Global Information Assurance Certification Paper

*** Northcutt, started out with a wonderful tutorial style but I think Jack ran out of time and the analysis suffers for that. Still I like some the traces a lot, don't remember seeing DNS reply content on a ftp99cmp before, in fact thought ftp99 ran on TCP :) This is just like the back orifice trace in your book in the false positive section, if it quacks like a DNS reply then don't focus on the dest port :) The netbios looks quite normal (unmangled) as well. Even so, there are some pretty traces here! 74 *

Intrusion Detection Analysis
Practical analysis of network traffic
Submitted by Jack Reed

Sample #1 Routine telnet session.

```
This first trace is part validation of what I've learned, and part getting
familiar with tcpdump. The client machine mdacitis2 has initiated a telnet
connection with elduke. The 3-way handshake is completed normally, data is
exchanged, and the client requests the session be terminated. Both sides issue
and acknowledge the FIN request.  This was intentional traffic, created for the
purpose of this analysis, with no cause for alarm.

10:17:23.305545 mdacitis2.32840 > elduke.telnet: S 335838160:335838160(0) win
8760 <mss 1460> (DF)
10:17:23.306240 elduke.telnet > mdacitis2.32840: S 1271278698:1271278698(0) ack
335838161 win 8760 <mss 1460> (DF)
10:17:23.307328 mdacitis2.32840 > elduke.telnet: . ack 1 win 8760 (DF)
10:17:23.308306 mdacitis2.32840 > elduke.telnet: P 1:25(24) ack 1 win 8760 (DF)
10:17:23.308403 elduke.telnet > mdacitis2.32840: . ack 25 win 8760 (DF)
10:17:23.341470 elduke.telnet > mdacitis2.32840: P 1:16(15) ack 25 win 8760 (DF)
10:17:23.342103 mdacitis2.32840 > elduke.telnet: . ack 16 win 8760 (DF)
10:17:23.342153 elduke.telnet > mdacitis2.32840: P 16:31(15) ack 25 win 8760
(DF)
10:17:23.342447 mdacitis2.32840 > elduke.telnet: P 25:40(15) ack 16 win 8760
(DF)
10:17:23.390045 mdacitis2.32840 > elduke.telnet: . ack 31 win 8760 (DF)
10:17:23.390098 elduke.telnet > mdacitis2.32840: P 31:49(18) ack 40 win 8760
(DF)
10:17:23.392519 mdacitis2.32840 > elduke.telnet: P 40:57(17) ack 49 win 8760
(DF)
10:17:23.393876 elduke.telnet > mdacitis2.32840: P 49:70(21) ack 57 win 8760
(DF)
10:17:23.440052 mdacitis2.32840 > elduke.telnet: . ack 70 win 8760 (DF)
10:17:23.440114 elduke.telnet > mdacitis2.32840: P 70:83(13) ack 57 win 8760
(DF)
10:17:23.441097 mdacitis2.32840 > elduke.telnet: P 57:63(6) ack 83 win 8760 (DF)
10:17:23.441306 elduke.telnet > mdacitis2.32840: P 83:86(3) ack 63 win 8760 (DF)
10:17:23.489983 mdacitis2.32840 > elduke.telnet: . ack 86 win 8760 (DF)
10:17:57.223519 mdacitis2.32840 > elduke.telnet: F 63:63(0) ack 86 win 8760 (DF)
10:17:57.223562 elduke.telnet > mdacitis2.32840: . ack 64 win 8760 (DF)
10:17:57.234151 elduke.telnet > mdacitis2.32840: F 86:86(0) ack 64 win 8760 (DF)
10:17:57.234805 mdacitis2.32840 > elduke.telnet: . ack 87 win 8760 (DF)
```

Sample #2 sendmail session not available

This sample depicts a request to establish a session with the smtp service, but the process is unavailable, so the server returns a RESET. This was intentional traffic, created for the purpose of this analysis, with no cause for alarm.

```
10:34:21.742913 mdacitis2.32841 > elduke.smtp: S 463232102:463232102(0) win 8760
<mss 1460> (DF)
10:34:21.742956 elduke.smtp > mdacitis2.32841: R 0:0(0) ack 463232103 win 0 (DF)
```

The same exchange with sendmail running, available to accept the SYN request to establish a session. The 3-way handshake completes and data is exchanged. A normal termination is requested.

```
10:40:05.731863 mdacitis2.32842 > elduke.smtp: S 506251022:506251022(0) win 8760
<mss 1460> (DF)
10:40:05.731908 elduke.smtp > mdacitis2.32842: S 1441683746:1441683746(0) ack
506251023 win 8760 <mss 1460> (DF)
10:40:05.732559 mdacitis2.32842 > elduke.smtp: . ack 1 win 8760 (DF)
10:40:05.819337 elduke.smtp > mdacitis2.32842: P 1:94(93) ack 1 win 8760 (DF)
10:40:05.820278 mdacitis2.32842 > elduke.smtp: . ack 94 win 8760 (DF)
10:40:15.832202 mdacitis2.32842 > elduke.smtp: P 1:12(11) ack 94 win 8760 (DF)
10:40:15.832250 elduke.smtp > mdacitis2.32842: . ack 12 win 8760 (DF)
10:40:15.856387 elduke.smtp > mdacitis2.32842: P 94:135(41) ack 12 win 8760 (DF)
10:40:15.900990 mdacitis2.32842 > elduke.smtp: . ack 135 win 8760 (DF)
10:40:20.295049 mdacitis2.32842 > elduke.smtp: P 12:18(6) ack 135 win 8760 (DF)
10:40:20.295495 elduke.smtp > mdacitis2.32842: P 135:169(34) ack 18 win 8760
(DF)
10:40:20.340945 mdacitis2.32842 > elduke.smtp: . ack 169 win 8760 (DF)
10:40:24.698624 mdacitis2.32842 > elduke.smtp: P 18:24(6) ack 169 win 8760 (DF)
10:40:24.698937 elduke.smtp > mdacitis2.32842: P 169:211(42) ack 24 win 8760
(DF)
10:40:24.699384 elduke.smtp > mdacitis2.32842: F 211:211(0) ack 24 win 8760 (DF)
10:40:24.700432 mdacitis2.32842 > elduke.smtp: . ack 212 win 8760 (DF)
10:40:24.700937 mdacitis2.32842 > elduke.smtp: F 24:24(0) ack 212 win 8760 (DF)
10:40:24.701052 elduke.smtp > mdacitis2.32842: . ack 25 win 8760 (DF)
```

Sample #3 Normal ICMP requests

The following is a single ping request. This is normal traffic, created for the purpose of this analysis, and should produce no cause for alarm.

```
11:11:35.986707 mdacitis2 > elduke: icmp: echo request (DF)
11:11:35.986756 elduke > mdacitis2: icmp: echo reply (DF)
```

... and this is a ping request with a packet size of 4096 plus the 8 byte ICMP header, (1480+1480+1144)

```
11:14:00.998113 elduke > mdacitis2: icmp: echo reply (frag 46081:1480@0+)
11:14:00.998166 elduke > mdacitis2: (frag 46081:1480@1480+)
11:14:00.998201 elduke > mdacitis2: (frag 46081:1144@2960)
```

Sample #4 FIN Scan packet

This packet was alerted by snort on a redhat linix system as suspicious.
Packets with the FIN flag set typically don't contain massive payloads.
The source port (20) indicates an ftp-data channel.
The data is not discernable, probably code, encrypted, or compressed.
The source IP is registered to a cable modem service provider.
This looks like a targeted attack. There is probably no cause for alarm; the target port is not open or listening on this box so the packet doesn't present any danger.

```
[**] FIN Scan [**]
04/14-16:03:31.283486 24.217.40.130:20 -> 208.188.225.125:1276
TCP TTL:47 TOS:0x0 ID:37613  DF
*F**** Seq: 0x6CFF527D   Ack: 0x782B5000   Win: 0x10A
00 14 04 FC 6C FF 52 7D 78 2B 50 00 00 01 01 0A  ....l.R}x+P.....
00 D0 AF AD 08 CA 22 2D 8C A9 1A 30 4E 03 C6 90  ......"-...0N...
A5 17 45 AA 1C 7C BE C3 56 04 3C B5 42 15 4E 28  ..E..|..V.<.B.N(
FD E9 CF 86 1A C4 34 C1 03 34 96 81 EB 50 5B A3  ......4..4...P[.
D7 B5 9C 3E F1 71 F6 37 2A A6 9D D6 6F 64 98 6B  ...>.q.7*...od.k
E2 64 7D 81 9C 06 F4 71 CB 2D C0 02 4A 34 96 94  .d}....q.-..J4..
EF 3B 6E 02 B1 2B 1C 4E 6C 83 30 4E 0A 0D 95 23  .;n..+.Nl.0N...#
57 4E 53 35 93 E4 16 28 F7 A2 C8 81 D7 E7 D3 3E  WNS5...(.......>
8C FA C6 BA 7C B8 46 0C 7F E1 4F 2D 18 34 26 9D  ....|.F...O-.4&.
19 29 73 2F 01 AE C3 20 02 58 01 13 44 46 95 B7  .)s/... .X..DF..
60 02 B2 04 9C 84 10 D2 CB 66 80 95 AF CC 6D 46  `........f....mF
6D 76 B1 05 B6 84 C1 74 D2 3F 14 34 AB 2B C5 52  mv.....t.?.4.+.R
82 E3 4C 31 DC A2 EB 12 94 73 70 BD C8 1A 6D 83  ..L1.....sp...m.
35 A8 6C 4C BA D9 AB 0B 17 6C D7 80 03 32 48 54  5.lL.....l...2HT
D3 09 32 E4 59 47 1A 9D 61 26 39 0C B9 1B 53 4C  ..2.YG..a&9...SL
25 0B 99 1C 8D 6A 75 84 98 E4 19 90 23 9B 91 5A  %....ju.....#..Z
05 85 D0 95 54 F0 4D 04 02 80 C1 E3 66 4A 8E 4B  ....T.M.....fJ.K
A3 53 82 C3 F6 39 97 03 38 05 C7 19 76 CB C0 34  .S...9..8...v..4
38 89 08 CB 2E 91 C3 28 99 0E AC DC FB 7D EC 49  8......(.....}.I
02 A8 45 CE 52 16 13 F0 64 9A 44 03 08 03 3A F6  ..E.R...d.D...:.
39 90 0A 29 C6 A6 DB DB F9 D8 AC 73 AD 28 79 67  9..).......s.(yg
DC BE E8 EF 96 74 91 D1 11 52 4E C6 08 CD 51 6E  .....t...RN...Qn
A0 C1 F4 C0 A6 20 24 51 2A 4B 70 0A 0A 10 F3 50  ..... $Q*Kp....P
90 24 5F F2 ED 32 44 67 CA 9E 51 89 0B AC A8 8E  .$_..2Dg..Q.....
B7 D9 1A 7C 13 D5 5C 2E 96 B9 24 E5 B8 00 2E B5  ...|..\...$.....
8A 9F 1A AC CD 1E 0C 38 E9 C5 AC 38 FF AE B9 21  .......8...8...!
6A 23 A8 15 CA 2D 7E 39 B5 9E F7 3F E9 5F 57 CA  j#...-~9...?._W.
E5 0D F7 4F 5D 53 8A 8E 04 22 A3 62 A8 B7 63 6A  ...O]S...".b..cj
30 2E CC 2E AE 9A 4B B8 C5 F5 D8 8D C6 7F C9 CA  0.....K.........
24 D3 48 1E 65 42 13 C4 70 40 81 86 F0 C2 35 67  $.H.eB..p@....5g
78 40 C0 51 A2 52 6D 37 25 BA 83 3B 09 A4 D4 1D  x@.Q.Rm7%..;....
90 80 08 A1 AC 01 C9 72 B0 A8 9D C5 1F 7B A9 39  .......r.....{.9
B0 8C 4A A1 45 A1 6C 2D A9 78 6A 60 97 0F 92 D3  ..J.E.l-.xj`....
9D 03 A0 FF D0 EF DF F2 9B EC 7F 58 FE 9B 5B E5  ...........X..[.
3D D7 F1 D3 9C 93 0D 5C 6A 53 7C AF BF 59 BB A7  =......\jS|..Y..
EB B3 77 DB 7F F4 B7 56 5E 6A 97 82 15 FD 14 06  ..w....V^j......
59 50 87 BB 07 CE FD 41 46 4A 49 B6 9C 14 99 06  YP.....AFJI.....
01 25 51 A0 40 15 11 1D 67 6E 4B A1 82 35 22 26  .%Q.@...gnK..5"&
42 43 03 70 46 8C 95 46 30 1A 72 49 8D F5 95 51  BC.pF..F0.rI...Q
57 4C 75 96 7F 9C AB A8 F4 52 36 80 E2 28 47 27  WLu......R6..(G'
F3 5B 25 AD 51 99 C1 7A 5C E6 DF 81 8D 55 36 B9  .[%.Q..z\....U6.
0F 5E B7 69 69 36 7E 11 D4 AD D3 9B FF FB 92 6C  .^.ii6~........l
```

```
9A 80 03 95 48 54 53 0C E4 5C 8E 89 13 55 AC 25  ....HTS..\...U.%
2B 91 A2 A3 2A 29 86 19 33 4D 32 EC BF 27 25 4A  +...*)..3M2..'%J
E3 5A E4 46 A9 0C 56 97 92 46 EE 3D 78 A6 FF 39  .Z.F..V..F.=x..9
68 FA 55 E9 27 2D C0 1A 32 47 E6 C7 2B 03 2C 32  h.U.'-..2G..+.,2
25 FF 2D 1D 33 A7 04 CB E9 67 25 C8 8F EB 55 83  %.-.3....g%...U.
D3 A7 34 94 21 93 58 9C D7 5F E2 68 FD 7B F6 AA  ..4.!.X.._.h.{..
DE DB 9D EE 24 F3 B4 BF F3 C9 97 38 3B BD BA B7  ....$......8;...
D3 13 41 0A 1B B8 40 92 A6 32 47 65 1F 72 36 08  ..A...@..2Ge.r6.
CE 90 3B C0 0E 40 12 71 A2 ED DB 80 02 3C 8C 43  ..;..@.q.....<.C
18 15 53 57 A5 A8 7D A0 DA 39 98 EE 6A 3D 8B 65  ..SW..}..9..j=.e
57 AF 63 20 38 16 60 97 B2 4E 89 16 91 E2 28 DD  W.c 8.`..N....(.
C5 AD 33 EF 87 C8 2E E1 09 FF 23 97 B1 F3 4B 25  ..3.......#...K%
1F 57 07 20 86 2F 59 B3 29 5A 7D CF B5 8C A1 BF  .W. ./Y.)Z}.....
76 8C DD 67 AD CC 86 AF 27 3D 12 88 FE B3 78 9D  v..g....'=....x.
5A B6 D2 52 B5 94 6B 5B 7B D7 6A 8E EB 0E 08 14  Z..R..k[{.j.....
5E B3 52 30 00 15 11 9D 69 16 B1 8D 94 09 86 8C  ^.R0....i.......
1B 07 85 1D 14 0A 88 87 BF 3D 14 A8 19 8E 74 4C  .........=....tL
8B 98 E2 06 D4 16 09 EC 56 E1 AF 95 FF FF FF F0  ........V.......
E6 CF F7 FE 99 5C A5 3E 21 19 76 D8 FB DF 2F 9E  .....\.>!.v.../.
B8 79 C7 EF 39 F3 2D F3 F9 7F DB FF FF FC BD 73  .y..9.-........s
05 AF D4 A1 3D 1E 52 D2 14 90 F7 87 72 2D EB 94  ....=.R.....r-..
DA FF C0 1A 21 38 50 02 BE 57 BB 5E 78 D2 EE 6E  ....!8P..W.^x..n
51 31 58 D2 EE 25 2E 71 58 FD F5 35 30 46 6C 74  Q1X..%.qX..50Flt
FF 94 A5 CB E3 C9 89 EE 18 3E E3 A0 ED FF FB 92  .........>......
6C 7E 80 03 5F 44 D3 6B 29 4A EA 5D 48 AA 8A 61  l~.._D.k)J.]H..a
E6 34 CC 35 0B 53 AC 31 0B A9 57 16 AA 69 94 A5  .4.5.S.1..W..i..
32 4D A4 B7 E3 85 AD 24 F6 ED D3 DF A1 C4 8C 49  2M.....$.......I
99 F8 18 90 CF 8C 55 7B D3 1E 3E 91 8E 19 C2 AF  ......U{..>.....
35 CD 33 2B D4 2E 73 FF E3 F9 E4 62 6C B6 50 04  5.3+..s....bl.P.
58 89 0C FF 46 0B A2 96 84 A1 87 07 5E 25 91 6C  X...F.......^%.l
CE 9B 3A 6C CB 06 89 04 82 29 C5 96 4B BA 7E AF  ..:l.....)..K.~.
FA 4B 61 EE 16 0A 9E 2A 9A 75 19 F7 34 8A E0 9E  .Ka....*.u..4...
EB 98 B4 EF 50 4A EE 57 72 FF 77 A6 AF 83 A3 34  ....PJ.Wr.w....4
97 07 44 A2 58 CF BD F8 72 A4 F5 FF 80 65 70 B9  ..D.X...r....ep.
16 0A 18 A0 25 12 28 92 E6 C1 03 CA 01 CD 07 D3  ....%.(.........
6C 9A 0B 92 B9 24 8A 8F 85 D0 64 0C D4 EB 67 B0  l....$....d...g.
41 9C 24 15 44 84 81 2C 10 82 E5 0C D2 A0 44 03  A.$.D..,......D.
81 85 80 20 92 C4 10 90 6E 38 BC C3 08 3A 2B 43  ... ....n8...:+C
30 20 86 2B 82 C4 B3 AB 29 C5 63 8E 5E DA 9C A4  0 .+....).c.^...
16 EE 3C 11 61 4C 89 15 1B 9B 7F 80 18 13 CC 96  ..<.aL..........
A2 57 7E 58 7A CE 18 93 21 1C 3B C1 1B 27 1B 8C  .W~Xz...!.;..'..
D4 3F 22 C2 A4 DA CC 2C 3D E2 9F 7C B1 36 57 A0  .?"....,=..|.6W.
D4 27 ED 57 C6 A9 64 77 F3 67 CA A6 33 8B 31 62  .'.W..dw.g..3.1b
C6 BD 18 73 B5 F6 38 72 0E 5F 8B D1 9B 9E 8C 33  ...s..8r._.....3
1C 0C 9E 0D 9B 29 D8 CC B1 F6 0D AD 5E 9B 96 EC  .....).....^...
00 18 07 E9 37 2F CE 08 C2 48 01 AF 43 2F CB 4C  ....7/...H..C/.L
DD 7A FF 95 D0 3E 5A 0F 45 07 24 83 E1 88 8D 90  .z...>Z.E.$.....
81 30 48 B6 CD 7F 7F F9 FF FB 92 6C 7D D3 EB 09  .0H........l}...
1A 6A 5D 67 0A 8F 61 28 5D 0C A5 15 55 47 B0 C5  .j]g..a(]...UG..
99 6E 1D 6A 75 94 95 33 CB D9 3A 7F A4 73 A4 17  .n.ju..3..:..s..
A5 AF E9 02 CF FE 52 51                          ......RQ
```

Sample #5 Web Server probe

```
This appears to be a Microsoft Internet Information Server probe.
The _vti* files are FrontPage web directories that could provide
```

the requestor with detailed filesystem info for further exploitation.
The source address is a proxy server so the real origin is unknown.
It's doubtful this is dubious activity, but I have not uncovered any
information about what exploit snort's default rule here has alerted me to.
It looks as though the host is being scanned for specific web server
Configuration data. The host doesn't have any of these directories on
It, so there isn't much cause for alarm. There are patches to IIS software
that address vulnerabilities. These kind of attacks are a good reason to
be running snort!

```
[**] IIS vti_inf access attempt [**]
04/12-13:41:53.747199 12.13.248.12:52630 -> 208.188.225.121:80
TCP TTL:41 TOS:0x0 ID:62979  DF
***PA* Seq: 0x46B79F44   Ack: 0x4756E0BC   Win: 0x558C
47 45 54 20 2F 5F 76 74 69 5F 69 6E 66 2E 68 74  GET /_vti_inf.ht
6D 6C 20 48 54 54 50 2F 31 2E 30 0D 0A 4D 49 4D  ml HTTP/1.0..MIM
45 2D 56 65 72 73 69 6F 6E 3A 20 31 2E 30 0D 0A  E-Version: 1.0..
41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 55 73 65  Accept: */*..Use
72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61  r-Agent: Mozilla
2F 32 2E 30 20 28 63 6F 6D 70 61 74 69 62 6C 65  /2.0 (compatible
3B 20 4D 53 20 46 72 6F 6E 74 50 61 67 65 20 34  ; MS FrontPage 4
2E 30 29 0D 0A 41 63 63 65 70 74 3A 20 61 75 74  .0)..Accept: aut
68 2F 73 69 63 69 6C 79 0D 0A 50 72 61 67 6D 61  h/sicily..Pragma
3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 56 69 61 3A  : no-cache..Via:
20 4E 65 74 43 61 63 68 65 40 77 77 77 2D 73 74   NetCache@www-st
6C 2D 70 72 6F 78 79 31 2E 62 6F 65 69 6E 67 2E  l-proxy1.xxxxxx.
63 6F 6D 3A 20 56 65 72 73 69 6F 6E 20 4E 65 74  com: Version Net
41 70 70 20 52 65 6C 65 61 73 65 20 33 2E 34 44  App Release 3.4D
36 3A 20 4D 6F 6E 20 41 75 67 20 32 33 20 31 36  6: Mon Aug 23 16
3A 34 30 3A 31 39 20 50 44 54 20 31 39 39 39 2D  :40:19 PDT 1999-
53 6F 6C 61 72 69 73 0D 0A 44 61 74 65 3A 20 54  Solaris..Date: T
75 65 2C 20 31 31 20 41 70 72 20 32 30 30 30 20  ue, 11 Apr 2000
31 38 3A 34 33 3A 34 36 20 47 4D 54 0D 0A 48 6F  18:43:46 GMT..Ho
73 74 3A 20 32 30 38 2E 31 38 38 2E 32 32 35 2E  st: 208.188.225.
31 32 31 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E  121..Content-Len
67 74 68 3A 20 30 0D 0A 43 6F 6E 6E 65 63 74 69  gth: 0..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A  on: Keep-Alive..
0D 0A                                            ..
```

Sample #6 Netbios name probe

This is a netbios (UDP port 137) name probe. It appears to be a
targeted probe to this host. The content string CKAAAA..., is the
Samba-managled wildcard name "*" followed by null characters.
Under most circumstances, name service listeners are required to
reply to queries for this wildcard name as well as for their own
computernames. So the expected response is a list of resource
records containing a list of netbios names. Three hits in 3 seconds
is peculiar, also the ID values are being incremented by 256.
This is a targeted scan attack, designed to gather configuration information
about our machine. There is some concern here, since this Linix machine is
running SAMBA, more investigation is necessary before recommendations can be
made. Exposing SAMBA shares to the internet is not a smart move.

```
[**] SMB Name Wildcard [**]
04/07-08:01:18.905581 209.192.65.17:137 -> 208.188.225.121:137
UDP TTL:44 TOS:0x0 ID:2983
Len: 58
6C 3C 00 10 00 01 00 00 00 00 00 20 43 4B 41  l<.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAA..!
00 01                                         ..

[**] SMB Name Wildcard [**]
04/07-08:01:20.579581 209.192.65.17:137 -> 208.188.225.121:137
UDP TTL:44 TOS:0x0 ID:3239
Len: 58
6C 3E 00 10 00 01 00 00 00 00 00 20 43 4B 41  l>.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAA..!
00 01                                         ..

[**] SMB Name Wildcard [**]
04/07-08:01:21.883100 209.192.65.17:137 -> 208.188.225.121:137
UDP TTL:44 TOS:0x0 ID:3495
Len: 58
6C 40 00 10 00 01 00 00 00 00 00 20 43 4B 41  l@.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 00 00 21  AAAAAAAAAAAA..!
00 01                                         ..
```

Sample #7 Ping reconn

Someone is pinging us from a cable modem host.
This is reconn activity, designed to verify a target's existence. Cyberkit tools are internet utilities that come with a netscanner capable of pinging multiple targets at once. There isn't much that can be done here, other than a packet filtering this from responding. It's something almost all hosts reply to, and just how paranoid do you want to be?

```
[**] PING Windows Type [**]
03/15-01:46:37.097631 24.217.18.162 -> 208.188.225.125
ICMP TTL:16 TOS:0x0 ID:18437
ID:3   Seq:9  ECHO

[**] PING Windows Type [**]
03/15-01:46:38.127319 24.217.18.162 -> 208.188.225.125
ICMP TTL:16 TOS:0x0 ID:18949
ID:3   Seq:10  ECHO

[**] PING Windows Type [**]
03/15-01:46:39.136720 24.217.18.162 -> 208.188.225.125
ICMP TTL:16 TOS:0x0 ID:19205
ID:3   Seq:11  ECHO

[**] PING Windows Type [**]
```

```
03/15-01:46:40.126163 24.217.18.162 -> 208.188.225.125
ICMP TTL:16 TOS:0x0 ID:19461
ID:3   Seq:12  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:22.687609 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:46085
ID:3   Seq:13  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:22.888898 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:46597
ID:3   Seq:14  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:22.983611 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:46853
ID:3   Seq:15  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:23.185051 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:48133
ID:3   Seq:16  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:23.289114 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:48901
ID:3   Seq:17  ECHO

[**] PING CyberKit 2.2 Windows [**]
03/15-01:49:23.429936 24.217.18.162 -> 208.188.225.125
ICMP TTL:112 TOS:0x0 ID:49413
ID:3   Seq:18  ECHO
```

Sample #8 Netbus Trojan

This is a trojan scan, port 12345 is the signature for the netbus/gabanbus trojan. These are remote administration trojans that infect windows systems. nothing here... I haven't found a lot of information on this Trojan, so I'm not sure what to look for other than a listening 12345 port. It's not, so our machine is safe. Possibly this is Trojan code that's detectable by most up to date anti-virus software.

```
[**] Netbus/GabanBus [**]
04/03-15:54:03.903678 208.188.19.10:2840 -> 208.188.225.125:12345
TCP TTL:22 TOS:0x0 ID:48955  DF
S***** Seq: 0x30CA5F   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460


[**] Netbus/GabanBus [**]
04/03-15:57:09.847679 208.188.19.10:3076 -> 208.188.225.125:12345
```

```
TCP TTL:22 TOS:0x0 ID:39487  DF
S***** Seq: 0x33A082   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460


[**] Netbus/GabanBus [**]
04/03-15:57:26.864101 208.188.19.10:3077 -> 208.188.225.125:12345
TCP TTL:22 TOS:0x0 ID:40511  DF
S***** Seq: 0x33E363   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460


[**] Netbus/GabanBus [**]
04/02-19:19:16.046562 140.109.103.245:3584 -> 208.188.225.125:12345
TCP TTL:45 TOS:0x0 ID:52413  DF
S***** Seq: 0xA2EB928A   Ack: 0x0   Win: 0xB68
TCP Options => MSS: 1460 SackOK TS: 210852865 0 NOP NOP NOP NOP


[**] Netbus/GabanBus [**]
04/02-17:16:29.832688 208.188.23.68:4416 -> 208.188.225.125:12345
TCP TTL:22 TOS:0x0 ID:26938  DF
S***** Seq: 0xABB556   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460


[**] Netbus/GabanBus [**]
04/03-16:05:40.773534 208.188.19.10:4644 -> 208.188.225.125:12345
TCP TTL:22 TOS:0x0 ID:21612  DF
S***** Seq: 0x3B6F41   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460


[**] Netbus/GabanBus [**]
04/03-16:11:42.050723 208.188.19.10:4910 -> 208.188.225.125:12345
TCP TTL:22 TOS:0x0 ID:56944  DF
S***** Seq: 0x40F2D2   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460
```

Sample #9 VooDoo Doll Trojan

Similar to the GabanBus trojan, this is a probe looking to contact a trojan program on a windows machine. Destination port 1245 is the signature. This port isn't open on our machine either, so we aren't vulnerable. Ditto on documentation on this one as well. I start getting a little paranoid myself searching the web for hacker Tools.

```
[**] VooDoo Doll [**]
04/09-05:54:54.757144 151.164.1.8:53 -> 208.188.225.121:1245
UDP TTL:246 TOS:0x0 ID:6329  DF
Len: 46
06 95 81 82 00 01 00 00 00 00 00 00 08 70 31 31  .............p11
39 36 31 34 30 07 64 72 69 76 65 72 61 03 63 6F  96140.drivera.co
6D 00 00 06 00 01                                m.....
```

```
[**] VooDoo Doll [**]
04/09-05:54:55.035797 216.70.64.1:53 -> 208.188.225.121:1245
UDP TTL:45 TOS:0x0 ID:1918
Len: 46
06 95 81 82 00 01 00 00 00 00 00 00 08 70 31 31  .............p11
39 36 31 34 30 07 64 72 69 76 65 72 61 03 63 6F  96140.drivera.co
6D 00 00 06 00 01                                m.....

[**] VooDoo Doll [**]
04/09-05:54:55.164325 151.164.1.7:53 -> 208.188.225.121:1245
UDP TTL:246 TOS:0x0 ID:10069  DF
Len: 46
06 95 81 82 00 01 00 00 00 00 00 00 08 70 31 31  .............p11
39 36 31 34 30 07 64 72 69 76 65 72 61 03 63 6F  96140.drivera.co
6D 00 00 06 00 01                                m.....

[**] VooDoo Doll [**]
04/09-05:54:55.622438 216.70.64.2:53 -> 208.188.225.121:1245
UDP TTL:45 TOS:0x0 ID:54055
Len: 46
06 95 81 82 00 01 00 00 00 00 00 00 08 70 31 31  .............p11
39 36 31 34 30 07 64 72 69 76 65 72 61 03 63 6F  96140.drivera.co
6D 00 00 06 00 01                                m.....
```

Sample #10 FTP99cmp Trojan

Destination port 1492 signatures this trojan, similar to the others. Our port is not open, so we appear to safe. These Trojans are all Targeted attacks, probably with intent to be malicious or at the very Least, mischievous. When recognized, steps should always be taken to Verify your machine is not infected.

```
[**] FTP99cmp [**]
04/09-23:18:35.467634 151.164.1.8:53 -> 208.188.225.121:1492
UDP TTL:246 TOS:0x0 ID:35890  DF
Len: 175
07 11 81 80 00 01 00 01 00 02 00 02 03 32 32 35  .............225
03 31 38 38 03 32 30 38 07 69 6E 2D 61 64 64 72  .188.208.in-addr
04 61 72 70 61 00 00 06 00 01 C0 0C 00 06 00 01  .arpa...........
00 00 1A F3 00 31 03 6E 73 31 06 73 77 62 65 6C  .....1.ns1.swbel
6C 03 6E 65 74 00 0A 70 6F 73 74 6D 61 73 74 65  l.net..postmaste
72 C0 3A 0B EA 5F 5A 00 00 0E 10 00 00 03 84 00  r.:.._Z.........
09 3A 80 00 00 0E 10 C0 0C 00 02 00 01 00 00 1A  .:..............
F3 00 02 C0 36 C0 0C 00 02 00 01 00 00 1A F3 00  ....6...........
06 03 6E 73 32 C0 3A C0 36 00 01 00 01 00 00 1C  ..ns2.:.6.......
20 00 04 97 A4 01 01 C0 81 00 01 00 01 00 00 1C   ...............
20 00 04 97 A4 01 07                              ......
```

Sample #11 Sub Seven Trojan

Destination port 1243 signatures this trojan, similar to the others. This one is apparently well known by the experts. I seem to be missing where to look for information on the exact nature of these Trojans, but generally

they all represent mischievous activity. Our system is safe, this port is not listening. Virus checkers exist to help eradicate these from your systems.

```
[**] Possible SubSeven access [**]
04/02-17:16:29.735670 208.188.23.68:4415 -> 208.188.225.125:1243
TCP TTL:22 TOS:0x0 ID:26170  DF
S***** Seq: 0xABB4EC   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

[**] Possible SubSeven access [**]
04/02-17:16:30.415166 208.188.23.68:4415 -> 208.188.225.125:1243
TCP TTL:22 TOS:0x0 ID:31034  DF
S***** Seq: 0xABB4EC   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

[**] Possible SubSeven access [**]
04/02-17:16:31.038428 208.188.23.68:4415 -> 208.188.225.125:1243
TCP TTL:22 TOS:0x0 ID:35130  DF
S***** Seq: 0xABB4EC   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

[**] Possible SubSeven access [**]
04/02-17:16:31.704722 208.188.23.68:4415 -> 208.188.225.125:1243
TCP TTL:22 TOS:0x0 ID:38970  DF
S***** Seq: 0xABB4EC   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460
```

Note to reviewers:

Thanks for the opportunity to become certified level 1,
This has been an extremely interesting exercise, one that has helped me understand much more about layer 3 protocols and threats to network security. Today is 4/24/00, 30 days from the day I took the written test at SANS2000. Just under the wire!

Jack Reed

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