Global Information Assurance Certification Paper

*** Northcutt, I enjoyed reading detect 2. 70 *

Larry E Erdahl
#1

The following trace was given to me by an employee who is running Sort on his home Linux (SuSe) system.

The first three frames show a normal three way TCP/IP connection. This is the employee's private web server and is listening on port 80, so the connection is accepted and established.

```
04/04-20:50:17.982869 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x4A
xxx.xxx.11.254:51347 -> yyy.yyy.228.97:80 TCP TTL:50 TOS:0x0 ID:32809  DF
**S***** Seq: 0x7BFAD296   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 1233060 0

04/04-20:50:17.982981 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x4A
yyy.yyy.97:80 -> xxx.xxx.11.254:51347 TCP TTL:64 TOS:0x0 ID:51531  DF
**S***A* Seq: 0x6DE68E35   Ack: 0x7BFAD297   Win: 0x7D78
TCP Options => MSS: 1460 NOP NOP TS: 43475603 1233060 NOP WS: 0

04/04-20:50:18.163104 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x42
xxx.xxx.11.254:51347 -> yyy.yyy.228.97:80 TCP TTL:50 TOS:0x0 ID:33045  DF
******A* Seq: 0x7BFAD297   Ack: 0x6DE68E36   Win: 0x2238
TCP Options => NOP NOP TS: 1233060 43475603
```

The fourth frame shows an attack to the counterfiglet application. This appears to be an attempt to gather information about the user and id of this application.

```
04/04-20:50:18.919030 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0xC3
xxx.xxx.11.254:51347 -> yyy.yyy.228.97:80 TCP TTL:50 TOS:0x0 ID:34538  DF
*****PA* Seq: 0x7BFAD297   Ack: 0x6DE68E36   Win: 0x2238
TCP Options => NOP NOP TS: 1233062 43475603
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 63 6F 75  GET /cgi-bin/cou
6E 74 65 72 66 69 67 6C 65 74 2F 6E 63 2F 66 3D  nterfiglet/nc/f=
3B 65 63 68 6F 3B 65 63 68 6F 25 32 30 7B 5F 62  ;echo;echo%20{_b
65 67 69 6E 2D 63 6F 75 6E 74 65 72 66 69 67 6C  egin-counterfigl
65 74 5F 7D 3B 75 6E 61 6D 65 25 32 30 2D 61 3B  et_};uname%20-a;
69 64 3B 77 3B 65 63 68 6F 25 32 30 7B 5F 65 6E  id;w;echo%20{_en
64 2D 63 6F 75 6E 74 65 72 66 69 67 6C 65 74 5F  d-counterfiglet_
7D 3B 65 63 68 6F 20 48 54 54 50 2F 31 2E 30 0A  };echo HTTP/1.0.
0A                                               .

04/04-20:50:20.161261 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0xC3
xxx.xxx.11.254:51347 -> yyy.yyy.228.97:80 TCP TTL:50 TOS:0x0 ID:36904  DF
*****PA* Seq: 0x7BFAD297   Ack: 0x6DE68E36   Win: 0x2238
TCP Options => NOP NOP TS: 1233064 43475603
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 63 6F 75  GET /cgi-bin/cou
6E 74 65 72 66 69 67 6C 65 74 2F 6E 63 2F 66 3D  nterfiglet/nc/f=
3B 65 63 68 6F 3B 65 63 68 6F 25 32 30 7B 5F 62  ;echo;echo%20{_b
65 67 69 6E 2D 63 6F 75 6E 74 65 72 66 69 67 6C  egin-counterfigl
65 74 5F 7D 3B 75 6E 61 6D 65 25 32 30 2D 61 3B  et_};uname%20-a;
69 64 3B 77 3B 65 63 68 6F 25 32 30 7B 5F 65 6E  id;w;echo%20{_en
64 2D 63 6F 75 6E 74 65 72 66 69 67 6C 65 74 5F  d-counterfiglet_
7D 3B 65 63 68 6F 20 48 54 54 50 2F 31 2E 30 0A  };echo HTTP/1.0.
0A                                               .

04/04-20:50:23.160491 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0xC3
xxx.xxx.11.254:51347 -> yyy.yyy.228.97:80 TCP TTL:50 TOS:0x0 ID:41124  DF
*****PA* Seq: 0x7BFAD297   Ack: 0x6DE68E36   Win: 0x2238
TCP Options => NOP NOP TS: 1233070 43475603
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 63 6F 75  GET /cgi-bin/cou
6E 74 65 72 66 69 67 6C 65 74 2F 6E 63 2F 66 3D  nterfiglet/nc/f=
3B 65 63 68 6F 3B 65 63 68 6F 25 32 30 7B 5F 62  ;echo;echo%20{_b
69 67 69 6E 2D 63 6F 75 6E 74 65 72 66 69 67 6C  egin-counterfigl
```

```
65 74 5F 7D 3B 75 6E 61 6D 65 25 32 30 2D 61 3B  et_};uname%20-a;
69 64 3B 77 3B 65 63 68 6F 25 32 30 7B 5F 65 6E  id;w;echo%20{_en
64 2D 63 6F 75 6E 74 65 72 66 69 67 6C 65 74 5F  d-counterfiglet_
7D 3B 65 63 68 6F 20 48 54 54 50 2F 31 2E 30 0A  };echo HTTP/1.0.
0A                                               .
```

Summary:

This was a recon attack, the attacker targeted this IP address specifically, no other IP addresses were tried. The attacker was searching for uname and id information, which leads me to believe that this attacker was planning on being mischievous. I did do a like research on counterfiglet and found that it is a web page hit counter that can be configured and queried remotely. I have suggested to the employee that he place this IP address on his watch list.

#2
This trace was giving to me by an employee who is running snort on his home Linux (SuSe) box.

The first three frames show a normal TCP/IP handshake. The attacker is attempting to make a connection to port 512, which is the exec port.

```
04/04-20:50:17.988188 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x4A
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:32811  DF
**S***** Seq: 0x7BFCA97A   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 1233060 0

04/04-20:50:17.988243 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x4A
yyy.yyy.228.97:512 -> xxx.xxx.11.254:51349 TCP TTL:64 TOS:0x0 ID:51533  DF
**S***A* Seq: 0x6DD7DCAE   Ack: 0x7BFCA97B   Win: 0x7D78
TCP Options => MSS: 1460 NOP NOP TS: 43475604 1233060 NOP WS: 0

04/04-20:50:18.175677 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x42
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:33068  DF
******A* Seq: 0x7BFCA97B   Ack: 0x6DD7DCAF   Win: 0x2238
TCP Options => NOP NOP TS: 1233060 43475604
```

Frame three shows the connection being established, however frame four sends a Fin to the attacker to close the connection. I found out after visiting with the employee that he is running Port Sentry on this box and that port 512 is not really responding Port Sentry is. Helps to keep the attacker guessing, while gathering a little more forensic evidence.

```
04/04-20:50:18.182883 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x42
yyy.yyy.228.97:512 -> xxx.xxx.11.254:51349 TCP TTL:64 TOS:0x0 ID:51538  DF
***F**A* Seq: 0x6DD7DCAF   Ack: 0x7BFCA97B   Win: 0x7D78
TCP Options => NOP NOP TS: 43475623 1233060
```

It appears that the attacker is trying to log on here with the username guest

```
04/04-20:50:18.921147 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x8A
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:34539  DF
*****PA* Seq: 0x7BFCA97B   Ack: 0x6DD7DCB0   Win: 0x2238
TCP Options => NOP NOP TS: 1233062 43475623
30 00 67 75 65 73 74 00 67 75 65 73 74 00 65 63  0.guest.guest.ec
68 6F 20 27 7B 5F 67 75 65 73 74 2D 62 65 67 69  ho '{_guest-begi
6E 5F 7D 27 3B 75 6E 61 6D 65 20 2D 61 3B 69 64  n_}';uname -a;id
3B 77 3B 65 63 68 6F 20 27 7B 5F 67 75 65 73 74  ;w;echo '{_guest
2D 65 6E 64 5F 7D 27 00                          -end_}'.
```

This next frame sent by the attacker acknowledges the close attempt but never closes his half of the connection. In the following frames the attacker keeps trying and the attacked host keeps trying to close the connection.

```
04/04-20:50:19.920100 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x42
```

```
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:36385  DF
***F**A* Seq: 0x7BFCA9C3   Ack: 0x6DD7DCB0   Win: 0x2238
TCP Options => NOP NOP TS: 1233064 43475623

04/04-20:50:20.158005 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x8A
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:36903  DF
***F*PA* Seq: 0x7BFCA97B   Ack: 0x6DD7DCB0   Win: 0x2238
TCP Options => NOP NOP TS: 1233064 43475623
30 00 67 75 65 73 74 00 67 75 65 73 74 00 65 63  0.guest.guest.ec
68 6F 20 27 7B 5F 67 75 65 73 74 2D 62 65 67 69  ho '{_guest-begi
6E 5F 7D 27 3B 75 6E 61 6D 65 20 2D 61 3B 69 64  n_}';uname -a;id
3B 77 3B 65 63 68 6F 20 27 7B 5F 67 75 65 73 74  ;w;echo '{_guest
2D 65 6E 64 5F 7D 27 00                          -end_}'.

04/04-20:50:21.177106 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x42
yyy.yyy.228.97:512 -> xxx.xxx.11.254:51349 TCP TTL:64 TOS:0x0 ID:51542  DF
***F**A* Seq: 0x6DD7DCAF   Ack: 0x7BFCA97B   Win: 0x7D78
TCP Options => NOP NOP TS: 43475923 1233060

04/04-20:50:21.270322 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x42
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:38121  DF
***F**A* Seq: 0x7BFCA9C3   Ack: 0x6DD7DCB0   Win: 0x2238
TCP Options => NOP NOP TS: 1233067 43475923

04/04-20:50:23.157182 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x8A
xxx.xxx.11.254:51349 -> yyy.yyy.228.97:512 TCP TTL:50 TOS:0x0 ID:41123  DF
***F*PA* Seq: 0x7BFCA97B   Ack: 0x6DD7DCB0   Win: 0x2238
TCP Options => NOP NOP TS: 1233070 43475923
30 00 67 75 65 73 74 00 67 75 65 73 74 00 65 63  0.guest.guest.ec
68 6F 20 27 7B 5F 67 75 65 73 74 2D 62 65 67 69  ho '{_guest-begi
6E 5F 7D 27 3B 75 6E 61 6D 65 20 2D 61 3B 69 64  n_}';uname -a;id
3B 77 3B 65 63 68 6F 20 27 7B 5F 67 75 65 73 74  ;w;echo '{_guest
2D 65 6E 64 5F 7D 27 00                          -end_}'.
```

Summary:

This attacker has targeted this web site's IP address which leads me to believe that he my have done recon for this attack in the past. The attack was being directed against the well-known TCP port of 512, which is assigned to exec. Exec is a remote process execution for authentication performed using passwords and UNIX login names. The time frames between packets leads me to believe that this was a automated attack with malicious intent. I suggested to this employee that he adds this IP Address to his watch list or better yet block this IP.

#3
This was giving to me by a employee that is running snort on his home web site.

This attack is a known exploit, it is an attempt to gain a root sh.

```
04/04-20:50:17.986850 0:E0:D0:11:55:2D -> 0:10:4B:9F:3:47 type:0x800 len:0x4A
xxx.xxx.11.254:51348 -> yyy.yyy.228.97:5556 TCP TTL:50 TOS:0x0 ID:32810  DF
**S***** Seq: 0x7BFB974E   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 1233060 0

04/04-20:50:17.986909 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:5556 -> xxx.xxx.11.254:51348 TCP TTL:255 TOS:0x0 ID:51532
****R*A* Seq: 0x0   Ack: 0x7BFB974F   Win: 0x0


04/04-20:50:17.994894 0:E0:D0:11:55:2D -> 0:E0:29:37:2B:76 type:0x800 len:0x4A
xxx.xxx.11.254:51351 -> yyy.yyy.228.98:5556 TCP TTL:50 TOS:0x0 ID:32813  DF
**S***** Seq: 0x7BFEAB38   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP WS: 0 NOP NOP TS: 1233060 0

04/04-20:50:17.994974 0:E0:29:37:2B:76 -> 0:E0:D0:11:55:2D type:0x800 len:0x3C
yyy.yyy.228.98:5556 -> xxx.xxx.11.254:51351 TCP TTL:128 TOS:0x0 ID:23429
```

```
****R*A* Seq: 0x0   Ack: 0x7BFEAB39   Win: 0x0
F3 75 30 73 00 00                              .u0s..
```

Summary:
This attack is directed specify to this IP address, because of this I feel that this site has been reconed in the past by this attacker. This attack is an attempt to gain access to this box. The exploit being used is a well document attack used to gain a root shell. This IP address should be blocked from this site and if possible the attackers ISP should be notified.

#4
I was asked to analyze this by an employee who is running Snort on his home web site. He was afraid that he my have been hacked, because this showed up on his Snort report and he claims that he never sent anything to this site, although this site is on his watch list. The UDP frames seem to be sending data to this site.

At first glance I thought that this was a UDP port scan, because of the incrementing UDP port numbers. That was until I noticed the TTLs. I called the employee quizzed him on this. It seems that he was doing a traceroute to this host after he found its IP address included in his Snort reports.

```
4/04-23:01:27.102563 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:50681 -> xxx.xxx.11.254:33435 UDP TTL:1 TOS:0x0 ID:53099
Len: 20
01 01 00 00 97 BA EA 38 4F 90 01 00              .......8O...

04/04-23:01:27.140400 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:50681 -> xxx.xxx.11.254:33436 UDP TTL:1 TOS:0x0 ID:53101
Len: 20
02 01 00 00 97 BA EA 38 4C 24 02 00              .......8L$..

04/04-23:01:27.142757 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:50681 -> xxx.xxx.11.254:33437 UDP TTL:1 TOS:0x0 ID:53102
Len: 20
03 01 00 00 97 BA EA 38 84 2D 02 00              .......8.-..


04/04-23:01:27.146662 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:50681 -> xxx.xxx.11.254:33438 UDP TTL:2 TOS:0x0 ID:53103
Len: 20
04 02 00 00 97 BA EA 38 C6 3C 02 00              .......8.<..

04/04-23:01:27.209127 0:10:4B:9F:3:47 -> 0:E0:D0:11:55:2D type:0x800 len:0x36
yyy.yyy.228.97:50681 -> xxx.xxx.11.254:33439 UDP TTL:2 TOS:0x0 ID:53105
Len: 20
05 02 00 00 97 BA EA 38 C4 30 03 00              .......8.0..
```

MORE OF THE SAME TYPE OF FRAMES

Summary:

This is the result of a traceroute too xxx.xxx.11.254. This was indicated by the incrementing of the TTL counter by 1 for each set (3 frames) of frames. It seems that SuSe increases the UDP port number as well as the TTL count. I confirmed this by having the employee redo the traceroute to the target host.

#5

This trace was sent to my by GIAC.

4/15/00
10:50:38AM

Source IP Address: XXX.XXX.185.98

From Port	Priority	Date		To	To Port	Event
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.1	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.2	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.3	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.4	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.5	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.6	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.7	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.8	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.9	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.10	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.11	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.12	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.13	31337	BackOrifice
31338	High	4/15/00	7:39:26AM	yyy.yyy.183.14	31337	BackOrifice

This is a recon attack. The attacker is scanning looking for BackOrifice. This attacker is scanning the entire subnet using an automated process. This is evident because the source port remains the same through the entire attack and the frames are very close together. Even though this is only a scan and in itself is not mischievous this IP address bears watching.

#6

This trace was sent to me by GIAC

Source IP Report **Generated:**
4/13/00
7:15:09AM

Source IP Address: xxx.xxx.193.25

From Port	Priority	Date		To	To Port	Event
109	High	4/13/00	2:01:08AM	yyy.yyy.42.1	109	IPHalfScan
110	High	4/13/00	2:01:08AM	yyy.yyy.42.1	110	IPHalfScan
109	High	4/13/00	2:01:08AM	yyy.yyy.42.2	109	IPHalfScan
110	High	4/13/00	2:01:08AM	yyy.yyy.42.2	110	IPHalfScan
109	High	4/13/00	2:01:08AM	yyy.yyy.42.3	109	IPHalfScan
110	High	4/13/00	2:01:08AM	yyy.yyy.42.3	110	IPHalfScan
109	High	4/13/00	2:01:08AM	yyy.yyy.42.4	109	IPHalfScan
110	High	4/13/00	2:01:08AM	yyy.yyy.42.4	110	IPHalfScan
109	High	4/13/00	2:01:08AM	yyy.yyy.42.5	109	IPHalfScan
110	High	4/13/00	2:01:08AM	yyy.yyy.42.5	110	IPHalfScan

This scan continues through the entire subnet in the same manner.

I am not familiar with the event IPHalfScan I can only assume that this means that the handshake between the two devices is not completed. This attacker is doing recon by scanning the entire subnet for POP2 (port 109) and POP3 (port 110) servers. There is a CERT advisory (CA-98.08) for older POP servers that maybe vulnerable to buffer overflows. The attacker my also be looking for a mail server that he can bounce e-mail off (e-mail relay). My suggestions for this targeted site would to make sure all-POP servers are at the current REV. of software and that all security patches are installed and tested. I believe that although this attack is not malicious in nature now, because it's only a scan, it does

warrant further monitoring of the source IP address. I can only assume that if the attacker is looking for POP servers in this manner he plans on doing something other then sending e-mail to a friend.

#7

This trace was sent to me by GIAC

Destination IP Report Generated: 4/15/00 4:52:06PM

Destination IP Address: **xxx.xxx.7.0**

To Port	Priority	Date	From	From Port	Event	
0	High	4/12/00 1:08:09AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:08:21AM	yyy.yyy.121.196	0	PingFlood	
	High	4/12/00 1:08:34AM	yyy.yyy.121.196	0	PingFlood	pattern between frames range from 11 to
0	High	4/12/00 1:08:44AM	yyy.yyy.121.196	0	PingFlood	24 sec.
0	High	4/12/00 1:08:55AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:09:19AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:09:31AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:09:44AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:09:56AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:10:19AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:10:30AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:10:41AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:10:53AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/12/00 1:11:06AM	yyy.yyy.121.196	0	PingFlood	
0	High	4/13/00 11:51:05AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:08AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:11AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:18AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:21AM	yyy.yyy.30.10	0	PingFlood	Pattern bwteen Frames 3 secs
0	High	4/13/00 11:51:24AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:27AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:30AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:33AM	yyy.yyy 30.10	0	PingFlood	
0	High	4/13/00 11:51:36AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:39AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:42AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:45AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:48AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:51AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:54AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:51:57AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:52:00AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:52:06AM	yyy.yyy.30.10	0	PingFlood	
0	High	4/13/00 11:52:26AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:29AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:32AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:35AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:38AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:41AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:44AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:47AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:50AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:52AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:55AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:52:58AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:53:01AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:53:04AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:53:07AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:53:10AM	yyy.yyy.161.226	0	PingFlood	
0	High	4/13/00 11:53:13AM	yyy.yyy.161.226	0	PingFlood	

0		High	4/13/00	11:53:15AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:18AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:21AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:27AM	yyy.yyy 161.226	0	PingFlood
0		High	4/13/00	11:53:30AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:33AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:36AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:39AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:42AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:45AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:48AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:50AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:53AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:56AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:53:59AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:02AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:05AM	yyy.yyy 161.226	0	PingFlood
0		High	4/13/00	11:54:09AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:12AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:15AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:18AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:21AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:23AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:29AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:32AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:35AM	yyy.yyy 161.226	0	PingFlood
0		High	4/13/00	11:54:38AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:42AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:44AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:47AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:51AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:54AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:54:57AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:00AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:03AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:05AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:08AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:11AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:14AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:17AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:20AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:24AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:26AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:32AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:35AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:38AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:41AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:45AM	yyy.yyy.161.226	0	PingFlood
0		High	4/13/00	11:55:48AM	yyy.yyy.161.226	0	PingFlood----------
0		High	4/13/00	12:03:11PM	yyy.yyy 30.10	0	PingFlood
0		High	4/13/00	12:03:15PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:19PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:23PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:27PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:32PM	yyy.yyy.30.10	0	PingFlood Pattern between frames 4 secs
0		High	4/13/00	12:03:36PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:41PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:45PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:50PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:55PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:03:59PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:04:03PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:04:12PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:04:16PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:04:21PM	yyy.yyy.30.10	0	PingFlood
0		High	4/13/00	12:04:25PM	yyy.yyy.30.10	0	PingFlood

0	High	4/13/00	12:04:29PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:34PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:38PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:42PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:47PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:52PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:04:57PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:02PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:06PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:15PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:19PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:23PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:28PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:33PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:37PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:42PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:46PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:51PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:05:55PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:00PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:04PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:08PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:17PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:21PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:25PM	yyy.yyy 30.10	0	PingFlood
0	High	4/13/00	12:06:30PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:34PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:38PM	yyy.yyy.30.10	0	PingFlood
0	High	4/13/00	12:06:43PM	yyy.yyy.30.10	0	PingFlood
0						
0	High	4/15/00	3:15:02AM	yyy.yyy.208.50	0	PingFlood_____
0	High	4/15/00	3:15:06AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:12AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:16AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:15:17AM	yyy.yyy.30.10	0	PingFlood pattern between frames for 208.50
0	High	4/15/00	3:15:23AM	yyy.yyy.30.10	0	PingFlood 10sec to 14 sec
0	High	4/15/00	3:15:26AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:15:30AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:37AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:15:42AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:47AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:48AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:15:53AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:15:59AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:16:05AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:16:11AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:16:12AM	yyy.yyy.208.50	0	PingFlood_____
0	High	4/15/00	3:31:50AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:31:56AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:00AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:32:02AM	yyy.yyy .30.10	0	PingFlood
0	High	4/15/00	3:32:08AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:14AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:32:19AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:25AM	yyy.yyy.208.50	0	PingFlood
0	High	4/15/00	3:32:26AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:31AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:36AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:32:42AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:34:25AM	yyy.yyy.240.176	0	PingFlood pattern between frames for 240.176
0	High	4/15/00	3:34:29AM	yyy.yyy.30.10	0	PingFlood 9 to 10 sec
0	High	4/15/00	3:34:34AM	yyy.yyy.240.176	0	PingFlood
0	High	4/15/00	3:34:36AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:34:41AM	yyy.yyy.30.10	0	PingFlood

0	High	4/15/00	3:34:44AM	yyy.yyy.240.176	0	PingFlood
0	High	4/15/00	3:34:47AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:34:53AM	yyy.yyy.30.10	0	PingFlood
0	High	4/15/00	3:34:55AM	yyy.yyy.240.176	0	PingFlood

Total Event Count: **38,553**

Summary:

This trace shows the presence of multiple attackers using different automated processes, but it does not appear to be a DDOS. The time frames between IP frames of each attacker are relatively constant, however the attackers are using different intervals between there own frames. This automated process is using crafted packets. Source port and destination ports are set to 0, because of this and the type of attack I would guess that the source addresses are spoofed. This appears to be a denial of service attack, however the effectiveness of the process they are using is in question. This is a class B address, if the target is just a host within this class B then this would not be a very effective approach to a DOS. The frames are too far apart and depending on the type of system the target was it my not even know its being targeted. On the other hand if the target is a subnet within the class B address then this would be an some what effective DOS. If the routers were to pass this broadcast to all of the nodes on this subnet, all would reply, but still this my not completely shut of access to the subnet even 3 second (the fastest that I've seen) is a long time network wise.

Its unclear to me why this attacks has such a long period between frames. This maybe because the attacker is pinging more then one site and its taken this long to get back around to this target. I would suggest to the target site to make sure his/hers routers are not passing sub-net broadcasts and to block this IP address and any inbound ping requests other then ones that are trusted.

#8

This is part of a Snort trace that was sent to me by GIAC

4/07-23:03:39.038251 MY.NET.97.109:1047 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:03:40.878260 MY.NET.97.109:1048 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:04:41.073975 MY.NET.97.109:1049 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:05:43.123409 MY.NET.97.109:1054 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:05:44.993114 MY.NET.97.109:1055 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:06:47.047434 MY.NET.97.109:1057 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:07:48.905464 MY.NET.97.109:1059 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:08:52.323836 MY.NET.97.109:1061 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:09:52.842161 MY.NET.97.109:1062 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:09:54.628907 MY.NET.97.109:1063 -> MY.NET.101.192:161
[**] SNMP public access [**]
04/07-23:11:08.720583 MY.NET.97.109:1082 -> MY.NET.101.192:161
[**] SNMP public access [**]

Summary:
This appears to be a recon attack of the targets SNMP service. I would think that this is an automated attempt because there is no attempt to change the community string (public) over the course of the attack. Seeing that this attack showed up in the watch list I assume this source IP address has shown up before for this type or other types of attacks, because of this I would keep this IP address as part of my watch list. One thing to note, however is that the network position of the IP address given to me are both MY.NET. If I assume that these two IP address are within the same network than this maybe a false positive. This attack maybe the result of a mis-configured SNMP pulling device. I would suggest that if this address is within their own network to track it down and check it out, then change my watch list accordingly.

#9

```
3/24-22:14:49.945123 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:49.995437 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.103846 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.212387 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.290962 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.400374 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.401877 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.497033 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.498397 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.513334 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.526063 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.606741 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.617964 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:50.640456 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
[**] GIAC 000218 VA-CIRT port 34555 [**]
03/24-22:14:52.022045 XXX.XXX.72.2:25 -> MY.NET.253.24:34555
```

This is a trace of an attacker looking for the troj_trinoo (port 34555). The address MY.NET.253.24 seems to be the only target during this period. I would suggest that this host be virus scanned and checked for trojans. This attacker my know something that we don't.
This is a targeted attack, and malicious in nature, I would suggest that these IP addresses be watched closely. The attack is automated in nature, intervals between frames are very close. It appears that the source address is trying to get by a firewall or ACL by using the well-known port number (25) for SMTP.

#10

```
04/07-01:19:19.639994 159.226.63.200:25 -> MY.NET.253.53:63607
[**] Watchlist 000222 NET-NCFC [**]
04/07-01:19:20.363474 159.226.63.200:25 -> MY.NET.253.53:63607
[**] Watchlist 000222 NET-NCFC [**]
04/07-01:19:21.130108 159.226.63.200:25 -> MY.NET.253.53:63607
04/07-01:27:50.884175 159.226.63.200:25 -> MY.NET.253.53:63635
[**] Watchlist 000222 NET-NCFC [**]
04/07-01:27:53.976445 159.226.63.200:25 -> MY.NET.253.53:63635
 [**] Watchlist 000222 NET-NCFC [**]
04/07-01:54:53.157845 159.226.63.200:25 -> MY.NET.253.53:63734
[**] Watchlist 000222 NET-NCFC [**]
04/07-01:54:53.157956 159.226.63.200:25 -> MY.NET.253.53:63734
04/07-02:19:19.106024 159.226.63.200:25 -> MY.NET.253.53:63838
04/07-02:26:06.504295 159.226.63.200:25 -> MY.NET.253.53:63838
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:26:07.238809 159.226.63.200:25 -> MY.NET.253.53:63838
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:28:19.746015 159.226.63.200:25 -> MY.NET.253.53:63867
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:28:20.150176 159.226.63.200:25 -> MY.NET.253.53:63867
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:28:21.320000 159.226.63.200:25 -> MY.NET.253.53:63867
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:49:18.908847 159.226.63.200:25 -> MY.NET.253.53:63932
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:49:20.337642 159.226.63.200:25 -> MY.NET.253.53:63932
```

```
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:56:06.280048 159.226.63.200:25 -> MY.NET.253.53:63932
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:57:52.365788 159.226.63.200:25 -> MY.NET.253.53:63953
[**] Watchlist 000222 NET-NCFC [**]
04/07-02:57:53.888370 159.226.63.200:25 -> MY.NET.253.53:63953
[**] Watchlist 000222 NET-NCFC [**]
04/07-03:04:40.629737 159.226.63.200:25 -> MY.NET.253.53:63953
[**] Watchlist 000222 NET-NCFC [**]
04/07-03:19:17.192949 159.226.63.200:25 -> MY.NET.253.53:64018
04/07-04:08:04.788540 159.226.63.200:25 -> MY.NET.253.53:64082
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:09:06.492723 159.226.63.200:25 -> MY.NET.253.53:64096
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:09:09.973460 159.226.63.200:25 -> MY.NET.253.53:64096
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:11:15.240733 159.226.63.200:1172 -> MY.NET.253.53:113
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:14:35.913477 159.226.63.200:25 -> MY.NET.253.53:64096
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:15:17.385138 159.226.63.200:25 -> MY.NET.100.230:37977
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:15:17.387149 159.226.63.200:25 -> MY.NET.100.230:37977
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:15:18.234433 159.226.63.200:25 -> MY.NET.100.230:37977
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:18:11.724966 159.226.63.200:25 -> MY.NET.253.53:64099
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:20:00.685006 159.226.63.200:25 -> MY.NET.253.53:64082
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:20:00.685073 159.226.63.200:25 -> MY.NET.253.53:64082
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:20:00.685193 159.226.63.200:25 -> MY.NET.253.53:64082
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:21:31.170994 159.226.63.200:25 -> MY.NET.100.230:3
04/07-04:45:02.849220 159.226.63.200:25 -> MY.NET.253.53:64158
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:45:03.730684 159.226.63.200:25 -> MY.NET.253.53:64158
[**] Watchlist 000222 NET-NCFC [**]
04/07-04:45:04.502108 159.226.63.200:25 -> MY.NET.253.53:64158
[**] WinGate 8080 Attempt [**]
04/07-06:33:10.727763 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:13.772514 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:14.481356 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:17.282749 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:18.035964 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:18.733937 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:18.734024 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:30.943393 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:30.944915 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:30.944968 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-06:33:31.711193 159.226.63.200:25 -> MY.NET.253.53:64318
04/07-06:44:40.424206 159.226.63.200:25 -> MY.NET.253.53:64318
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:45.924506 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:33:52.242544 159.226.63.200:1983 -> MY.NET.100.230:113
```

```
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:52.899917 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:53.316122 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:53.561155 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:53.561249 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:54.240138 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:54.905347 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:32:59.909662 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-07:33:01.295542 159.226.63.200:25 -> MY.NET.100.230:38985
04/07-07:39:02.624250 159.226.63.200:25 -> MY.NET.100.230:38985
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:21:56.427944 159.226.63.200:1686 -> MY.NET.100.230:113
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:21:57.193461 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:21:57.543247 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:21:57.853301 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:21:58.534923 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:22:04.407264 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:22:08.816944 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:22:11.157922 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:22:11.252886 159.226.63.200:25 -> MY.NET.100.230:39409
04/07-08:28:11.948026 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:28:11.948324 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:28:11.948585 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:28:12.624168 159.226.63.200:25 -> MY.NET.100.230:39409
[**] Watchlist 000222 NET-NCFC [**]
04/07-08:28:13.881270 159.226.63.200:25 -> MY.NET.100.230:39409
```

Summary:

This appears to be a recon attack on these devices. The attacker is using an automated process to systematically attack these hosts to gain information about the hosts. Each host is scanned for a number of upper TCP or UDP ports. It's hard telling from this trace if these are TCP or UDP ports (the source port of the attacker port 25 can be either UDP or TCP). The only port that I am sure of is port 113, which is a TCP authentication port. Each port is scanned a multiple number of times, this maybe because some of these are UDP frames and are not reliable enough for the attacker. By sending multiple packets at least one should get through.

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 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 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 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
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced