Global Information Assurance Certification Paper

GIAC Intrusion Detection Practical Assignment for SANS Security DC 2000

by Al Evans

Assignment 1- Network Detects

Detect 1

```
-*> 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)

08/09-11:16:01.351038 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:38174  DF
*****PA* Seq: 0x1030D   Ack: 0x12E2E   Win: 0x2110
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 06 22 FF 00 67 00 00 09 08 01 00 00 00  ..@."..g........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.351844 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:31500  DF
*****PA* Seq: 0x12DC6   Ack: 0x1030D   Win: 0x2211
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 06 18 FF 00 00 00 00 0E 00 06 00 00 00  ..@.............
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
02 00 00 00 01 11 00 FB 5C 00 73 00 72 00 76 00  ........\.s.r.v.
73 00 76 00 63 00 00 00                          s.v.c...

08/09-11:16:01.356406 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:38430  DF
*****PA* Seq: 0x10378   Ack: 0x12ECE   Win: 0x2070
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 06 0A 00 00 44 00 00 00 00 00 38 00 00  .......D.....8..
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 00 00 00 00 30 16 30 16  ....D.......0.0.
05 AB 00 00 0D 00 5C 50 49 50 45 5C 6E 74 73 76  ......\PIPE\ntsv
63 73 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  cs...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.356927 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:31756  DF
*****PA* Seq: 0x12E2E   Ack: 0x10378   Win: 0x21A6
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
```

```
02 08 80 06 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 09 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 00 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
01 00 00 00 00 00 01 00 C8 4F 32 4B 70 16 D3 01  .........O2Kp...
12 78 5A 47 BF 6E E1 88 03 00 00 00 04 5D 88 8A  .xZG.n.......]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.360356 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:38686  DF
*****PA* Seq: 0x103F8   Ack: 0x12F62   Win: 0x1FDC
00 00 00 A0 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 06 0A 00 00 68 00 00 00 00 00 38 00 00  .......h.....8..
00 68 00 38 00 00 00 00 00 69 00 3C 05 00 02 03  .h.8.....i.<....
10 00 00 00 68 00 00 00 01 00 00 00 50 00 00 00  ....h.......P...
00 00 00 00 65 00 00 00 38 04 18 00 F4 01 00 00  ....e...8.......
50 04 18 00 04 00 00 00 00 00 00 00 03 90 01 00  P...............
5E 04 18 00 07 00 00 00 00 00 00 00 07 00 00 00  ^...............
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00 44 00  D.o.n.a.l.d...D.
01 00 00 00 00 00 00 00 01 00 00 00 00 00 62 00  ..............b.
00 00 00 00                                      ....

08/09-11:16:01.360946 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:32012  DF
*****PA* Seq: 0x12ECE   Ack: 0x103F8   Win: 0x2126
00 00 00 90 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 06 10 00 00 3C 00 00 00 00 00 04 00 00  .......<........
00 00 00 00 00 00 00 00 00 54 00 3C 00 54 00 02  .........T.<.T..
00 26 00 09 08 4D 00 00 5C 00 50 00 49 00 50 00  .&...M..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
3C 00 00 00 01 00 00 00 24 00 00 00 00 00 15 00  <.......$.......
92 0E 92 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00 88 8A  D.o.n.a.l.d.....
65 00 00 00                                      e...

08/09-11:16:01.364001 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:38942  DF
*****PA* Seq: 0x1049C   Ack: 0x12F90   Win: 0x1FAE
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 00 07 00 00 00                             .......

08/09-11:16:01.364513 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:32268  DF
*****PA* Seq: 0x12F62   Ack: 0x1049C   Win: 0x2082
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 00 07 03 09 08 FF FF FF FF 00 00 38        .............8

08/09-11:16:01.372143 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:39198  DF
*****PA* Seq: 0x104C3   Ack: 0x12FF8   Win: 0x1F46
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
```

```
02 08 40 07 22 FF 00 67 00 00 0A 08 01 00 00 00  ..@."..g........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.372514 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:32524  DF
*****PA* Seq: 0x12F90   Ack: 0x104C3   Win: 0x205B
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 07 18 FF 00 00 00 00 0E 00 06 00 00 00  ..@.............
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
01 00 00 00 01 11 00 FB 5C 00 77 00 6B 00 73 00  ........\.w.k.s.
73 00 76 00 63 00 00 00                          s.v.c...

08/09-11:16:01.375492 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:39454  DF
*****PA* Seq: 0x1052E   Ack: 0x13098   Win: 0x1EA6
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 07 0A 00 00 44 00 00 00 00 00 38 00 00  .......D.....8..
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 01 00 00 00 30 16 30 16  ....D.......0.0.
06 AB 00 00 0D 00 5C 50 49 50 45 5C 6E 74 73 76  ......\PIPE\ntsv
63 73 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  cs...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.375837 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:32780  DF
*****PA* Seq: 0x12FF8   Ack: 0x1052E   Win: 0x1FF0
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 07 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 0A 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 01 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
01 00 00 00 00 00 01 00 98 D0 FF 6B 12 A1 10 36  ...........k...6
98 33 46 C3 F8 7E 34 5A 01 00 00 00 04 5D 88 8A  .3F..~4Z.....]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.378855 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:39710  DF
*****PA* Seq: 0x105AE   Ack: 0x1312C   Win: 0x1E12
00 00 00 BC FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 07 0A 00 00 84 00 00 00 00 00 38 00 00  .............8..
00 84 00 38 00 00 00 00 00 85 00 3C 05 00 02 03  ...8.......<....
10 00 00 00 84 00 00 00 01 00 00 00 6C 00 00 00  ............l...
00 00 00 00 65 00 00 00 70 10 15 00 F4 01 00 00  ....e...p.......
96 10 15 00 88 10 15 00 04 00 00 00 00 00 00 00  ................
A4 10 15 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 4F 00 4E 00 41 00 4C 00 44 00 00 00 44 00  D.O.N.A.L.D...D.
07 00 00 00 00 00 00 00 00 07 00 00 00 44 00 49 00  ............D.I.
53 00 4E 00 45 00 59 00 00 00 6B 00 01 00 00 00  S.N.E.Y...k.....
```

```
00 00 00 00 01 00 00 00 00 00 4E 41 00 00 00 00  ..........NA....

08/09-11:16:01.379206 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:33036  DF
*****PA* Seq: 0x13098   Ack: 0x105AE   Win: 0x1F70
00 00 00 90 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 07 10 00 00 3C 00 00 00 00 04 00 00 00  .......<........
00 00 00 00 00 00 00 00 00 54 00 3C 00 54 00 02  .........T.<.T..
00 26 00 0A 08 4D 00 00 5C 00 50 00 49 00 50 00  .&...M..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
3C 00 00 00 01 00 00 00 24 00 00 00 00 00 00 00  <.......$.......
92 0E 92 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00 88 8A  D.o.n.a.l.d.....
65 00 00 00                                      e...

08/09-11:16:01.382142 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:39966  DF
*****PA* Seq: 0x1066E   Ack: 0x1315A   Win: 0x1DE4
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 00 08 00 00 00                             .......

08/09-11:16:01.382401 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:33292  DF
*****PA* Seq: 0x1312C   Ack: 0x1066E   Win: 0x1EB0
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 00 08 03 0A 08 FF FF FF FF 00 00 38        ............8

08/09-11:16:01.403886 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:40222  DF
*****PA* Seq: 0x10695   Ack: 0x131C2   Win: 0x1D7C
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 08 22 FF 00 67 00 00 0B 08 01 00 00 00  ..@."..g........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.404509 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:33548  DF
*****PA* Seq: 0x1315A   Ack: 0x10695   Win: 0x1E89
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 08 18 FF 00 00 00 00 0E 00 06 00 00 00  ..@.............
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
02 00 00 00 00 11 00 FB 5C 00 77 00 69 00 6E 00  ........\.w.i.n.
72 00 65 00 67 00 00 00                          r.e.g...

08/09-11:16:01.420513 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:40478  DF
*****PA* Seq: 0x10700   Ack: 0x13262   Win: 0x1CDC
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
```

```
02 08 80 08 0A 00 00 44 00 00 00 00 00 38 00 00  .......D.....8..
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 00 00 00 00 30 16 30 16  ....D.......0.0.
A3 9E 00 00 0D 00 5C 50 49 50 45 5C 77 69 6E 72  ......\PIPE\winr
65 67 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  eg...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.421245 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:33804  DF
*****PA* Seq: 0x131C2   Ack: 0x10700   Win: 0x1E1E
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 08 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 0B 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 00 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
01 00 00 00 00 00 01 00 01 D0 8C 33 44 22 F1 31  ...........3D".1
AA AA 90 00 38 00 10 03 01 00 00 00 04 5D 88 8A  ....8........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.430715 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:40734  DF
*****PA* Seq: 0x10780   Ack: 0x132DE   Win: 0x2238
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 08 0A 00 00 30 00 00 00 00 00 00 38 00 00  .......0.....8..
00 30 00 38 00 00 00 00 00 31 00 24 05 00 02 03  .0.8.....1.$....
10 00 00 00 30 00 00 00 01 00 00 00 18 00 00 00  ....0...........
00 00 00 00 00 00 00 00 EC 2A 33 1E 4D 6D D4 11  .........*3.Mm..
B3 2F 00 A0 24 00 CA EF 00 00 00 00               ./..$.......

08/09-11:16:01.431426 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:34060  DF
*****PA* Seq: 0x13262   Ack: 0x10780   Win: 0x1D9E
00 00 00 78 FF 53 4D 42 25 00 00 00 00 18 03 80  ...x.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 08 10 00 00 24 00 00 00 00 04 00 00 00  .......$........
00 00 00 00 00 00 00 00 00 54 00 24 00 54 00 02  .........T.$.T..
00 26 00 0B 08 35 00 00 5C 00 50 00 49 00 50 00  .&...5..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
24 00 00 00 01 00 00 00 0C 00 00 00 00 00 02 00  $...............
B8 B1 12 00 18 41 01 00 00 00 00 02               .....A......

08/09-11:16:01.435566 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:40990  DF
*****PA* Seq: 0x107EC   Ack: 0x133DA   Win: 0x213C
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 09 0A 00 00 30 00 00 00 00 00 00 38 00 00  .......0.....8..
00 30 00 38 00 00 00 00 00 31 00 A4 05 00 02 03  .0.8.....1......
10 00 00 00 30 00 00 00 02 00 00 00 18 00 00 00  ....0...........
00 00 00 00 00 00 00 00 ED 2A 33 1E 4D 6D D4 11  .........*3.Mm..
B3 2F 00 A0 24 00 CA EF 00 00 00 00               ./..$.......

08/09-11:16:01.436050 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:34316  DF
```

```
*****PA* Seq: 0x132DE   Ack: 0x107EC   Win: 0x1D32
00 00 00 F8 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 09 10 00 00 A4 00 00 00 00 04 00 00 00  ................
00 00 00 00 00 00 00 00 00 54 00 A4 00 54 00 02  .........T...T..
00 26 00 0B 08 B5 00 00 5C 00 50 00 49 00 50 00  .&......\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
A4 00 00 00 02 00 00 00 8C 00 00 00 00 00 0F 00  ................
00 00 00 00 EC 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 5A 00 5A 00 B4 DA 42 00 2D 00 00 00  $...Z.Z...B.-...
00 00 00 00 2D 00 00 00 53 00 6F 00 66 00 74 00  ....-...S.o.f.t.
77 00 61 00 72 00 65 00 5C 00 4D 00 69 00 63 00  w.a.r.e.\.M.i.c.
72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00  r.o.s.o.f.t.\.W.
69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4E 00  i.n.d.o.w.s. .N.
54 00 5C 00 43 00 75 00 72 00 72 00 65 00 6E 00  T.\.C.u.r.r.e.n.
74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00  t.V.e.r.s.i.o.n.
00 00 00 00 00 00 00 00 01 00 00 00              ............

08/09-11:16:01.439680 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:41246  DF
*****PA* Seq: 0x10858   Ack: 0x134B2   Win: 0x2064
00 00 00 9C FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 09 0A 00 00 64 00 00 00 00 00 00 38 00 00  ..@....d.....8..
00 64 00 38 00 00 00 00 00 65 00 80 05 00 02 03  .d.8.....e......
10 00 00 00 64 00 00 00 03 00 00 00 4C 00 00 00  ....d.......L...
00 00 00 00 0C C3 14 00 01 00 00 00 88 A1 14 00  ................
1E 00 00 00 00 00 00 00 1E 00 00 00 53 00 65 00  ............S.e.
72 00 76 00 69 00 63 00 65 00 20 00 50 00 61 00  r.v.i.c.e. .P.a.
63 00 6B 00 20 00 34 00 00 00 5F 7F 24 C3 14 00  c.k. .4..._.$...
1E 00 00 00 2C C3 14 00 1E 00 00 00 00 00 00 00  ....,...........

08/09-11:16:01.440271 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:34572  DF
*****PA* Seq: 0x133DA   Ack: 0x10858   Win: 0x1CC6
00 00 00 D4 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 09 10 00 00 80 00 00 00 00 04 00 00 00  ..@.............
00 00 00 00 00 00 00 00 00 54 00 80 00 54 00 02  .........T...T..
00 26 00 0B 08 91 00 00 5C 00 50 00 49 00 50 00  .&......\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
80 00 00 00 03 00 00 00 68 00 00 00 00 00 11 00  ........h.......
00 00 00 00 ED 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 16 00 16 00 74 DA 42 00 0B 00 00 00  $.......t.B.....
00 00 00 00 0B 00 00 00 43 00 53 00 44 00 56 00  ........C.S.D.V.
65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 63 00  e.r.s.i.o.n...c.
C4 B1 12 00 5A 00 5A 00 74 FA 12 00 08 02 00 00  ....Z.Z.t.......
00 00 00 00 00 00 00 00 C8 B1 12 00 08 02 00 00  ................
C0 B1 12 00 00 00 00 00                          ........

08/09-11:16:01.443309 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:41502  DF
*****PA* Seq: 0x108F8   Ack: 0x13536   Win: 0x1FE0
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 09 0A 00 00 30 00 00 00 00 00 00 38 00 00  .......0.....8..
00 30 00 38 00 00 00 00 00 31 00 2C 05 00 02 03  .0.8.....1.,....
```

```
10 00 00 00 30 00 00 00 04 00 00 00 18 00 00 00  ....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              ............

08/09-11:16:01.443653 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:34828  DF
*****PA* Seq: 0x134B2   Ack: 0x108F8   Win: 0x2238
00 00 00 80 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 09 10 00 00 2C 00 00 00 00 04 00 00 00  .......,........
00 00 00 00 00 00 00 00 00 54 00 2C 00 54 00 02  .........T.,.T..
00 26 00 0B 08 3D 00 00 5C 00 50 00 49 00 50 00  .&...=..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
2C 00 00 00 04 00 00 00 14 00 00 00 00 00 05 00  ,...............
00 00 00 00 EC 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF                                      $...

08/09-11:16:01.448228 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:41758  DF
*****PA* Seq: 0x10964   Ack: 0x135B2   Win: 0x1F64
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 09 0A 00 00 30 00 00 00 00 00 00 38 00  .......0.....8..
00 30 00 38 00 00 00 00 00 00 31 00 24 05 00 02  .0.8.....1.$....
10 00 00 00 30 00 00 00 05 00 00 00 18 00 00 00  ....0...........
00 00 00 00 00 00 00 00 EE 2A 33 1E 4D 6D D4 11  .........*3.Mm..
B3 2F 00 A0 24 00 CA EF 00 00 00 00              ./..$.......

08/09-11:16:01.448587 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:35084  DF
*****PA* Seq: 0x13536   Ack: 0x10964   Win: 0x21CC
00 00 00 78 FF 53 4D 42 25 00 00 00 00 18 03 80  ...x.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 09 10 00 00 24 00 00 00 00 04 00 00 00  .......$........
00 00 00 00 00 00 00 00 00 54 00 24 00 54 00 02  .........T.$.T..
00 26 00 0B 08 35 00 00 5C 00 50 00 49 00 50 00  .&...5..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
24 00 00 00 05 00 00 00 0C 00 00 00 00 00 02 00  $...............
B8 B1 12 00 98 4B 33 1E 00 00 00 02              .....K3.....

08/09-11:16:01.452010 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:42014  DF
*****PA* Seq: 0x109D0   Ack: 0x136BA   Win: 0x1E5C
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0A 0A 00 00 30 00 00 00 00 00 00 38 00  .......0.....8..
00 30 00 38 00 00 00 00 00 00 31 00 B0 05 00 02  .0.8.....1......
10 00 00 00 30 00 00 00 06 00 00 00 18 00 00 00  ....0...........
00 00 00 00 00 00 00 00 EF 2A 33 1E 4D 6D D4 11  .........*3.Mm..
B3 2F 00 A0 24 00 CA EF 00 00 00 00              ./..$.......

08/09-11:16:01.452359 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:35340  DF
*****PA* Seq: 0x135B2   Ack: 0x109D0   Win: 0x2160
00 00 01 04 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0A 10 00 00 B0 00 00 00 00 04 00 00 00  ................
```

```
00 00 00 00 00 00 00 00 00 54 00 B0 00 54 00 02  .........T...T..
00 26 00 0B 08 C1 00 00 5C 00 50 00 49 00 50 00  .&......\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
B0 00 00 00 06 00 00 00 98 00 00 00 00 00 0F 00  ................
00 00 00 00 EE 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 68 00 68 00 E0 D8 42 00 34 00 00 00  $...h.h...B.4...
00 00 00 00 34 00 00 00 53 00 6F 00 66 00 74 00  ....4...S.o.f.t.
77 00 61 00 72 00 65 00 5C 00 4D 00 69 00 63 00  w.a.r.e.\.M.i.c.
72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00  r.o.s.o.f.t.\.W.
69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4E 00  i.n.d.o.w.s. .N.
54 00 5C 00 43 00 75 00 72 00 72 00 65 00 6E 00  T.\.C.u.r.r.e.n.
74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00  t.V.e.r.s.i.o.n.
5C 00 48 00 6F 00 74 00 66 00 69 00 78 00 00 00  \.H.o.t.f.i.x...
00 00 00 00 08 00 00 00                          ........

08/09-11:16:01.455558 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:42270  DF
*****PA* Seq: 0x10A3C   Ack: 0x1376E   Win: 0x1DA8
00 00 00 90 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0A 0A 00 00 58 00 00 00 00 00 00 38 00  ..@....X.....8..
00 58 00 38 00 00 00 00 00 59 00 5C 05 00 02 03  .X.8.....Y.\....
10 00 00 00 58 00 00 00 07 00 00 00 40 00 00 00  ....X.......@...
00 00 00 00 10 00 00 10 00 D0 14 00 00 08 00 00  ................
00 00 00 00 08 00 00 00 51 00 31 00 34 00 37 00  ........Q.1.4.7.
32 00 32 00 32 00 00 00 F8 C2 14 00 00 00 00 00  2.2.2...........
00 00 00 00 04 C3 14 00 10 72 5F 7F 11 C7 BF 01  .........r_.....
00 00 00 00                                      ....

08/09-11:16:01.455923 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:35596  DF
*****PA* Seq: 0x136BA   Ack: 0x10A3C   Win: 0x20F4
00 00 00 B0 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0A 10 00 00 5C 00 00 00 00 04 00 00 00  ..@....\........
00 00 00 00 00 00 00 00 00 54 00 5C 00 54 00 02  .........T.\.T..
00 26 00 0B 08 6D 00 00 5C 00 50 00 49 00 50 00  .&...m..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
5C 00 00 00 07 00 00 00 44 00 00 00 00 00 09 00  \.......D.......
00 00 00 00 EF 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 00 00 00 00 00 00 00 10 70 F2 12 00  $...........p...
00 08 00 00 00 00 00 00 00 00 00 BC B1 12 00     ................
00 00 00 00 00 00 00 00 64 F2 12 00 CC CC CC CC  ........d.......
CC CC CC CC                                      ....

08/09-11:16:01.458800 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:42526  DF
*****PA* Seq: 0x10AD0   Ack: 0x13822   Win: 0x1CF4
00 00 00 90 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 0A 0A 00 00 58 00 00 00 00 00 00 38 00  .......X.....8..
00 58 00 38 00 00 00 00 00 59 00 5C 05 00 02 03  .X.8.....Y.\....
10 00 00 00 58 00 00 00 08 00 00 00 40 00 00 00  ....X.......@...
00 00 00 00 10 00 00 10 00 D0 14 00 00 08 00 00  ................
00 00 00 00 08 00 00 00 51 00 31 00 34 00 37 00  ........Q.1.4.7.
32 00 32 00 32 00 00 00 F8 C2 14 00 00 00 00 00  2.2.2...........
00 00 00 00 04 C3 14 00 10 72 5F 7F 11 C7 BF 01  .........r_.....
```

```
00 00 00 00                                          ....

08/09-11:16:01.459130 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:35852  DF
*****PA* Seq: 0x1376E   Ack: 0x10AD0   Win: 0x2060
00 00 00 B0 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 0A 10 00 00 5C 00 00 00 00 04 00 00 00  .......\........
00 00 00 00 00 00 00 00 00 54 00 5C 00 54 00 02  .........T.\.T..
00 26 00 0B 08 6D 00 00 5C 00 50 00 49 00 50 00  .&...m..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
5C 00 00 00 08 00 00 00 44 00 00 00 00 00 09 00  \.......D.......
00 00 00 00 EF 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 00 00 00 00 00 00 00 10 70 F2 12 00  $...........p...
00 08 00 00 00 00 00 00 00 00 00 00 BC B1 12 00  ................
00 00 00 00 00 00 00 00 64 F2 12 00 10 72 5F 7F  ........d....r_.
11 C7 BF 01                                      ....

08/09-11:16:01.462214 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:42782  DF
*****PA* Seq: 0x10B64   Ack: 0x138D2   Win: 0x2238
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0A 0A 00 00 30 00 00 00 00 00 00 38 00  .......0......8..
00 30 00 38 00 00 00 00 00 31 00 58 05 00 02 03  .0.8.....1.X....
10 00 00 00 30 00 00 00 09 00 00 00 18 00 00 00  ....0...........
00 00 00 00 00 00 00 00 F0 2A 33 1E 4D 6D D4 11  .........*3.Mm..
B3 2F 00 A0 24 00 CA EF 00 00 00 00              ./..$.......

08/09-11:16:01.462589 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:36108  DF
*****PA* Seq: 0x13822   Ack: 0x10B64   Win: 0x1FCC
00 00 00 AC FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0A 10 00 00 58 00 00 00 00 04 00 00 00  .......X........
00 00 00 00 00 00 00 00 00 54 00 58 00 54 00 02  .........T.X.T..
00 26 00 0B 08 69 00 00 5C 00 50 00 49 00 50 00  .&...i..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
58 00 00 00 09 00 00 00 40 00 00 00 00 00 0F 00  X.......@.......
00 00 00 00 EF 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 10 00 10 00 70 F2 12 00 08 00 00 00  $.......p.......
00 00 00 00 08 00 00 00 51 00 31 00 34 00 37 00  ........Q.1.4.7.
32 00 32 00 32 00 00 00 00 00 00 00 19 00 02 00  2.2.2...........

08/09-11:16:01.465874 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:43038  DF
*****PA* Seq: 0x10BD0   Ack: 0x139A6   Win: 0x2164
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0B 0A 00 00 44 00 00 00 00 00 00 38 00  .......D......8..
00 44 00 38 00 00 00 00 00 45 00 7C 05 00 02 03  .D.8.....E.|....
10 00 00 00 44 00 00 00 0A 00 00 00 2C 00 00 00  ....D.......,...
00 00 00 00 08 C3 14 00 10 00 10 00 00 D0 14 00  ................
00 20 00 00 00 00 00 00 00 00 00 00 20 C3 14 00  . .......... ...
00 20 00 00 28 C3 14 00 00 00 00 00 02 00 00 00  . ..(...........

08/09-11:16:01.466231 devil.goodness.org:1079 -> server.goodness.org:139
```

```
TCP TTL:128 TOS:0xC ID:36364  DF
*****PA* Seq: 0x138D2   Ack: 0x10BD0   Win: 0x1F60
00 00 00 D0 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0B 10 00 00 7C 00 00 00 00 04 00 00 00  .......|........
00 00 00 00 00 00 00 00 00 54 00 7C 00 54 00 02  .........T.|.T..
00 26 00 0B 08 8D 00 00 5C 00 50 00 49 00 50 00  .&......\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
7C 00 00 00 0A 00 00 00 64 00 00 00 00 00 11 00  |.......d.......
00 00 00 00 F0 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 12 00 12 00 C8 D8 42 00 09 00 00 00  $.........B.....
00 00 00 00 09 00 00 00 43 00 6F 00 6D 00 6D 00  ........C.o.m.m.
65 00 6E 00 74 00 73 00 00 00 00 00 C4 B1 12 00  e.n.t.s.........
10 00 10 00 50 B2 12 00 00 20 00 00 00 00 00 00  ....P.... ......
00 00 00 00 C8 B1 12 00 00 20 00 00 C0 B1 12 00  ......... ......
00 00 00 00                                      ....

08/09-11:16:01.470451 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:43294  DF
*****PA* Seq: 0x10C50   Ack: 0x13A5A   Win: 0x20B0
00 00 00 80 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0B 0A 00 00 48 00 00 00 00 00 00 38 00  ..@....H......8..
00 48 00 38 00 00 00 00 00 00 49 00 5C 05 00 02  .H.8......I.\....
10 00 00 00 48 00 00 00 0B 00 00 00 30 00 00 00  ....H.......0...
00 00 00 00 00 00 00 00 10 00 D0 14 00 00 08 00  ................
00 00 00 00 00 00 00 00 00 F8 C2 14 00 00 00 00  ................
00 00 00 00 04 C3 14 00 10 72 5F 7F 11 C7 BF 01  .........r_.....
03 01 00 00                                      ....

08/09-11:16:01.470791 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:36620  DF
*****PA* Seq: 0x139A6   Ack: 0x10C50   Win: 0x1EE0
00 00 00 B0 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0B 10 00 00 5C 00 00 00 00 04 00 00 00  ..@....\........
00 00 00 00 00 00 00 00 00 54 00 5C 00 54 00 02  .........T.\.T..
00 26 00 0B 08 6D 00 00 5C 00 50 00 49 00 50 00  .&...m..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 00 03 10 00 00 00  E.\.............
5C 00 00 00 0B 00 00 00 44 00 00 00 00 00 09 00  \.......D.......
00 00 00 00 EF 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm.../..
24 00 CA EF 01 00 00 00 00 00 00 10 70 F2 12 00  $...........p...
00 08 00 00 00 00 00 00 00 00 00 00 BC B1 12 00  ................
00 00 00 00 00 00 00 00 64 F2 12 00 10 72 5F 7F  ........d....r_.
11 C7 BF 01                                      ....

08/09-11:16:01.473720 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:43550  DF
*****PA* Seq: 0x10CD4   Ack: 0x13ADE   Win: 0x202C
00 00 00 68 FF 53 4D 42 25 00 00 00 00 98 03 80  ...h.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 0B 0A 00 00 30 00 00 00 00 00 00 38 00  .......0......8..
00 30 00 38 00 00 00 00 00 00 31 00 2C 05 00 02  .0.8......1.,....
10 00 00 00 30 00 00 00 0C 00 00 00 18 00 00 00  ....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              ............
```

```
08/09-11:16:01.474062 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:36876  DF
*****PA* Seq: 0x13A5A   Ack: 0x10CD4   Win: 0x1E5C
00 00 00 80 FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 80 0B 10 00 00 2C 00 00 00 00 04 00 00 00  .......,........
00 00 00 00 00 00 00 00 00 54 00 2C 00 54 00 02  .........T.,.T..
00 26 00 0B 08 3D 00 00 5C 00 50 00 49 00 50 00  .&...=..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
2C 00 00 00 0C 00 00 00 14 00 00 00 00 00 05 00  ,...............
00 00 00 00 EE 2A 33 1E 4D 6D D4 11 B3 2F 00 A0  .....*3.Mm../..
24 00 CA EF                                      $...

08/09-11:16:01.481210 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:43806  DF
*****PA* Seq: 0x10D40   Ack: 0x13B46   Win: 0x1FC4
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0B 22 FF 00 67 00 00 0C 08 01 00 00 00  ....".."g.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.481545 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:37132  DF
*****PA* Seq: 0x13ADE   Ack: 0x10D40   Win: 0x1DF0
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0B 18 FF 00 00 00 00 0E 00 06 00 00 00  ................
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
02 00 00 00 01 11 00 00 5C 00 73 00 72 00 76 00  ........\.s.r.v.
73 00 76 00 63 00 00 00                          s.v.c...

08/09-11:16:01.484470 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:44062  DF
*****PA* Seq: 0x10DAB   Ack: 0x13BE6   Win: 0x1F24
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0C 0A 00 00 44 00 00 00 00 00 38 00 00  .......D.....8..
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 00 00 00 00 30 16 30 16  ....D.......0.0.
07 AB 00 00 0D 00 5C 50 49 50 45 5C 6E 74 73 76  ......\PIPE\ntsv
63 73 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  cs...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.484836 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:37388  DF
*****PA* Seq: 0x13B46   Ack: 0x10DAB   Win: 0x1D85
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0C 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 0C 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 00 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
```

```
01 00 00 00 00 00 01 00 C8 4F 32 4B 70 16 D3 01  .........O2Kp...
12 78 5A 47 BF 6E E1 88 03 00 00 00 04 5D 88 8A  .xZG.n.......]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.488208 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:44318  DF
*****PA* Seq: 0x10E2B   Ack: 0x13C96   Win: 0x1E74
00 00 01 78 FF 53 4D 42 25 00 00 00 00 98 03 80  ...x.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0C 0A 00 00 40 01 00 00 00 00 38 00 00  ..@....@.....8..
00 40 01 38 00 00 00 00 00 41 01 58 05 00 02 03  .@.8.....A.X....
10 00 00 00 40 01 00 00 01 00 00 00 28 01 00 00  ....@.......(...
00 00 00 00 00 00 00 00 00 00 00 00 BC 07 18 00  ................
02 00 00 00 D8 FD 17 00 02 00 00 00 01 00 00 00  ................
AE FE 17 00 8E FE 17 00 06 00 00 00 94 FE 17 00  ................
00 00 00 00 64 FE 17 00 44 FE 17 00 06 00 00 00  ....d...D.......
4A FE 17 00 15 00 00 00 00 00 00 00 15 00 00 00  J...............
5C 00 44 00 65 00 76 00 69 00 63 00 65 00 5C 00  \.D.e.v.i.c.e.\.
4E 00 65 00 74 00 42 00 54 00 5F 00 45 00 6C 00  N.e.t.B.T._.E.l.
6E 00 6B 00 33 00 31 00 00 00 00 00 06 00 00 00  n.k.3.1.........
44 4F 4E 41 4C 44 34 00 0D 00 00 00 00 00 00 00  DONALD4.........
0D 00 00 00 30 00 30 00 61 00 30 00 32 00 34 00  ....0.0.a.0.2.4.
30 00 30 00 63 00 61 00 65 00 66 00 00 00 18 00  0.0.c.a.e.f.....
15 00 00 00 00 00 00 00 15 00 00 00 5C 00 44 00  ............\.D.
65 00 76 00 69 00 63 00 65 00 5C 00 4E 00 65 00  e.v.i.c.e.\.N.e.
74 00 42 00 54 00 5F 00 45 00 6C 00 6E 00 6B 00  t.B.T._.E.l.n.k.
33 00 31 00 00 00 65 00 06 00 00 00 44 4F 4E 41  3.1...e.....DONA
4C 44 41 00 0D 00 00 00 00 00 00 00 0D 00 00 00  LDA.............
30 00 30 00 61 00 30 00 32 00 34 00 30 00 30 00  0.0.a.0.2.4.0.0.
63 00 61 00 65 00 66 00 00 00 54 00 03 00 00 00  c.a.e.f...T.....
CC 07 18 00 02 00 00 00 EA 00 00 00              ............

08/09-11:16:01.488592 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:37644  DF
*****PA* Seq: 0x13BE6   Ack: 0x10E2B   Win: 0x1D05
00 00 00 AC FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0C 10 00 00 58 00 00 00 00 04 00 00 00  ..@....X........
00 00 00 00 00 00 00 00 00 54 00 58 00 54 00 02  .........T.X.T..
00 26 00 0C 08 69 00 00 5C 00 50 00 49 00 50 00  .&...i..\.P.I.P.
45 00 5C 00 00 00 00 00 FB 05 00 00 03 10 00 00  E.\.............
58 00 00 00 01 00 00 00 40 00 00 00 00 00 1A 00  X.......@.......
92 0E 92 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00 88 8A  D.o.n.a.l.d.....
00 00 00 00 00 00 00 00 CC FB 12 00 00 00 00 00  ................
00 00 00 00 00 01 00 00 7C FC 12 00 00 00 00 00  ........|.......

08/09-11:16:01.491559 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:44574  DF
*****PA* Seq: 0x10FA7   Ack: 0x13CC4   Win: 0x1E46
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0C 00 00 00                             .......

08/09-11:16:01.491834 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:37900  DF
*****PA* Seq: 0x13C96   Ack: 0x10FA7   Win: 0x2238
```

```
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0C 03 0C 08 FF FF FF FF 00 00 38        .............8

08/09-11:16:01.499454 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:44830  DF
*****PA* Seq: 0x10FCE   Ack: 0x13D2C   Win: 0x1DDE
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0C 22 FF 00 67 00 00 0D 08 01 00 00 00  ....".g.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.499787 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:38156  DF
*****PA* Seq: 0x13CC4   Ack: 0x10FCE   Win: 0x2211
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0C 18 FF 00 00 00 00 0E 00 06 00 00 00  ................
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
02 00 00 00 01 11 00 00 5C 00 73 00 72 00 76 00  ........\.s.r.v.
73 00 76 00 63 00 00 00                          s.v.c...

08/09-11:16:01.502730 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:45086  DF
*****PA* Seq: 0x11039   Ack: 0x13DCC   Win: 0x1D3E
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0D 0A 00 00 44 00 00 00 00 00 00 38 00  .......D......8.
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 01 00 00 00 30 16 30 16  ....D.......0.0.
08 AB 00 00 0D 00 5C 50 49 50 45 5C 6E 74 73 76  ......\PIPE\ntsv
63 73 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  cs...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.503090 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:38412  DF
*****PA* Seq: 0x13D2C   Ack: 0x11039   Win: 0x21A6
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0D 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 0D 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 01 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
01 00 00 00 00 00 01 00 C8 4F 32 4B 70 16 D3 01  .........O2Kp...
12 78 5A 47 BF 6E E1 88 03 00 00 00 04 5D 88 8A  .xZG.n.......]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.506260 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:45342  DF
*****PA* Seq: 0x110B9   Ack: 0x13E7C   Win: 0x1C8E
00 00 00 F4 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
```

```
02 08 40 0D 0A 00 00 BC 00 00 00 00 00 38 00 00  ..@..........8..
00 BC 00 38 00 00 00 00 00 BD 00 58 05 00 02 03  ...8.......X....
10 00 00 00 BC 00 00 00 01 00 00 00 A4 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 BC 07 18 00  ................
01 00 00 00 D8 FD 17 00 01 00 00 00 00 00 00 00  ................
B2 FE 17 00 92 FE 17 00 06 00 00 00 98 FE 17 00  ................
13 00 00 00 00 00 00 00 13 00 00 00 5C 00 44 00  ............\.D.
65 00 76 00 69 00 63 00 65 00 5C 00 4E 00 62 00  e.v.i.c.e.\.N.b.
66 00 5F 00 45 00 6C 00 6E 00 6B 00 33 00 31 00  f._.E.l.n.k.3.1.
00 00 65 00 06 00 00 00 44 4F 4E 41 4C 44 6C 00  ..e.....DONALDl.
0D 00 00 00 00 00 00 00 0D 00 00 00 30 00 30 00  ............0.0.
61 00 30 00 32 00 34 00 30 00 30 00 63 00 61 00  a.0.2.4.0.0.c.a.
65 00 66 00 00 00 30 00 01 00 00 00 CC 07 18 00  e.f...0.........
03 00 00 00 00 00 00 00                          ........

08/09-11:16:01.506646 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:38668  DF
*****PA* Seq: 0x13DCC   Ack: 0x110B9   Win: 0x2126
00 00 00 AC FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0D 10 00 00 58 00 00 00 00 04 00 00 00  ..@....X........
00 00 00 00 00 00 00 00 00 54 00 58 00 54 00 02  .........T.X.T..
00 26 00 0D 08 69 00 00 5C 00 50 00 49 00 50 00  .&...i..\.P.I.P.
45 00 5C 00 00 00 00 00 FB 05 00 00 03 10 00 00  E.\.............
58 00 00 00 01 00 00 00 40 00 00 00 00 00 00 1A  X.......@.......
92 0E 92 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00 88 8A  D.o.n.a.l.d.....
00 00 00 00 00 00 00 00 CC FB 12 00 00 00 00 00  ................
00 00 00 00 00 01 00 00 7C FC 12 00 02 00 00 00  ........|.......

08/09-11:16:01.509568 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:45598  DF
*****PA* Seq: 0x111B1   Ack: 0x13EAA   Win: 0x2238
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0D 00 00 00                             .......

08/09-11:16:01.509845 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:38924  DF
*****PA* Seq: 0x13E7C   Ack: 0x111B1   Win: 0x202E
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0D 03 0D 08 FF FF FF FF 00 00 38        .............8

08/09-11:16:01.533077 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:45854  DF
*****PA* Seq: 0x111D8   Ack: 0x13F12   Win: 0x21D0
00 00 00 67 FF 53 4D 42 A2 00 00 00 00 98 03 80  ...g.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0D 22 FF 00 67 00 00 0E 08 01 00 00 00  ....".g.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
80 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 02 00 FF 05 00 00 00                 ...........

08/09-11:16:01.533419 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:39180  DF
```

```
*****PA* Seq: 0x13EAA   Ack: 0x111D8   Win: 0x2007
00 00 00 64 FF 53 4D 42 A2 00 00 00 00 18 03 80  ...d.SMB........
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 C0 0D 18 FF 00 00 00 00 0E 00 06 00 00 00  ................
00 00 00 00 9F 01 02 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00  ................
02 00 00 00 01 11 00 00 5C 00 73 00 72 00 76 00  ........\.s.r.v.
73 00 76 00 63 00 00 00                          s.v.c...

08/09-11:16:01.536313 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:46110  DF
*****PA* Seq: 0x11243   Ack: 0x13FB2   Win: 0x2130
00 00 00 7C FF 53 4D 42 25 00 00 00 00 98 03 80  ...|.SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0E 0A 00 00 44 00 00 00 00 00 38 00 00  .......D.....8..
00 44 00 38 00 00 00 00 00 45 00 48 05 00 0C 03  .D.8.....E.H....
10 00 00 00 44 00 00 00 01 00 00 00 30 16 30 16  ....D.......0.0.
09 AB 00 00 0D 00 5C 50 49 50 45 5C 6E 74 73 76  ......\PIPE\ntsv
63 73 00 00 01 00 00 00 00 00 00 00 04 5D 88 8A  cs...........]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.536683 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:39436  DF
*****PA* Seq: 0x13F12   Ack: 0x11243   Win: 0x1F9C
00 00 00 9C FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 00 0E 10 00 00 48 00 00 00 00 04 00 00 00  .......H........
00 00 00 00 00 00 00 00 00 54 00 48 00 54 00 02  .........T.H.T..
00 26 00 0E 08 59 00 00 5C 00 50 00 49 00 50 00  .&...Y..\.P.I.P.
45 00 5C 00 00 00 00 00 05 00 0B 00 10 00 00 00  E.\.............
48 00 00 00 01 00 00 00 30 16 30 16 00 00 00 00  H.......0.0.....
01 00 00 00 00 00 01 00 C8 4F 32 4B 70 16 D3 01  .........O2Kp...
12 78 5A 47 BF 6E E1 88 03 00 00 00 04 5D 88 8A  .xZG.n.......]..
EB 1C C9 11 9F E8 08 00 2B 10 48 60 02 00 00 00  ........+.H`....

08/09-11:16:01.539330 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:46366  DF
*****PA* Seq: 0x112C3   Ack: 0x14040   Win: 0x20A2
00 00 00 88 FF 53 4D 42 25 00 00 00 00 98 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0E 0A 00 00 50 00 00 00 00 00 00 38 00  ..@....P.....8..
00 50 00 38 00 00 00 00 00 00 51 00 36 05 00 02  .P.8.....Q.6....
10 00 00 00 50 00 00 00 01 00 00 00 38 00 00 00  ....P.......8...
00 00 00 00 10 B4 16 00 45 75 91 39 39 AD 6A 13  ........Eu.99.j.
0F 00 00 00 0E 00 00 00 0D 00 00 00 19 00 00 00  ................
F0 00 00 00 36 01 00 00 09 00 00 00 08 00 00 00  ....6...........
D0 07 00 00 03 00 00 00 00 00 00 00              ............

08/09-11:16:01.539695 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:39692  DF
*****PA* Seq: 0x13FB2   Ack: 0x112C3   Win: 0x1F1C
00 00 00 8A FF 53 4D 42 25 00 00 00 00 18 03 80  .....SMB%.......
41 80 00 00 00 00 00 00 00 00 00 00 01 08 A0 42  A..............B
02 08 40 0E 10 00 00 36 00 00 00 00 04 00 00 00  ..@....6........
00 00 00 00 00 00 00 00 00 54 00 36 00 54 00 02  .........T.6.T..
00 26 00 0E 08 47 00 00 5C 00 50 00 49 00 50 00  .&...G..\.P.I.P.
45 00 5C 00 00 00 00 FB 05 00 00 03 10 00 00 00  E.\.............
```

```
36 00 00 00 01 00 00 00 1E 00 00 00 00 00 1C 00  6...............
92 0E 92 00 07 00 00 00 00 00 00 00 07 00 00 00  ................
44 00 6F 00 6E 00 61 00 6C 00 64 00 00 00        D.o.n.a.l.d...

08/09-11:16:01.542554 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:46622  DF
*****PA* Seq: 0x1134F   Ack: 0x1406E   Win: 0x2074
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0E 00 00 00                             .......

08/09-11:16:01.543122 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:39948  DF
*****PA* Seq: 0x14040   Ack: 0x1134F   Win: 0x1E90
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 80 0E 03 0E 08 FF FF FF FF 00 00 38        ..............8

08/09-11:16:01.713660 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:40204  DF
******A* Seq: 0x1406E   Ack: 0x11376   Win: 0x1E69

08/09-11:16:03.151080 server.goodness.org:139 -> devil.goodness.org:1079
TCP TTL:128 TOS:0x0 ID:46878  DF
*****PA* Seq: 0x11376   Ack: 0x1409C   Win: 0x2046
00 00 00 23 FF 53 4D 42 04 00 00 00 00 98 03 80  ...#.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 C0 0E 00 00 00                             .......

08/09-11:16:03.151867 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:40460  DF
*****PA* Seq: 0x1406E   Ack: 0x11376   Win: 0x1E69
00 00 00 2A FF 53 4D 42 04 00 00 00 00 18 03 80  ...*.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 01 08 FE CA  ................
02 08 C0 0E 03 0B 08 FF FF FF FF 00 00 38        ..............8

08/09-11:16:03.315500 devil.goodness.org:1079 -> server.goodness.org:139
TCP TTL:128 TOS:0xC ID:40716  DF
******A* Seq: 0x1409C   Ack: 0x1139D   Win: 0x1E42
```

1. Source of trace:

My network

2. Detect was generated by:

Snort intrusion detection system.

08/09-11:16:01.351038 **[Date & Time]** server.goodness.org:139 **[Source address & Port]** -> devil.goodness.org:1079 **[Destination address & Port]**
TCP **[Protocol]** TTL:128 **[Timeto live]** TOS:0x0 **[Type os service]** ID:38174 **[ID#]** DF *****PA* **[TCP flags]** Seq: 0x1030D **[Sequence #]** Ack: 0x12E2E **[Acknowledge #]** Win: 0x2110 **[Win size]**

3. Probability the source address was spoofed:

Low, this attack will not work if the address is spoofed.

4. Description of attack:

A null session user accessed the registry of a NT server through the Winreg named pipe.
Common Vulnerabilities and Exposures CAN-1999-0520

5. Attack mechanism:

A named pipe is a share name to which remote services and applications can connect. A workstation service can use SMB to communicate with a remote server and access the NPFS. Named pipes are secretly used by applications and services, users cannot see them. In this example the registry value for RestrictNullSessAccess was set to 0, giving the null session user the same permissions assigned to the everyone group. This allowed a null session user to access the registry on the server through the Winreg named pipe.

6. Correlations:

Security violations involving null session access is well documented through SANS and CERT.

Windump

```
11:12:07.818552 server.goodness.org.138 > broadcast.goodness.org.138: udp 201
11:12:53.464127 server.goodness.org.139 > devil.goodness.org.1079: S
62509:62509(0) ack 73912 win 8760 <mss 1460> (DF)
11:12:53.465240 devil.goodness.org.1079 > server.goodness.org.139: S
73911:73911(0) win 8192 <mss 1460> (DF) [tos 0xc]
11:12:53.465381 devil.goodness.org.1079 > server.goodness.org.139: . ack 1
win 8760 (DF) [tos 0xc]
11:12:53.465482 devil.goodness.org.1079 > server.goodness.org.139: P 1:73(72)
ack 1 win 8760 (DF) [tos 0xc]
11:12:53.466259 server.goodness.org.139 > devil.goodness.org.1079: P 1:5(4)
ack 73 win 8688 (DF)
11:12:53.468998 server.goodness.org.139 > devil.goodness.org.1079: P
5:100(95) ack 247 win 8514 (DF)
11:12:53.469329 devil.goodness.org.1079 > server.goodness.org.139: P
73:247(174) ack 5 win 8756 (DF) [tos 0xc]
11:12:53.479793 server.goodness.org.1149 > 10.1.41.30.139: P 65486:65974(488)
ack 110158 win 7840 (DF) [tos 0x64]
11:12:53.480074 devil.goodness.org.1079 > server.goodness.org.139: P
247:513(266) ack 100 win 8661 (DF) [tos 0xc]
11:12:53.491426 10.1.41.30.139 > server.goodness.org.1149: P 1:461(460) ack
488 win 8272 (DF)
11:12:53.500347 server.goodness.org.139 > devil.goodness.org.1079: P
100:244(144) ack 513 win 8248 (DF)
11:12:53.505626 server.goodness.org.139 > devil.goodness.org.1079: P
244:351(107) ack 617 win 8144 (DF)
11:12:53.506057 devil.goodness.org.1079 > server.goodness.org.139: P
513:617(104) ack 244 win 8517 (DF) [tos 0xc]
```

```
11:12:53.509364 server.goodness.org.139 > devil.goodness.org.1079: P
351:479(128) ack 777 win 7984 (DF)
11:12:53.509750 devil.goodness.org.1079 > server.goodness.org.139: P
617:777(160) ack 351 win 8410 (DF) [tos 0xc]
11:12:53.512852 server.goodness.org.139 > devil.goodness.org.1079: P
479:643(164) ack 925 win 7836 (DF)
11:12:53.513214 devil.goodness.org.1079 > server.goodness.org.139: P
777:925(148) ack 479 win 8282 (DF) [tos 0xc]
11:12:53.516256 server.goodness.org.139 > devil.goodness.org.1079: P
643:682(39) ack 971 win 7790 (DF)
11:12:53.516539 devil.goodness.org.1079 > server.goodness.org.139: P
925:971(46) ack 643 win 8118 (DF) [tos 0xc]
11:12:53.524614 server.goodness.org.139 > devil.goodness.org.1079: P
682:789(107) ack 1075 win 7686 (DF)
11:12:53.524939 devil.goodness.org.1079 > server.goodness.org.139: P
971:1075(104) ack 682 win 8079 (DF) [tos 0xc]
11:12:53.527906 server.goodness.org.139 > devil.goodness.org.1079: P
789:917(128) ack 1235 win 7526 (DF)
11:12:53.528273 devil.goodness.org.1079 > server.goodness.org.139: P
1075:1235(160) ack 789 win 7972 (DF) [tos 0xc]
11:12:53.536517 server.goodness.org.139 > devil.goodness.org.1079: P
917:1109(192) ack 1383 win 7378 (DF)
11:12:53.537023 devil.goodness.org.1079 > server.goodness.org.139: P
1235:1383(148) ack 917 win 7844 (DF) [tos 0xc]
11:12:53.539905 server.goodness.org.139 > devil.goodness.org.1079: P
1109:1148(39) ack 1429 win 7332 (DF)
11:12:53.540197 devil.goodness.org.1079 > server.goodness.org.139: P
1383:1429(46) ack 1109 win 7652 (DF) [tos 0xc]
11:12:53.547559 server.goodness.org.139 > devil.goodness.org.1079: P
1148:1255(107) ack 1533 win 8760 (DF)
11:12:53.548017 devil.goodness.org.1079 > server.goodness.org.139: P
1429:1533(104) ack 1148 win 7613 (DF) [tos 0xc]
11:12:53.550908 server.goodness.org.139 > devil.goodness.org.1079: P
1255:1383(128) ack 1693 win 8600 (DF)
11:12:53.551280 devil.goodness.org.1079 > server.goodness.org.139: P
1533:1693(160) ack 1255 win 7506 (DF) [tos 0xc]
11:12:53.555761 server.goodness.org.139 > devil.goodness.org.1079: P
1383:2179(796) ack 1869 win 8424 (DF)
11:12:53.556185 devil.goodness.org.1079 > server.goodness.org.139: P
1693:1869(176) ack 1383 win 7378 (DF) [tos 0xc]
11:12:53.559360 server.goodness.org.139 > devil.goodness.org.1079: P
2179:2218(39) ack 1915 win 8378 (DF)
11:12:53.559649 devil.goodness.org.1079 > server.goodness.org.139: P
1869:1915(46) ack 2179 win 8760 (DF) [tos 0xc]
11:12:53.568151 server.goodness.org.139 > devil.goodness.org.1079: P
2218:2325(107) ack 2019 win 8274 (DF)
11:12:53.568485 devil.goodness.org.1079 > server.goodness.org.139: P
1915:2019(104) ack 2218 win 8721 (DF) [tos 0xc]
11:12:53.571452 server.goodness.org.139 > devil.goodness.org.1079: P
2325:2453(128) ack 2179 win 8114 (DF)
11:12:53.571826 devil.goodness.org.1079 > server.goodness.org.139: P
2019:2179(160) ack 2325 win 8614 (DF) [tos 0xc]
11:12:53.575260 server.goodness.org.139 > devil.goodness.org.1079: P
2453:2833(380) ack 2355 win 7938 (DF)
11:12:53.575644 devil.goodness.org.1079 > server.goodness.org.139: P
2179:2355(176) ack 2453 win 8486 (DF) [tos 0xc]
```

```
11:12:53.578750 server.goodness.org.139 > devil.goodness.org.1079: P
2833:2872(39) ack 2401 win 7892 (DF)
11:12:53.579184 devil.goodness.org.1079 > server.goodness.org.139: P
2355:2401(46) ack 2833 win 8106 (DF) [tos 0xc]
11:12:53.586892 server.goodness.org.139 > devil.goodness.org.1079: P
2872:2979(107) ack 2505 win 7788 (DF)
11:12:53.587363 devil.goodness.org.1079 > server.goodness.org.139: P
2401:2505(104) ack 2872 win 8067 (DF) [tos 0xc]
11:12:53.590256 server.goodness.org.139 > devil.goodness.org.1079: P
2979:3107(128) ack 2665 win 7628 (DF)
11:12:53.590619 devil.goodness.org.1079 > server.goodness.org.139: P
2505:2665(160) ack 2979 win 7960 (DF) [tos 0xc]
11:12:53.593766 server.goodness.org.139 > devil.goodness.org.1079: P
3107:3355(248) ack 2841 win 7452 (DF)
11:12:53.594057 server.goodness.org.1149 > 10.1.41.30.139: . ack 461 win 7380
(DF) [tos 0x64]
11:12:53.594263 devil.goodness.org.1079 > server.goodness.org.139: P
2665:2841(176) ack 3107 win 7832 (DF) [tos 0xc]
11:12:53.597187 server.goodness.org.139 > devil.goodness.org.1079: P
3355:3394(39) ack 2887 win 7406 (DF)
11:12:53.597485 devil.goodness.org.1079 > server.goodness.org.139: P
2841:2887(46) ack 3355 win 7584 (DF) [tos 0xc]
11:12:53.619554 server.goodness.org.139 > devil.goodness.org.1079: P
3394:3501(107) ack 2991 win 7302 (DF)
11:12:53.619881 devil.goodness.org.1079 > server.goodness.org.139: P
2887:2991(104) ack 3394 win 7545 (DF) [tos 0xc]
11:12:53.622816 server.goodness.org.139 > devil.goodness.org.1079: P
3501:3629(128) ack 3151 win 8760 (DF)
11:12:53.623198 devil.goodness.org.1079 > server.goodness.org.139: P
2991:3151(160) ack 3501 win 7438 (DF) [tos 0xc]
11:12:53.625965 server.goodness.org.139 > devil.goodness.org.1079: P
3629:3769(140) ack 3293 win 8618 (DF)
11:12:53.626337 devil.goodness.org.1079 > server.goodness.org.139: P
3151:3293(142) ack 3629 win 7310 (DF) [tos 0xc]
11:12:53.629207 server.goodness.org.139 > devil.goodness.org.1079: P
3769:3808(39) ack 3339 win 8572 (DF)
11:12:53.629492 devil.goodness.org.1079 > server.goodness.org.139: P
3293:3339(46) ack 3769 win 8760 (DF) [tos 0xc]
11:12:53.839956 devil.goodness.org.1079 > server.goodness.org.139: . ack 3808 win 8721 (DF) [tos 0xc]
```

6. Evidence of active targeting:

A specific host, an NT server was targeted and access via port 139 tcp NETBIOS Session Service.

8. Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(3 + 2) – (3 + 2) = 0

9. Defensive recommendation:

A value in the registry (NullSessionPipes) lists the named pipes that are available to null session users. All of these named pipes in this list will be open to anonymous users. Control null session access by setting the registry value for RestrictNullSessAccess so

that it equals 1. Then null session users will not be able to access named pipes (or any shares).

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

What resources can be accessed through null sessions?
A.) Share codes
B.) Share folders and name pipes
C.) Share names
D.) pipe length

answer: B and C

Detect 2

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)

08/12-19:02:44.611078 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:272  DF
**S***** Seq: 0x5F71936C   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 122698 0 NOP WS: 0

08/12-19:02:44.611329 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21273  DF
**S***A* Seq: 0x5D9857D8   Ack: 0x5F71936D   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 19367658 122698 NOP WS: 0

08/12-19:02:44.611493 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:273  DF
******A* Seq: 0x5F71936D   Ack: 0x5D9857D9   Win: 0x7D78
TCP Options => NOP NOP TS: 122698 19367658

08/12-19:02:44.618543 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:275  DF
*****PA* Seq: 0x5F71936D   Ack: 0x5D9857D9   Win: 0x7D78
TCP Options => NOP NOP TS: 122699 19367658
FF FD 26 FF FB 26 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                                               #

08/12-19:02:44.618601 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21274  DF
******A* Seq: 0x5D9857D9   Ack: 0x5F71938E   Win: 0x7D78
TCP Options => NOP NOP TS: 19367658 122699

08/12-19:02:44.626551 goodness.org:1025 -> dns.goodness.org:53
UDP TTL:64 TOS:0x0 ID:21275
Len: 53
5D 35 01 00 00 01 00 00 00 00 00 00 03 32 34 39  ]5...........249
02 31 30 03 31 36 38 03 31 39 32 07 69 6E 2D 61  .10.168.191.in-a
```

```
64 64 72 04 61 72 70 61 00 00 0C 00 01          ddr.arpa.....

08/12-19:02:44.627452 dns.goodnes.org:53 -> goodness.org:1025
UDP TTL:127 TOS:0x0 ID:36842
Len: 130
5D 35 85 83 00 01 00 00 00 01 00 00 03 32 34 39  ]5...........249
02 31 30 03 31 36 38 03 31 39 32 07 69 6E 2D 61  .10.168.191.in-a
64 64 72 04 61 72 70 61 00 00 0C 00 01 02 31 30  ddr.arpa......10
03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 64 72  .168.191.in-addr
04 61 72 70 61 00 00 06 00 01 00 00 0E 10 00 2A  .arpa..........*
05 6D 69 7A 61 72 03 6E 6F 63 05 64 63 69 74 70  .mi2ar.noc.dddip
03 67 6F 76 00 00 00 00 00 0B 00 00 0E 10 00 00  .com............
02 58 00 01 51 80 00 00 0E 10                    .X..Q.....

08/12-19:02:44.628022 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21276  DF
*****PA* Seq: 0x5D9857D9   Ack: 0x5F71938E   Win: 0x7D78
TCP Options => NOP NOP TS: 19367659 122699
FF FD 18 FF FD 20 FF FD 23 FF FD 27              ..... ..#..'

08/12-19:02:44.628161 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:276  DF
******A* Seq: 0x5F71938E   Ack: 0x5D9857E5   Win: 0x7D78
TCP Options => NOP NOP TS: 122700 19367659

08/12-19:02:44.628203 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21277  DF
*****PA* Seq: 0x5D9857E5   Ack: 0x5F71938E   Win: 0x7D78
TCP Options => NOP NOP TS: 19367659 122700
FF FC 26 FF FE 26 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           ...'.........

08/12-19:02:44.633587 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:277  DF
******A* Seq: 0x5F71938E   Ack: 0x5D985812   Win: 0x7D78
TCP Options => NOP NOP TS: 122701 19367659

08/12-19:02:44.635382 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:278  DF
*****PA* Seq: 0x5F71938E   Ack: 0x5D985812   Win: 0x7D78
TCP Options => NOP NOP TS: 122701 19367659
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 74 68  00,38400....#.th
65 6B 69 64 2E 6F 72 67 3A 30 FF F0 FF FA 27 00  ekid.org:0....'.
00 44 49 53 50 4C 41 59 01 74 68 65 6B 69 64 2E  .DISPLAY.thekid.
6F 72 67 3A 30 FF F0 FF FA 18 00 58 54 45 52 4D  org:0......XTERM
FF F0                                            ..

08/12-19:02:44.635917 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21278  DF
*****PA* Seq: 0x5D985812   Ack: 0x5F7193E0   Win: 0x7D78
TCP Options => NOP NOP TS: 19367660 122701
FF FD 01                                         ...

08/12-19:02:44.636108 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:279  DF
```

```
*****PA* Seq: 0x5F7193E0   Ack: 0x5D985815   Win: 0x7D78
TCP Options => NOP NOP TS: 122701 19367660
FF FC 01                                          ...

08/12-19:02:44.636810 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21279  DF
*****PA* Seq: 0x5D985815   Ack: 0x5F7193E3   Win: 0x7D78
TCP Options => NOP NOP TS: 19367660 122701
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
36 38 36 0D 0A                                   686..

08/12-19:02:44.637057 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:280  DF
*****PA* Seq: 0x5F7193E3   Ack: 0x5D98585A   Win: 0x7D78
TCP Options => NOP NOP TS: 122701 19367660
FF FD 01                                          ...

08/12-19:02:44.650505 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21280  DF
******A* Seq: 0x5D98585A   Ack: 0x5F7193E6   Win: 0x7D78
TCP Options => NOP NOP TS: 19367662 122701

08/12-19:02:44.651309 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21281  DF
*****PA* Seq: 0x5D98585A   Ack: 0x5F7193E6   Win: 0x7D78
TCP Options => NOP NOP TS: 19367662 122701
6C 6F 67 69 6E 3A 20                             login:

08/12-19:02:44.653587 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:281  DF
******A* Seq: 0x5F7193E6   Ack: 0x5D985861   Win: 0x7D78
TCP Options => NOP NOP TS: 122703 19367662

08/12-19:02:49.041474 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:282  DF
*****PA* Seq: 0x5F7193E6   Ack: 0x5D985861   Win: 0x7D78
TCP Options => NOP NOP TS: 123141 19367662
73                                                s

08/12-19:02:49.041751 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21282  DF
*****PA* Seq: 0x5D985861   Ack: 0x5F7193E7   Win: 0x7D78
TCP Options => NOP NOP TS: 19368101 123141
73                                                s

08/12-19:02:49.053575 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:283  DF
******A* Seq: 0x5F7193E7   Ack: 0x5D985862   Win: 0x7D78
TCP Options => NOP NOP TS: 123143 19368101

08/12-19:02:49.816161 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:284  DF
*****PA* Seq: 0x5F7193E7   Ack: 0x5D985862   Win: 0x7D78
TCP Options => NOP NOP TS: 123219 19368101
```

```
6C                                                  l

08/12-19:02:49.816435 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21283  DF
*****PA* Seq: 0x5D985862   Ack: 0x5F7193E8   Win: 0x7D78
TCP Options => NOP NOP TS: 19368178 123219
6C                                                  l

08/12-19:02:49.833573 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:285  DF
******A* Seq: 0x5F7193E8   Ack: 0x5D985863   Win: 0x7D78
TCP Options => NOP NOP TS: 123221 19368178

08/12-19:02:50.136177 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:286  DF
*****PA* Seq: 0x5F7193E8   Ack: 0x5D985863   Win: 0x7D78
TCP Options => NOP NOP TS: 123251 19368178
61                                                  a

08/12-19:02:50.136366 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21284  DF
*****PA* Seq: 0x5D985863   Ack: 0x5F7193E9   Win: 0x7D78
TCP Options => NOP NOP TS: 19368210 123251
61                                                  a

08/12-19:02:50.153572 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:287  DF
******A* Seq: 0x5F7193E9   Ack: 0x5D985864   Win: 0x7D78
TCP Options => NOP NOP TS: 123253 19368210

08/12-19:02:50.451867 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:288  DF
*****PA* Seq: 0x5F7193E9   Ack: 0x5D985864   Win: 0x7D78
TCP Options => NOP NOP TS: 123282 19368210
63                                                  c

08/12-19:02:50.452053 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21285  DF
*****PA* Seq: 0x5D985864   Ack: 0x5F7193EA   Win: 0x7D78
TCP Options => NOP NOP TS: 19368242 123282
63                                                  c

08/12-19:02:50.463571 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:289  DF
******A* Seq: 0x5F7193EA   Ack: 0x5D985865   Win: 0x7D78
TCP Options => NOP NOP TS: 123284 19368242

08/12-19:02:50.852188 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:290  DF
*****PA* Seq: 0x5F7193EA   Ack: 0x5D985865   Win: 0x7D78
TCP Options => NOP NOP TS: 123322 19368242
6B                                                  k

08/12-19:02:50.852372 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21286  DF
*****PA* Seq: 0x5D985865   Ack: 0x5F7193EB   Win: 0x7D78
TCP Options => NOP NOP TS: 19368282 123322
```

```
6B                                                  k

08/12-19:02:50.863570 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:291  DF
******A* Seq: 0x5F7193EB   Ack: 0x5D985866   Win: 0x7D78
TCP Options => NOP NOP TS: 123324 19368282

08/12-19:02:51.238738 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:292  DF
*****PA* Seq: 0x5F7193EB   Ack: 0x5D985866   Win: 0x7D78
TCP Options => NOP NOP TS: 123361 19368282
65                                                  e

08/12-19:02:51.238928 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21287  DF
*****PA* Seq: 0x5D985866   Ack: 0x5F7193EC   Win: 0x7D78
TCP Options => NOP NOP TS: 19368320 123361
65                                                  e

08/12-19:02:51.253570 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:293  DF
******A* Seq: 0x5F7193EC   Ack: 0x5D985867   Win: 0x7D78
TCP Options => NOP NOP TS: 123363 19368320

08/12-19:02:51.588446 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:294  DF
*****PA* Seq: 0x5F7193EC   Ack: 0x5D985867   Win: 0x7D78
TCP Options => NOP NOP TS: 123396 19368320
72                                                  r

08/12-19:02:51.588728 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21288  DF
*****PA* Seq: 0x5D985867   Ack: 0x5F7193ED   Win: 0x7D78
TCP Options => NOP NOP TS: 19368355 123396
72                                                  r

08/12-19:02:51.603571 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:295  DF
******A* Seq: 0x5F7193ED   Ack: 0x5D985868   Win: 0x7D78
TCP Options => NOP NOP TS: 123398 19368355

08/12-19:02:52.305831 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:296  DF
*****PA* Seq: 0x5F7193ED   Ack: 0x5D985868   Win: 0x7D78
TCP Options => NOP NOP TS: 123468 19368355
0D 00                                               ..

08/12-19:02:52.306025 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21289  DF
*****PA* Seq: 0x5D985868   Ack: 0x5F7193EF   Win: 0x7D78
TCP Options => NOP NOP TS: 19368427 123468
0D 0A                                               ..

08/12-19:02:52.323571 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:297  DF
******A* Seq: 0x5F7193EF   Ack: 0x5D98586A   Win: 0x7D78
TCP Options => NOP NOP TS: 123470 19368427
```

```
08/12-19:02:52.323621 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21290  DF
*****PA* Seq: 0x5D98586A   Ack: 0x5F7193EF   Win: 0x7D78
TCP Options => NOP NOP TS: 19368429 123470
50 61 73 73 77 6F 72 64 3A 20                    Password:

08/12-19:02:52.343568 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:298  DF
******A* Seq: 0x5F7193EF   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 123472 19368429

08/12-19:02:57.015699 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:299  DF
*****PA* Seq: 0x5F7193EF   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 123939 19368429
63                                                c

08/12-19:02:57.030489 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21293  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F0   Win: 0x7D78
TCP Options => NOP NOP TS: 19368900 123939

08/12-19:02:57.899566 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:300  DF
*****PA* Seq: 0x5F7193F0   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124027 19368900
61                                                a

08/12-19:02:57.910502 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21294  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F1   Win: 0x7D78
TCP Options => NOP NOP TS: 19368988 124027

08/12-19:02:58.301306 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:301  DF
*****PA* Seq: 0x5F7193F1   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124067 19368988
6E                                                n

08/12-19:02:58.320488 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21295  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F2   Win: 0x7D78
TCP Options => NOP NOP TS: 19369029 124067

08/12-19:02:58.741275 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:302  DF
*****PA* Seq: 0x5F7193F2   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124111 19369029
67                                                g

08/12-19:02:58.760487 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21296  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F3   Win: 0x7D78
TCP Options => NOP NOP TS: 19369073 124111

08/12-19:02:59.122094 devil.net:1043 -> goodness.org:23
```

```
TCP TTL:64 TOS:0x0 ID:303  DF
*****PA* Seq: 0x5F7193F3   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124149 19369073
65                                                  e

08/12-19:02:59.140488 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21297  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F4   Win: 0x7D78
TCP Options => NOP NOP TS: 19369111 124149

08/12-19:02:59.455237 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:304  DF
*****PA* Seq: 0x5F7193F4   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124183 19369111
74                                                  t

08/12-19:02:59.470493 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21298  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F5   Win: 0x7D78
TCP Options => NOP NOP TS: 19369144 124183

08/12-19:03:00.005162 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:305  DF
*****PA* Seq: 0x5F7193F5   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124238 19369144
69                                                  i

08/12-19:03:00.020488 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21299  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F6   Win: 0x7D78
TCP Options => NOP NOP TS: 19369199 124238

08/12-19:03:00.441745 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:306  DF
*****PA* Seq: 0x5F7193F6   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124281 19369199
6E                                                  n

08/12-19:03:00.460487 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21300  DF
******A* Seq: 0x5D985874   Ack: 0x5F7193F7   Win: 0x7D78
TCP Options => NOP NOP TS: 19369243 124281

08/12-19:03:01.543755 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:307  DF
*****PA* Seq: 0x5F7193F7   Ack: 0x5D985874   Win: 0x7D78
TCP Options => NOP NOP TS: 124392 19369243
0D 00                                               ..

08/12-19:03:01.544094 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21301  DF
*****PA* Seq: 0x5D985874   Ack: 0x5F7193F9   Win: 0x7D78
TCP Options => NOP NOP TS: 19369351 124392
0D 0A                                               ..

08/12-19:03:01.563556 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:308  DF
```

```
******A* Seq: 0x5F7193F9   Ack: 0x5D985876   Win: 0x7D78
TCP Options => NOP NOP TS: 124394 19369351

08/12-19:03:01.638566 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21302  DF
*****PA* Seq: 0x5D985876   Ack: 0x5F7193F9   Win: 0x7D78
TCP Options => NOP NOP TS: 19369360 124394
1B 5D 30 3B 73 6C 61 63 6B 65 72 40 64 65 76 3A  .]0;slacker@dev:
20 2F 68 6F 6D 65 2F 73 6C 61 63 6B 65 72 07      /home/slacker.

08/12-19:03:01.653567 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:309  DF
******A* Seq: 0x5F7193F9   Ack: 0x5D985895   Win: 0x7D78
TCP Options => NOP NOP TS: 124403 19369360

08/12-19:03:01.653629 goodness.org:23 -> devil.net:1043
TCP TTL:64 TOS:0x0 ID:21303  DF
*****PA* Seq: 0x5D985895   Ack: 0x5F7193F9   Win: 0x7D78
TCP Options => NOP NOP TS: 19369362 124403
5B 73 6C 61 63 6B 65 72 40 64 65 76 20 73 6C 61  [slacker@dev sla
63 6B 65 72 5D 24 20                             cker]$

08/12-19:03:01.673577 devil.net:1043 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:310  DF
******A* Seq: 0x5F7193F9   Ack: 0x5D9858AC   Win: 0x7D78
TCP Options => NOP NOP TS: 124405 19369362
```

1. **Source of trace**

   My network

2. **Detect was generated by:**

   Snort intrusion detection system.

```
08/12-19:02:44.611078 [Date & time] devil.net:1043 [Source address & Port] ->
goodness.org:23 [Destination address & Port] TCP [Protocol] TTL:64 [Time to
live] TOS:0x0 [Type of service] ID:272 [ID#]  DF [Do not fragment]
**S***** [TCP flag] Seq: 0x5F71936C [Sequence #]   Ack: 0x0 [Acknowledgement
#]   Win: 0x7D78 [Win size] TCP Options => MSS: 1460 [Maximum Segment Size]
SackOK TS: 122698 0 NOP WS: 0
```

3. **Probability the source address was spoofed:**

   Low, the attacker established a three-way handshake and subsequently gained access through password guessing.

Description of attack:

Attacker guessed password. Common Vulnerabilities and Exposures CAN-1999-0501

4. Attack mechanism:

The attacker attempts to gain access by guessing weak passwords.

6. Correlations:

Password guessing attacks are well documented.

7. Evidence of active targeting:

After gathering intelligence (social engineering / dumpster diving) the attacker went after a specific linux host and guessed its weak password.

8. **Severity:** (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(2 + 3) – (4 + 1) = 0

9. Defensive recommendation:

Create an acceptable password policy to verify password quality. Include in the policy a requirement to change all default passwords on first login. Test passwords with password cracking utilities. Implement utilities that check passwords when they are created. Force passwords to expire periodically. Maintain password histories so that users cannot recycle old passwords.

10. Multiple choice test question, write a question based on the trace and your analysis with your answer.

Password policies should:
A.) Require passwords to be changed weekly
B.) Require passwords to be written down and saved next to each system
C.) Require all passwords be a combination of letters and numbers 6-8 characters in length
D.) Require passwords to be an easily remembered name

Answer: C

Detect 3

```
-*> 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)

07/31-13:37:17.351355 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim
```

```
07/31-13:37:17.351854 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.351950 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352035 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352123 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352207 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352295 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352380 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352467 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim

07/31-13:37:17.352553 devil.net -> goodness.org
ICMP TTL:255 TOS:0x0 ID:1109
Frag Offset: 0x1FFE   Frag Size: 0x1A
08 00 00 00 00 00 00 00 00 DB 01 00 00 01 00 00  ................
00 00 00 00 06 6D 69 63 6B 65                    .....victim
(Continues)
```

1. **Source of trace**

   My network

2. **Detect was generated by:**

   Snort intrusion detection system.

```
07/31-13:37:17.351355 [Time & date] devil.net [Source address] ->
goodness.org [Destination address] ICMP [Protocol] TTL:255 [Time to live]
TOS:0x0 [Type of service] ID:1109 [ID#] Frag Offset: 0x1FFE [Fragment offset]
Frag Size: 0x1A [Fragment size]
```

3. **Probability the source address was spoofed:**

   Low, although this DoS attack may be from a compromised machine.

4. **Description of attack:**

   DoS attack against a Windows NT server, forces cpu utilization to 100%. Common Vulnerabilities and Exposures CAN-2000-0305.

5. **Attack mechanism:**

   The attack works by sending a large number of identical fragmented ICMP packets to a Windows host causing the target to lock-up for the duration of the attack.

6. **Correlations:**

   This type of DoS attack is well documented by SANS and CERT.

   Windump

```
13:37:17.348414 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.348656 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.348746 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.348831 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.348919 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349002 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349092 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349176 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349265 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349348 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349437 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349521 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349609 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349694 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349781 devil.net > goodness.org: (frag 1109:9@65520)
```

(Continues)

7. Evidence of active targeting:

A specific Windows based host must be targeted for this attack.

8. **Severity**: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(5 + 4) – (3 + 1) = 5

9. Defensive recommendation:

Filter fragmented IP packets at the router.

10. Multiple choice test question

This attack may?

```
13:37:17.349694 devil.net > goodness.org: (frag 1109:9@65520)
13:37:17.349781 devil.net > goodness.org: (frag 1109:9@65520)
(continues)
```

A.) Forces cpu utilization to 100%
B.) Cause the target to lock-up
C.) Identical fragmented IP packets
D.) The devil made me do it

Answer: A, B and C

Detect 4

```
-*> 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)

07/31-15:02:49.347663 devil.net:1751 -> goodness.org:1
TCP TTL:64 TOS:0x0 ID:6740  DF
**S***** Seq: 0xE17D4258   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495822 0 NOP WS: 0

07/31-15:02:49.348171 goodness.org:1 -> devil.net:1751
TCP TTL:128 TOS:0x0 ID:61696
****R*A* Seq: 0x0   Ack: 0xE17D4259   Win: 0x0
00 00 00 00 00 00                                ......

07/31-15:02:49.366146 devil.net:1752 -> goodness.org:7
TCP TTL:64 TOS:0x0 ID:6741  DF
**S***** Seq: 0xE148BC8C   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495824 0 NOP WS: 0

07/31-15:02:49.366625 goodness.org:7 -> devil.net:1752
TCP TTL:128 TOS:0x0 ID:61952
****R*A* Seq: 0x0   Ack: 0xE148BC8D   Win: 0x0
```

```
00 00 00 00 00 00                                  ......

07/31-15:02:49.386516 devil.net:1753 -> goodness.org:15
TCP TTL:64 TOS:0x0 ID:6742  DF
**S***** Seq: 0xE2302E2B   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495826 0 NOP WS: 0

07/31-15:02:49.387010 goodness.org:15 -> devil.net:1753
TCP TTL:128 TOS:0x0 ID:62208
****R*A* Seq: 0x0   Ack: 0xE2302E2C   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.410796 devil.net:1754 -> goodness.org:19
TCP TTL:64 TOS:0x0 ID:6743  DF
**S***** Seq: 0xE1ECA3ED   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495828 0 NOP WS: 0

07/31-15:02:49.411271 goodness.org:19 -> devil.net:1754
TCP TTL:128 TOS:0x0 ID:62464
****R*A* Seq: 0x0   Ack: 0xE1ECA3EE   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.427290 devil.net:1755 -> goodness.org:21
TCP TTL:64 TOS:0x0 ID:6744  DF
**S***** Seq: 0xE22BFC9D   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495830 0 NOP WS: 0

07/31-15:02:49.427765 goodness.org:21 -> devil.net:1755
TCP TTL:128 TOS:0x0 ID:62720
****R*A* Seq: 0x0   Ack: 0xE22BFC9E   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.446154 devil.net:1756 -> goodness.org:22
TCP TTL:64 TOS:0x0 ID:6745  DF
**S***** Seq: 0xE18A39D1   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495832 0 NOP WS: 0

07/31-15:02:49.446634 goodness.org:22 -> devil.net:1756
TCP TTL:128 TOS:0x0 ID:62976
****R*A* Seq: 0x0   Ack: 0xE18A39D2   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.467232 devil.net:1757 -> goodness.org:23
TCP TTL:64 TOS:0x0 ID:6746  DF
**S***** Seq: 0xE19B783A   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495834 0 NOP WS: 0

07/31-15:02:49.467712 goodness.org:23 -> devil.net:1757
TCP TTL:128 TOS:0x0 ID:63232
****R*A* Seq: 0x0   Ack: 0xE19B783B   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.486338 devil.net:1758 -> goodness.org:25
TCP TTL:64 TOS:0x0 ID:6747  DF
**S***** Seq: 0xE1D4F556   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495836 0 NOP WS: 0
```

```
07/31-15:02:49.486814 goodness.org:25 -> devil.net:1758
TCP TTL:128 TOS:0x0 ID:63488
****R*A* Seq: 0x0   Ack: 0xE1D4F557   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.506343 devil.net:1759 -> goodness.org:43
TCP TTL:64 TOS:0x0 ID:6748  DF
**S***** Seq: 0xE1DB3921   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495838 0 NOP WS: 0

07/31-15:02:49.506837 goodness.org:43 -> devil.net:1759
TCP TTL:128 TOS:0x0 ID:63744
****R*A* Seq: 0x0   Ack: 0xE1DB3922   Win: 0x0
00 00 00 00 00 00                                  ......

07/31-15:02:49.526107 devil.net:1760 -> goodness.org:53
TCP TTL:64 TOS:0x0 ID:6749  DF
**S***** Seq: 0xE1B47D62   Ack: 0x0   Win: 0x400
TCP Options => MSS: 1460 SackOK TS: 1495840 0 NOP WS: 0
……
(Continues)
```

1. **Source of trace**

   My network

2. **Detect was generated by:**

   Snort intrusion detection system.

```
07/31-15:02:49.347663 [Date & time] devil.net:1751 [Source address & Port] ->
goodness.org:1 [Destination address & port] TCP [Protocol] TTL:64 [Time to
live] TOS:0x0 [Type os service] ID:6740 [ID#]  DF [Do not fragment]
**S***** [TCP flag] Seq: 0xE17D4258 [Sequence #]   Ack: 0x0 [Acknowledgement
#]   Win: 0x400 [Win size] TCP Options => MSS: 1460 [Maximum segment size]
SackOK TS: 1495822 0 NOP WS: 0
```

3. **Probability the source address was spoofed:**

   Low, this is a port scan therefore it is unlikely that this address being is spoofed.

4. **Description of attack:**

   The attacker port mapping. (half-open scanning)

5. **Attack mechanism:**

   The attacker is port scanning the target by sending packets with the syn flag set. If the target responds with a packet with the syn/ack flags set, the port is open. If the target sends a packet with the rst flag set the port is closed. This scan found that port 139 NETBIOS Session Service was open.

6. Correlations:

Networking mapping techniques are well documented.

Tcpdump

```
15:02:49.344669 devil.net.1751 > goodness.org.1: S 3783082584:3783082584(0)
win 1024 <mss 1460,sackOK,timestamp 1495822 0,nop,wscale 0> (DF)
15:02:49.344926 goodness.org.1 > devil.net.1751: R 0:0(0) ack 3783082585 win
0
15:02:49.363146 devil.net.1752 > goodness.org.7: S 3779640460:3779640460(0)
win 1024 <mss 1460,sackOK,timestamp 1495824 0,nop,wscale 0> (DF)
15:02:49.363378 goodness.org.7 > devil.net.1752: R 0:0(0) ack 3779640461 win
0
15:02:49.383518 devil.net.1753 > goodness.org.15: S 3794808363:3794808363(0)
win 1024 <mss 1460,sackOK,timestamp 1495826 0,nop,wscale 0> (DF)
15:02:49.383764 goodness.org.15 > devil.net.1753: R 0:0(0) ack 3794808364 win
0
15:02:49.407789 devil.net.1754 > goodness.org.19: S 3790382061:3790382061(0)
win 1024 <mss 1460,sackOK,timestamp 1495828 0,nop,wscale 0> (DF)
15:02:49.408025 goodness.org.19 > devil.net.1754: R 0:0(0) ack 3790382062 win
0
15:02:49.424285 devil.net.1755 > goodness.org.21: S 3794533533:3794533533(0)
win 1024 <mss 1460,sackOK,timestamp 1495830 0,nop,wscale 0> (DF)
15:02:49.424519 goodness.org.21 > devil.net.1755: R 0:0(0) ack 3794533534 win
0
15:02:49.443151 devil.net.1756 > goodness.org.22: S 3783932369:3783932369(0)
win 1024 <mss 1460,sackOK,timestamp 1495832 0,nop,wscale 0> (DF)
15:02:49.443388 goodness.org.22 > devil.net.1756: R 0:0(0) ack 3783932370 win
0
15:02:49.464230 devil.net.1757 > goodness.org.23: S 3785062458:3785062458(0)
win 1024 <mss 1460,sackOK,timestamp 1495834 0,nop,wscale 0> (DF)
15:02:49.464466 goodness.org.23 > devil.net.1757: R 0:0(0) ack 3785062459 win
0
15:02:49.483331 devil.net.1758 > goodness.org.25: S 3788830038:3788830038(0)
win 1024 <mss 1460,sackOK,timestamp 1495836 0,nop,wscale 0> (DF)
15:02:49.483567 goodness.org.25 > devil.net.1758: R 0:0(0) ack 3788830039 win
0
```

(Continues**)**

7. Evidence of active targeting:

The attacker is targeting a specific host for a port scan.

8. Severity: (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) = Severity

(2 + 1) – (3 + 2) = -2

9. Defensive recommendation:

Set a rule in your IDS

10.Multiple choice test question

Port scanning is used to:
A.) Identify operating systems
B.) Look for known trojans
C.) Identify docking facilities
D.) All of the above

Answer: A and B

Detect 5

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)

08/01-09:45:12.171201 spoofed.evil.net -> goodness.org
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 spoofed.evil.net -> goodness.org
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 spoofed.evil.net -> goodness.org
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 spoofed.evil.net -> goodness.org
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..............
              ..........
```

1. Source of trace:

My network

2. Detect was generated by:

Snort intrusion detection system.

08/01-09:45:12.171201 **[Date & time]** spoofed.evil.net **[Source address]** -> goodness.org **[Destination address]** UDP **[Protocol]** TTL:64 **[Time to live]** TOS:0x0 **[Type of service]** ID:242 **[ID#]** MF **[Must fragment]**

```
Frag Offset: 0x0 [Fragment offset]   Frag Size: 0x24 [Fragment size]
```

3. **Probability the source address was spoofed:**

   High, this is a DoS attack against a Linux host, therefore it is very likely that the address is spoofed.

4. **Description of attack:**

   This attack sends two fragments that do not overlap properly, causing some machines to crash when they try to reassemble them. Common Vulnerabilities and Exposures CAN-1999-0104.

5. **Attack mechanism:**

   The attack works by sending a stream of overlaping fragmented udp packets from a spoofed address. This will cause some older unpatched operating systems to hang or reboot.

6. **Correlations:**

   This attack is well documented at SANS and CERT.

   Tcpdump

```
09:45:12.171201 eth0 < spoofed.evil.net.56169 > goodness.org.3223: udp 28
(frag 242:36@0+)
09:45:12.171246 eth0 < spoofed.evil.net > goodness.org: (frag 242:4@24)
09:45:12.188516 eth0 < spoofed.evil.net.56169 > goodness.org.3223: udp 28
(frag 242:36@0+)
09:45:12.188566 eth0 < spoofed.evil.net > goodness.org: (frag 242:4@24)
```

7. **Evidence of active targeting:**

   This attack is targeted at a specific host, usually Linux.

8. Severity: (Criticality + Lethality) – (System Countermeasures + Network Coutermeasures)= Serverity

(3 + 4) – (3 + 2) = 2

9. **Defensive recommendation:**

   Set IDS rule to look for IP fragments that do not overlap correctly and non-final IP fragments carrying data that is not a multiple of 8 bytes in length.

10.Multiple choice test question

What best descibes the following trace?

```
09:45:12.171201 eth0 < spoofed.evil.net.56169 > goodness.org.3223: udp
28 (frag 242:36@0+)
09:45:12.171246 eth0 < spoofed.evil.net > goodness.org: (frag 242:4@24)
09:45:12.188516 eth0 < spoofed.evil.net.56169 > goodness.org.3223: udp
28 (frag 242:36@0+)
```

09:45:12.188566 eth0 < spoofed.evil.net > goodness.org: (frag 242:4@24)

A.) Network mapping

B.) Sesquipedalian DoS

C.) Teardrop DoS

D.) Traceroute

Answer: C

Assignment 2 - Evaluate an Attack

URL for Attack:

www.insecure.org Nmap 2.53

Command Run

```
Nmap –sF –O –P0 –D <decoy.devil.net> <goodness.net>

      -sF Stealth FIN
      -O  TCP/IP fingerprinting to guess OS
      -P0 Don't ping hosts
      -D  decoy
```

Description of attack: Stealth Scan for OS Detection

```
-*> Snort! <*-
Version 1.6
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
```

devil.net sends its packet with the FIN flag set to goodness.org port 1016 This is a stealthy way of determining if a given port is active An active port should not respond while a closed port should respond with a RST/ACK This type of scan is considered stealthy because some IDS will not pick it up

```
08/09-16:58:00.527708 devil.net:50458 -> goodness.net:1016
TCP TTL:55 TOS:0x0 ID:10263
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000
```

goodness.org responds with a packet with the RST/ACK flags set to devil.net This tell devil.net that goodness.org port 1016 is closed

```
08/09-16:58:00.527891 goodness.net:1016 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6418
```

```
****R*A*** Seq: 0x0   Ack: 0x0   Win: 0x0
00 00 00 00 00 00                                  ......
```

decoy.devil.net now sends its packet with the FIN flag set to goodness.org port 1016 goodness.org again responds with a packet with the RST/ACK flags set this time to decoy.devil.net Now goodness.org may not know who is the scanner and who is the decoy (there could have been multiple decoys)

```
08/09-16:58:00.528128 decoy.devil.net:50458 -> goodness.net:1016
TCP TTL:55 TOS:0x0 ID:33123
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000
```

This scenario repeats itself over and over

```
08/09-16:58:00.528254 devil.net:50458 -> goodness.net:521
TCP TTL:55 TOS:0x0 ID:44890
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.528399 goodness.net:521 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6420
****R*A*** Seq: 0x0   Ack: 0x0   Win: 0x0
00 00 00 00 B9 B5                                  ......

08/09-16:58:00.528529 decoy.devil.net:50458 -> goodness.net:521
TCP TTL:55 TOS:0x0 ID:11468
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.528656 devil.net:50458 -> goodness.net:528
TCP TTL:55 TOS:0x0 ID:57034
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.528775 decoy.devil.net:50458 -> goodness.net:528
TCP TTL:55 TOS:0x0 ID:17140
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.528796 goodness.net:528 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6422
****R*A*** Seq: 0x0   Ack: 0x0   Win: 0x0
00 00 00 00 2B 9B                                  ....+.

08/09-16:58:00.528997 devil.net:50458 -> goodness.net:1507
TCP TTL:55 TOS:0x0 ID:63144
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.529117 decoy.devil.net:50458 -> goodness.net:1507
TCP TTL:55 TOS:0x0 ID:19732
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.529137 goodness.net:1507 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6424
*****R*A*** Seq: 0x0   Ack: 0x0   Win: 0x0
02 04 01 09 01 01                                  ......

08/09-16:58:00.529340 devil.net:50458 -> goodness.net:720
TCP TTL:55 TOS:0x0 ID:2443
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000
```

```
08/09-16:58:00.529459 decoy.devil.net:50458 -> goodness.net:720
TCP TTL:55 TOS:0x0 ID:29073
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.529478 goodness.net:720 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6426
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
02 04 01 09 01 01                                  ......

08/09-16:58:00.529681 devil.net:50458 -> goodness.net:1379
TCP TTL:55 TOS:0x0 ID:60459
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.529799 decoy.devil.net:50458 -> goodness.net:1379
TCP TTL:55 TOS:0x0 ID:40574
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.529818 goodness.net:1379 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6428
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
02 04 02 18 CF 72                                  .....r

08/09-16:58:00.530020 devil.net:50458 -> goodness.net:1355
TCP TTL:55 TOS:0x0 ID:5361
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.530139 decoy.devil.net:50458 -> goodness.net:1355
TCP TTL:55 TOS:0x0 ID:46503
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.530160 goodness.net:1355 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6430
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
69 6E 20 74 68 65                                  in the

08/09-16:58:00.530363 devil.net:50458 -> goodness.net:34
TCP TTL:55 TOS:0x0 ID:29976
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.530482 decoy.devil.net:50458 -> goodness.net:34
TCP TTL:55 TOS:0x0 ID:31475
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.530502 goodness.net:34 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6432
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
51 29 7D 5F 5A A6                                  Q)}_Z.

08/09-16:58:00.552756 devil.net:50458 -> goodness.net:3984
TCP TTL:55 TOS:0x0 ID:52493
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.552899 goodness.net:3984 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6434
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
77 29 A3 A9 6D 28                                  w)..m(
```

```
08/09-16:58:00.552936 decoy.devil.net:50458 -> goodness.net:3984
TCP TTL:55 TOS:0x0 ID:58309
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.553289 devil.net:50458 -> goodness.net:633
TCP TTL:55 TOS:0x0 ID:65009
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.553410 decoy.devil.net:50458 -> goodness.net:633
TCP TTL:55 TOS:0x0 ID:16162
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.553427 goodness.net:633 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6436
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
65 75 D9 65 A7 5A                                  eu.e.Z

08/09-16:58:00.555840 devil.net:50458 -> goodness.net:951
TCP TTL:55 TOS:0x0 ID:57163
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.555984 goodness.net:951 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6438
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
00 00 00 00 68 65                                  ....he

08/09-16:58:00.556127 decoy.devil.net:50458 -> goodness.net:951
TCP TTL:55 TOS:0x0 ID:20334
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.556253 devil.net:50458 -> goodness.net:560
TCP TTL:55 TOS:0x0 ID:26038
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.556371 decoy.devil.net:50458 -> goodness.net:560
TCP TTL:55 TOS:0x0 ID:47508
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.556390 goodness.net:560 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6440
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
02 04 01 09 01 01                                  ......

08/09-16:58:00.556593 devil.net:50458 -> goodness.net:445
TCP TTL:55 TOS:0x0 ID:31834
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.556710 decoy.devil.net:50458 -> goodness.net:445
TCP TTL:55 TOS:0x0 ID:17532
***F**** Seq: 0x0   Ack: 0x0   Win: 0x1000

08/09-16:58:00.556730 goodness.net:445 -> devil.net:50458
TCP TTL:255 TOS:0x0 ID:6442
****R*A* Seq: 0x0   Ack: 0x0   Win: 0x0
02 04 01 09 01 01                                  ......
```

The above scan will continue. When it is done it will use the subtleties in the underlying operating system network stack of the computer being scaned to make a "fingerprint" of it. Then this fingerprint will be compared to its database of known OS "fingerprints".

Assignment 3 - "Analyze This" Scenario

Analysis of Snort detects collected from my.net between May 16th and June 23rd, 2000.

VA-CIRT 000218 – There were CIRT advisories on ports 34555 and 3555. These are known to be used by the Trinoo denial of service exploit. Below are the address that attempted to access these ports. Of possible concern is the fact that my.net.253.53:25 is scanning my.net.101.89:34555. Please be advised that due to space considerations only there first attempt is listed. Most of these address had multiple attempts to various systems on my.net.

05/23-06:01:05.735025	GIAC	218 VA-CIRT	port	34555 209.49.101.5:25	->	MY.NET.253.24:34555
05/23-07:48:23.995321	GIAC	218 VA-CIRT	port	35555 216.200.67.22:113	->	MY.NET.6.35:35555
05/24-00:10:33.940757	GIAC	218 VA-CIRT	port	35555 205.252.121.7:113	->	MY.NET.6.47:35555
05/24-10:39:05.598600	GIAC	218 VA-CIRT	port	35555 208.178.47.97:25	->	MY.NET.253.24:35555
05/24-11:03:35.440299	GIAC	218 VA-CIRT	port	34555 216.32.243.136:25	->	MY.NET.100.230:34555
05/24-21:36:09.427387	GIAC	218 VA-CIRT	port	35555 208.210.124.27:25	->	MY.NET.253.41:35555
05/25-01:47:17.966506	GIAC	218 VA-CIRT	port	34555 209.38.76.60:113	->	MY.NET.6.34:34555
05/25-04:00:48.153520	GIAC	218 VA-CIRT	port	34555 130.114.200.6:53	->	MY.NET.1.8:34555
05/25-04:05:11.344754	GIAC	218 VA-CIRT	port	34555 207.138.41.176:113	->	MY.NET.6.35:34555
05/25-09:04:45.535718	GIAC	218 VA-CIRT	port	35555 194.129.118.249:25	->	MY.NET.6.34:35555
05/25-11:21:05.328565	GIAC	218 VA-CIRT	port	34555 216.64.2.218:25	->	MY.NET.253.24:34555
05/25-12:15:41.750339	GIAC	218 VA-CIRT	port	35555 209.150.117.251:113	->	MY.NET.253.16:35555
05/26-10:52:31.465183	GIAC	218 VA-CIRT	port	34555 132.151.1.176:113	->	MY.NET.100.230:34555
05/26-11:12:02.962513	GIAC	218 VA-CIRT	port	34555 152.6.10.53:25	->	MY.NET.253.53:34555
05/26-11:12:14.537630	GIAC	218 VA-CIRT	port	34555 128.32.66.85:25	->	MY.NET.253.24:34555
05/26-11:47:16.686059	GIAC	218 VA-CIRT	port	35555 203.103.148.129:25	->	MY.NET.100.230:35555
05/26-12:16:20.156716	GIAC	218 VA-CIRT	port	35555 156.80.1.4:25	->	MY.NET.253.24:35555
05/26-18:43:28.020643	GIAC	218 VA-CIRT	port	34555 MY.NET.253.52:25	->	MY.NET.101.89:34555
05/26-22:01:22.934985	GIAC	218 VA-CIRT	port	34555 209.132.14.36:25	->	MY.NET.6.35:34555
05/27-02:02:36.233453	GIAC	218 VA-CIRT	port	34555 35.8.2.57:113	->	MY.NET.6.47:34555
05/27-19:56:02.733185	GIAC	218 VA-CIRT	port	35555 192.147.174.46:113	->	MY.NET.6.34:35555
05/28-05:37:28.990772	GIAC	218 VA-CIRT	port	35555 146.7.191.66:25	->	MY.NET.253.24:35555
05/28-07:40:41.111720	GIAC	218 VA-CIRT	port	35555 207.244.124.7:113	->	MY.NET.253.42:35555

Watchlist – the watchlist is made up of IP address that have demonstrated questionable behavior in the past. The watchlist generated a vast number of alerts from locations inside of China (Chinese Academy of Sciences was prevalent) and Israel. An analysis of these alerts not only indicated the detailed scanning of all well know ports on my.net, but a stream from 212.179.44.36:1213 (OTI-LAN, Israel) to my.net.217.86:6346 that took place on May 24th from 0157 to 0229. This incident will require further review. Below are the address from the watchlist that accessed my.net. Please be advised that due to space considerations only there first attempt is listed. Most of these address had multiple attempts to various systems on my.net.

05/23-00:02:56.631299	Watchlist	222 NET-NCFC	159.226.133.85:25	->	MY.NET.100.230:46552
05/23-05:13:22.138971	Watchlist	222 NET-NCFC	159.226.91.37:25	->	MY.NET.100.230:49563
05/23-10:19:15.956161	Watchlist	220 IL-ISDNNET-990517	212.179.31.8:2935	->	MY.NET.201.122:5500

05/23-10:34:35.971029	Watchlist	222 NET-NCFC	159.226.45.3:113	-> MY.NET.253.43:57794
05/23-12:48:33.428458	Watchlist	222 NET-NCFC	159.226.111.1:25	-> MY.NET.253.53:41682
05/23-15:16:11.106229	Watchlist	220 IL-ISDNNET-990517	212.179.26.233:6700	-> MY.NET.203.194:1289
05/23-15:43:00.006065	Watchlist	220 IL-ISDNNET-990517	212.179.26.233:6700	-> MY.NET.203.194:1289
05/23-16:59:19.035336	Watchlist	222 NET-NCFC	159.226.120.14:25	-> MY.NET.253.51:56082
05/23-17:47:53.359079	Watchlist	222 NET-NCFC	159.226.21.171:25	-> MY.NET.253.51:56536
05/23-21:35:38.464235	Watchlist	222 NET-NCFC	159.226.120.19:36164	-> MY.NET.253.42:25
05/24-01:31:53.275464	Watchlist	222 NET-NCFC	159.226.41.99:23	-> MY.NET.99.51:54054
05/24-01:57:25.752327	Watchlist	220 IL-ISDNNET-990517	212.179.44.36:1213	-> MY.NET.217.86:6346
05/24-03:38:38.245412	Watchlist	222 NET-NCFC	159.226.5.188:25	-> MY.NET.100.230:62574
05/24-06:05:44.198986	Watchlist	222 NET-NCFC	159.226.5.65:25	-> MY.NET.100.230:63898
05/24-06:43:27.768652	Watchlist	222 NET-NCFC	159.226.21.134:113	-> MY.NET.6.47:37348
05/24-07:08:13.397359	Watchlist	220 IL-ISDNNET-990517	212.179.13.6:6699	-> MY.NET.219.158:2642
05/24-07:13:19.139014	Watchlist	220 IL-ISDNNET-990517	212.179.102.136:1618	-> MY.NET.202.130:41033
05/24-13:37:24.051243	Watchlist	222 NET-NCFC	159.226.5.77:25	-> MY.NET.100.230:36795
05/24-20:24:14.739805	Watchlist	222 NET-NCFC	159.226.228.1:113	-> MY.NET.100.230:41565
05/24-20:44:48.149005	Watchlist	222 NET-NCFC	159.226.5.83:113	-> MY.NET.100.230:41691
05/25-06:43:22.926100	Watchlist	220 IL-ISDNNET-990517	212.179.7.187:1027	-> MY.NET.204.70:5500
05/25-10:52:45.387335	Watchlist	220 IL-ISDNNET-990517	212.179.104.194:1706	-> MY.NET.204.70:5500
05/25-20:57:44.615739	Watchlist	222 NET-NCFC	159.226.92.9:113	-> MY.NET.145.9:42816
05/26-08:15:07.701311	Watchlist	222 NET-NCFC	159.226.1.8:25	-> MY.NET.6.7:9881
05/26-09:07:07.750003	Watchlist	220 IL-ISDNNET-990517	212.179.31.2:1396	-> MY.NET.201.122:5500
05/26-09:32:29.618100	Watchlist	222 NET-NCFC	159.226.5.152:713	-> MY.NET.100.165:80
05/26-11:52:54.248464	Watchlist	222 NET-NCFC	159.226.63.200:1174	-> MY.NET.100.230:113
05/26-19:43:55.212038	Watchlist	222 NET-NCFC	159.226.5.222:1079	-> MY.NET.100.230:113
05/27-10:51:49.990830	Watchlist	220 IL-ISDNNET-990517	212.179.2.188:1091	-> MY.NET.97.103:15502

External procedure call - it is believed that the majority of recent denial of service attacks are from systems victimized by remote procedure call vulnerabilities. Therefore any external remote procedure call should be carefully examined. The logs indicated that there were three external procedure calls made all from 216.148.73.6:2666. Please be advised that due to space considerations only there first attempt is listed.

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

Sun RPC high port access - it is believed that the majority of recent denial of service attacks are from systems victimized by remote procedure call vulnerabilities. Therefore any remote procedure call high port access should be carefully examined. Of concern were the 1,137 high port accesses made by my.net.253.12:43746 to numerous my.net systems on port 32,771. This incident will require further review. Below are the addresses that obtained high port access to my.net. Please be advised that due to space considerations only there first attempt is listed.

05/24-14:18:05.175232	SUNRPC	highport	access!	128.8.10.141:23	->	MY.NET.2.203:32771
05/27-22:47:39.173725	SUNRPC	highport	access!	199.60.228.130:7000	->	MY.NET.97.106:32771
05/28-14:30:50.876461	SUNRPC	highport	access!	MY.NET.253.12:43746	->	MY.NET.16.0:32771

Attempted Sun RPC high port access – it is believed that the majority of recent denial of service attacks are from systems victimized by remote procedure call vulnerabilities. Below are the address from the logs that attempted high port access to my.net. Of concern is the 3,777 attempts that 205.188.153.113:4000 (America Online, Inc.) made to my.net.97.209:32771 from

May 24th at 0656 through May 28th at 2359. This incident will require further review. Below are the addresses from which the high port access was received. Please be advised that due to space considerations only there first attempt is listed.

05/23-16:32:09.288704	Attempted	Sun	RPC	high	port	access	205.188.179.41:4000	->	MY.NET.219.126:32771
05/24-06:56:35.441654	Attempted	Sun	RPC	high	port	access	205.188.153.113:4000	->	MY.NET.97.209:32771

Wingate connects/attempts – wingate proxy server commonly operates on ports 8080 or 1080. These ports are prone to probes because: 1) vulnerabilities with some versions of wingate allow an intruder access to the servers hard drive 2) intruders may use wingate proxies in an attempt to stay anonymous while on the internet 3) port 1080 is also known for the WinHole Trojan. Below are the address which accessed ports 8080 or 1080. Please be advised that due to space considerations only a sample is listed.

05/23-07:12:42.180663	WinGate	8080	Attempt	165.247.85.202:1168	->	MY.NET.253.105:8080
05/23-12:33:43.110655	WinGate	1080	Attempt	140.186.45.26:42660	->	MY.NET.202.38:1080
05/23-21:58:15.109412	WinGate	8080	Attempt	172.137.251.115:1118	->	MY.NET.253.105:8080
05/24-01:15:38.410099	WinGate	1080	Attempt	166.62.172.96:1301	->	MY.NET.97.113:1080
05/24-10:20:11.040668	WinGate	8080	Attempt	134.192.118.145:1098	->	MY.NET.253.105:8080
05/24-12:09:28.363242	WinGate	8080	Attempt	172.144.105.37:1030	->	MY.NET.253.105:8080
05/24-13:50:44.335886	WinGate	8080	Attempt	136.160.4.156:1244	->	MY.NET.253.105:8080
05/24-19:26:54.661379	WinGate	8080	Attempt	152.172.213.42:1052	->	MY.NET.253.105:8080
05/24-20:01:58.258711	WinGate	1080	Attempt	143.248.203.5:1158	->	MY.NET.60.16:1080
05/24-20:54:00.558420	WinGate	1080	Attempt	130.207.197.83:20	->	MY.NET.111.125:1080
05/24-20:57:01.397476	WinGate	1080	Attempt	129.242.219.27:1960	->	MY.NET.97.240:1080
05/25-00:51:48.301745	WinGate	8080	Attempt	158.135.8.148:4526	->	MY.NET.162.54:8080
05/25-10:30:35.660341	WinGate	8080	Attempt	136.160.5.145:1978	->	MY.NET.253.105:8080
05/25-14:48:36.329760	WinGate	8080	Attempt	156.106.192.3:2571	->	MY.NET.99.85:8080
05/25-15:05:24.185102	WinGate	8080	Attempt	152.175.240.195:1331	->	MY.NET.253.105:8080
05/25-15:53:34.609297	WinGate	8080	Attempt	172.131.129.222:1031	->	MY.NET.253.105:8080
05/25-16:08:55.436056	WinGate	8080	Attempt	172.143.228.52:1031	->	MY.NET.253.105:8080
05/25-16:21:38.065117	WinGate	8080	Attempt	156.106.194.184:1133	->	MY.NET.99.85:8080
05/25-16:25:41.396514	WinGate	1080	Attempt	168.143.0.8:20	->	MY.NET.97.209:1080
05/25-19:59:53.736582	WinGate	8080	Attempt	152.173.32.11:1156	->	MY.NET.253.105:8080
05/25-20:59:56.117100	WinGate	1080	Attempt	131.188.3.83:48063	->	MY.NET.201.10:1080
05/26-01:55:40.110970	WinGate	1080	Attempt	128.177.243.155:31263	->	MY.NET.100.65:1080
05/26-08:26:41.038335	WinGate	8080	Attempt	172.135.196.64:1033	->	MY.NET.253.105:8080
05/26-09:37:13.976583	WinGate	8080	Attempt	172.135.231.24:1033	->	MY.NET.253.105:8080
05/26-09:42:17.286518	WinGate	8080	Attempt	152.167.104.75:1103	->	MY.NET.253.105:8080
05/26-09:58:51.774026	WinGate	8080	Attempt	131.118.254.204:1028	->	MY.NET.253.105:8080
05/26-10:38:04.702874	WinGate	8080	Attempt	172.145.95.189:1054	->	MY.NET.253.105:8080
05/26-10:56:49.829342	WinGate	8080	Attempt	131.167.220.90:1125	->	MY.NET.253.105:8080
05/26-11:27:46.073334	WinGate	8080	Attempt	128.231.171.123:1037	->	MY.NET.253.105:8080
05/26-11:32:53.257699	WinGate	8080	Attempt	163.30.77.5:1990	->	MY.NET.15.248:8080
05/26-13:10:18.757795	WinGate	8080	Attempt	172.143.218.174:1032	->	MY.NET.253.105:8080
05/26-14:47:07.499687	WinGate	8080	Attempt	156.106.194.165:1157	->	MY.NET.99.85:8080
05/26-15:35:32.481583	WinGate	8080	Attempt	128.138.242.196:34351	->	MY.NET.99.85:8080
05/26-15:42:55.087455	WinGate	8080	Attempt	152.166.101.66:1323	->	MY.NET.253.105:8080
05/26-16:09:15.095955	WinGate	8080	Attempt	172.128.138.102:1235	->	MY.NET.97.69:8080
05/26-18:55:08.248179	WinGate	8080	Attempt	152.170.79.224:1922	->	MY.NET.253.105:8080
05/26-19:17:41.742570	WinGate	8080	Attempt	152.166.9.60:2156	->	MY.NET.253.105:8080

05/26-19:53:27.824229	WinGate	8080	Attempt	172.129.120.186:1038	->	MY.NET.253.105:8080
05/26-20:29:45.172878	WinGate	8080	Attempt	172.134.169.168:1031	->	MY.NET.253.105:8080
05/27-01:57:15.532713	WinGate	8080	Attempt	150.101.250.214:3095	->	MY.NET.97.203:8080
05/27-02:28:53.723899	WinGate	8080	Attempt	172.138.111.78:1462	->	MY.NET.97.203:8080
05/27-02:42:44.976384	WinGate	8080	Attempt	172.131.60.184:1064	->	MY.NET.97.203:8080
05/27-02:51:12.337159	WinGate	8080	Attempt	172.130.183.134:1323	->	MY.NET.97.203:8080
05/27-10:06:23.780855	WinGate	8080	Attempt	128.2.179.17:3256	->	MY.NET.99.85:8080
05/27-12:28:01.420304	WinGate	8080	Attempt	156.106.194.147:1160	->	MY.NET.99.85:8080
05/27-14:33:38.433229	WinGate	8080	Attempt	152.172.115.93:3398	->	MY.NET.253.105:8080
05/27-19:23:57.550117	WinGate	1080	Attempt	129.78.64.1:64009	->	MY.NET.97.61:1080
05/28-04:20:20.939268	WinGate	8080	Attempt	156.106.194.183:2138	->	MY.NET.99.85:8080
05/28-09:06:40.751753	WinGate	8080	Attempt	172.138.132.4:1418	->	MY.NET.253.105:8080
05/28-10:07:45.654537	WinGate	8080	Attempt	130.67.120.127:1468	->	MY.NET.253.83:8080
05/28-10:58:46.362522	WinGate	8080	Attempt	156.106.194.185:1201	->	MY.NET.99.85:8080
05/28-12:08:32.446183	WinGate	8080	Attempt	172.135.239.231:1031	->	MY.NET.253.105:8080
05/28-16:58:53.680777	WinGate	1080	Attempt	168.120.16.250:45260	->	MY.NET.97.189:1080
05/28-17:08:51.656301	WinGate	1080	Attempt	130.194.9.1:1286	->	MY.NET.97.145:1080
05/28-18:13:42.684820	WinGate	8080	Attempt	156.106.194.195:1079	->	MY.NET.99.85:8080
05/28-23:22:40.378908	WinGate	1080	Attempt	136.160.130.100:20	->	MY.NET.97.56:1080
05/28-23:47:45.494551	WinGate	1080	Attempt	165.247.192.187:3543	->	MY.NET.97.32:1080
05/28-23:48:34.497771	WinGate	1080	Attempt	172.140.228.182:1197	->	MY.NET.97.32:1080

Happy 99 virus – it is possible that one or more of the my.net computer systems may now be infected with the happy 99 virus. This incident will require further review. Below is the address involving 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

Scanning – my.net has been heavily scanned and mapped. Since scans are often a prelude to an attack they warrant further review. Below are some examples.

Nmap scan – Nmap is a network mapping tool. Of particular concern is the extensive mapping of my.net conducted by my.net.253.12:43756. This incident will require further review. Below are the addresses of concern. Please be advised that due to space considerations only there first attempt is listed.

05/27-02:04:27.903992	NMAP	TCP	ping!	141.223.180.1:80	->	MY.NET.6.7:80
05/27-23:44:47.358888	NMAP	TCP	ping!	MY.NET.253.12:43756	->	MY.NET.14.1:7
05/28-00:24:01.616425	NMAP	TCP	ping!	216.204.66.115:46528	->	MY.NET.20.10:23

Null scan – is a network mapping technique where a packet is sent in which no TCP flags are set. Below are the addresses of concern. Please be advised that due to space considerations only a sample is listed.

05/23-02:42:09.638598	Null	scan!	212.33.69.5:2012	->	MY.NET.218.82:6346
05/23-05:16:47.290377	Null	scan!	130.104.21.77:2759	->	MY.NET.204.194:2340
05/23-12:54:10.739033	Null	scan!	194.159.44.223:27065	->	MY.NET.20.10:27005
05/23-13:59:03.530996	Null	scan!	212.187.76.51:1675	->	MY.NET.204.194:2340
05/23-14:16:48.019242	Null	scan!	212.187.76.51:1675	->	MY.NET.204.194:2340

05/23-15:14:45.571703	Null	scan!	193.225.22.16:6688	->	MY.NET.160.143:2086
05/23-15:24:16.118707	Null	scan!	200.128.19.16:6699	->	MY.NET.205.174:2599
05/23-20:12:29.597171	Null	scan!	207.191.12.226:6699	->	MY.NET.100.196:49209
05/23-21:08:07.278961	Null	scan!	194.247.69.133:1080	->	MY.NET.20.10:2330
05/24-00:30:51.020597	Null	scan!	129.2.203.50:6699	->	MY.NET.201.78:1740
05/24-01:18:13.903830	Null	scan!	195.11.243.27:27075	->	MY.NET.20.10:1235
05/24-05:24:39.175717	Null	scan!	209.122.184.63:6688	->	MY.NET.97.101:1448
05/24-10:24:54.290052	Null	scan!	128.194.31.15:2670	->	MY.NET.203.22:6699
05/24-16:43:58.081202	Null	scan!	194.70.126.10:1406	->	MY.NET.253.42:27501
05/24-21:13:11.477040	Null	scan!	194.247.69.132:18902	->	MY.NET.20.10:48129
05/24-21:13:11.477040	Null	scan!	194.247.69.132:18902	->	MY.NET.20.10:48129
05/24-21:31:37.059137	Null	scan!	195.11.226.229:9999	->	MY.NET.20.10:1084
05/24-22:01:03.215612	Null	scan!	194.217.242.35:27055	->	MY.NET.253.24:19409
05/25-04:59:41.338687	Null	scan!	212.33.69.5:2125	->	MY.NET.218.82:6346
05/25-09:24:08.266435	Null	scan!	194.159.188.15:6970	->	MY.NET.153.110:6770
05/25-12:31:37.740741	Null	scan!	194.217.242.20:27964	->	MY.NET.1.2:27960
05/26-02:17:58.399333	Null	scan!	169.237.30.234:6688	->	MY.NET.201.6:1040
05/26-12:31:14.394452	Null	scan!	194.217.242.88:27990	->	MY.NET.1.2:27960
05/27-01:38:07.852324	Null	scan!	195.173.151.254:27960	->	MY.NET.20.10:27960
05/27-12:00:08.720279	Null	scan!	194.247.68.105:27960	->	MY.NET.20.10:27960
05/27-16:21:32.733041	Null	scan!	194.159.250.7:10667	->	MY.NET.20.10:10666
05/27-16:21:32.733041	Null	scan!	194.159.250.7:10667	->	MY.NET.20.10:10666
05/27-18:43:37.407428	Null	scan!	195.173.142.46:27970	->	MY.NET.20.10:27960
05/28-16:18:21.004316	Null	scan!	212.242.100.188:1379	->	MY.NET.162.196:5504

Tiny fragments – fragment the header to be less than 20 bytes. They are used as part of network mapping and for DoS attacks against vulnerable operating systems. This incident will require further review. Below are the addresses of concern. Please be advised that due to space considerations only a sample is listed.

05/23-15:24:32.519971	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.147:32771	TCP(55),	UDP(0)
05/23-15:24:44.262475	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.148:32771	TCP(55),	UDP(0)
05/23-15:24:58.105314	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.149:32771	TCP(50),	UDP(0)
05/23-15:25:07.770044	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.150:32771	TCP(45),	UDP(0)
05/23-15:25:28.421673	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.151:32771	TCP(49),	UDP(0)
05/23-15:25:47.687593	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.152:32771	TCP(45),	UDP(0)
05/23-15:26:02.514861	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.153:32771	TCP(2),	UDP(1)
05/23-15:26:12.814314	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.154:32771	TCP(2),	UDP(1)
05/23-15:26:27.154945	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.155:32771	TCP(50),	UDP(0)
05/23-15:26:39.879961	Tiny	Fragments	-	Possible	Hostile	Activity	MY.NET.16.156:32771	TCP(50),	UDP(0)

My.net – for further review: 1) My.net.253.12 as mentioned above is scanning the internal network (Sun RPC high port access) 2) My.net.254.52 as mentioned above scanned my.net.253.52 for port 34555, which is known for the trinoo exploit (VA-CIRT 000218).

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
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced