Address	Activity	Plausible explanation	Severity
210.61.144.125	SYN-FIN scans. The address space has been scanned numerous times using SYN-FIN packets generally from port 21 to port 21. This scanning method uses TCP packets with both the SYN and FIN packet flags set which will not occur in normal TCP traffic. The use of port 21 is probably used to evade firewalls that will often allow ftp traffic.	SYNFIN scans are done to map a network to determine what operating systems are on hosts.	MED -** although it is normal reconnaissance the attacker scanned for 45 minutes.

Sample of Traffic:

```
09/11-07:00:46.262912  [**] SYN-FIN scan! [**] 210.61.144.125:21 -> MY.NET.183.226:21
09/11-07:00:46.304557  [**] SYN-FIN scan! [**] 210.61.144.125:21 -> MY.NET.183.228:21
09/11-07:00:46.383615  [**] SYN-FIN scan! [**] 210.61.144.125:21 -> MY.NET.183.232:21

From 06:40 -- 07:25  --- 5298 alerts generated SYN-FIN and port scans....
```

Correlation:
http://www.sans.org/y2k/092400.htm
Server used for this query: [whois.apxxx.net]
inetnum: 210.61.144.0 - 210.61.144.255
netname: HINET8-144-TW
descr: Abnet Information Co., Ltd
descr: 6F. No.22-5
descr: Ning Hsia Rd Taipei, Taiwan
country: TW
Server used for this query: [www.whois.twxxx.net]
Organization Name First Securities Co., LTD.
Street Address 12F, No. 39, Sec. 2, Tun-Hwa S. Rd,
City Taipei
State Taiwan
Country Code TW
IP Network 210.61.144.64/26
Network Name FSCL-NET
Sep 21 17:27:21 hostp in.ftpd[23546]: connect from 210.61.144.125
Sep 21 17:27:21 hostp in.ftpd[23547]: connect from 210.61.144.125
Sep 21 17:28:40 hostca in.ftpd[17331]: connect from 210.61.144.125
Sep 21 17:28:40 hostca in.ftpd[17333]: connect from 210.61.144.125
Sep 21 17:28:43 hostba in.ftpd[2779]: refused connect from 210.61.144.125
Sep 21 17:30:32 hostmau Connection attempt to
TCP 198.82.161.28:21 from 210.61.144.125:21
Sep 21 17:36:02 hosty snort[395880]: SCAN-SYN FIN:
210.61.144.125:21 >z.y.w.34:21
Sep 21 17:36:03 hostj snort[341]: SCAN-SYN FIN:
210.61.144.125:21 -> z.y.w.66:21
Sep 21 17:36:03 hostmi snort[15718]: SCAN-SYN FIN:
210.61.144.125:21 >z.y.w.98:21

IP Address	Activity	Plausible explanation	Severity
210.125.174.11	scan	reconnaissance	LOW

Sample of Traffic:

```
Sep  8 15:10:31 210.125.174.11:53086 -> MY.NET.97.199:56308 UDP
Sep  8 15:10:31 210.125.174.11:53132 -> MY.NET.97.199:43262 UDP
continuously
Sep  8 15:19:56 210.125.174.11:53943 -> MY.NET.97.199:32968 UDP
Sep  8 15:19:56 210.125.174.11:53952 -> MY.NET.97.199:12489 UDP
```

IP Address	Activity	Plausible explanation	Severity
35.10.82.111	scan	reconnaissance	MED lengthy scan

Sample of Traffic:

```
Aug 16 04:35:21 35.10.82.111:2814 -> MY.NET.1.6:27374 SYN **S*****
Aug 16 04:35:20 35.10.82.111:2815 -> MY.NET.1.7:27374 SYN **S*****
continuously
Aug 16 05:16:28 35.10.82.111:3143 -> MY.NET.254.253:27374 SYN **S*****
Aug 16 05:16:28 35.10.82.111:3144 -> MY.NET.254.254:27374 SYN **S*****
```

IP Address	Activity	Plausible explanation	Severity
206.186.79.9	scan	Reconnaissance for DNS multiple hosts	MED – lengthy scan

Sample of Traffic:

```
Sep  9 22:35:21 206.186.79.9:2351 -> MY.NET.1.4:53 SYN **S*****
Sep  9 22:35:21 206.186.79.9:2352 -> MY.NET.1.5:53 SYN **S*****
continuously
Sep 10 02:13:08 206.186.79.9:2422 -> MY.NET.254.176:53 SYN **S*****
Sep 10 02:13:08 206.186.79.9:2450 -> MY.NET.254.204:53 SYN **S*****
```

IP Address	Activity	Plausible explanation	Severity
195.114.226.41	scan	Reconnaissance for ftp multiple hosts	MED lengthy scan

Sample of Traffic:

```
Aug 15 00:46:11 195.114.226.41:2244 -> MY.NET.1.2:21 SYN **S*****
Aug 15 00:46:12 195.114.226.41:2250 -> MY.NET.1.8:21 SYN **S*****
countinously....until
Aug 15 02:35:53 195.114.226.41:4248 -> MY.NET.254.251:21 SYN **S*****
Aug 15 02:35:53 195.114.226.41:4250 -> MY.NET.254.253:21 SYN **S*****
42652 packets sent
```

Assignment #4 Analysis Process

Organization and prioritization is key. The IDS data set given was incomplete, differed in format, had gaps in it, and was very large. It is easy to be overwhelmed by the task at hand. The first step I would recommend is to prioritize your searching through the data set. Find those source and destination addresses that logged the most alarms, scans, and alerts. This provides you with a good starting point for the data. For example the four charts I constructed was my attempt to quickly see where the "action" was occurring in the network. Ask yourself for all these hosts – is this the normal amount of traffic I should be seeing? This is where I would do my first analysis. Once this was complete I would concentrate on an examination of the traffic as a result of any watchlists or high priority alarms.

What would be a high priority alarm? Depends on you network, the services you are running and what you are trying to protect. A good example would be the use of alarm files by the Snort IDS. You could construct multiple alarm files that you could run tcpdump traffic through to prioritize the alarms. Perhaps you want to alarm on all core server accesses. Next you could look through the data set for strange patterns or accesses, the things that don't immediately jump out. Time is of a premium not only because events that are detected quickly are typically easier to deal with but because analysts are usually dedicated but overworked individuals.

The specific tools I used to go through the logs were:

1. Perl scripts taken from www.zeltser.com
2. "grep" for string patterns
3. an excel spreadsheet for sorting and graphing

Last Updated: October 19th, 2017

Upcoming Training

SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced