Global Information Assurance Certification Paper

SANS GIAC Certification
GCIA Practical Assignment
V 2.7 January 28, 2001

Brian Varine

Assignment 1

Detect 1 Analysis

```
[**] IDS181/shellcode-x86-nops [**]
02/16-19:22:49.960151 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:61461 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9BFA9733  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : BB 07 00 B4 0E CD 10 AC 84 C0 75 F4 B4 01 F9 C3   ..........u.....
010 : 52 B4 08 CD 13 88 F5 5A 72 F5 80 E1 3F 74 ED FA   R......Zr...?t..
020 : 66 8B 46 08 52 66 0F B6 D9 66 31 D2 66 F7 F3 88   f.F.Rf...f1.f...
030 : EB 88 D5 43 30 D2 66 F7 F3 88 D7 5A 66 3D FF 03   ...C0.f....Zf=..
040 : 00 00 FB 77 44 86 C4 C0 C8 02 08 E8 40 91 88 FE   ...wD.......@...
050 : 28 E0 8A 66 02 38 E0 72 02 88 E0 BF 05 00 C4 5E   (..f.8.r.......^
060 : 04 50 B4 02 CD 13 5B 73 0A 4F 74 1C 30 E4 CD 13   .P....[s.Ot.0...
070 : 93 EB EB 0F B6 C3 01 46 08 73 03 FF 46 0A D0 E3   .......F.s..F...
080 : 00 5E 05 28 46 02 77 88 C3 2E F6 06 99 08 80 0F   .^.(F.w.........
090 : 84 79 FF BB AA 55 52 B4 41 CD 13 5A 0F 82 6F FF   .y...UR.A..Z..o.
0a0 : 81 FB 55 AA 0F 85 64 FF F6 C1 01 0F 84 5D FF 89   ..U...d......]..
0b0 : EE B4 42 CD 13 C3 52 65 61 64 00 42 6F 6F 74 00   ..B...Read.Boot.
0c0 : 20 65 72 72 6F 72 0D 0A 00 80 90 90 90 90 90 90    error..........
0d0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0e0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 00 00 00   ................
0f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
100 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
110 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00   ................
120 : 01 00 A5 FF FF FF 00 00 00 00 50 C3 00 00 55 AA   ..........P...U.
130 : 23 21 2F 62 69 6E 2F 73 68 0A 23 0A 0A 23 20 54   #!/bin/sh.#..# T
140 : 68 69 73 20 69 73 20 72 63 2E 63 6F 6E 66 20 2D   his is rc.conf -
150 : 20 61 20 66 69 6C 65 20 66 75 6C 6C 20 6F 66 20    a file full of
160 : 75 73 65 66 75 6C 20 76 61 72 69 61 62 6C 65 73   useful variables
170 : 20 74 68 61 74 20 79 6F 75 20 63 61 6E 20 73 65    that you can se
180 : 74 20 0A 23 20 74 6F 20 63 68 61 6E 67 65 20 74   t .# to change t
190 : 68 65 20 64 65 66 61 75 6C 74 20 73 74 61 72 74   he default start
1a0 : 75 70 20 62 65 68 61 76 69 6F 72 20 6F 66 20 79   up behavior of y
```

```
1b0 : 6F 75 72 20 73 79 73 74 65 6D 2E 20 20 59 6F 75   our system.  You
1c0 : 20 73 68 6F 75 6C 64 0A 23 20 6E 6F 74 20 65 64    should.# not ed
1d0 : 69 74 20 74 68 69 73 20 66 69 6C 65 21 20 20 50   it this file!  P
1e0 : 75 74 20 61 6E 79 20 6F 76 65 72 72 69 64 65 73   ut any overrides
1f0 : 20 69 6E 74 6F 20 6F 6E 65 20 6F 66 20 74 68 65    into one of the
200 : 20 24 7B 72 63 5F 63 6F 6E 66 5F 66 69 6C 65 73    ${rc_conf_files
210 : 7D 0A 23 20 69 6E 73 74 65 61 64 20 61 6E 64 20   }.# instead and
220 : 79 6F 75 20 77 69 6C 6C 20 62 65 20 61 62 6C 65   you will be able
230 : 20 74 6F 20 75 70 64 61 74 65 20 74 68 65 73 65    to update these
240 : 20 64 65 66 61 75 6C 74 73 20 6C 61 74 65 72 20    defaults later
250 : 77 69 74 68 6F 75 74 0A 23 20 73 70 61 6D 6D 69   without.# spammi
260 : 6E 67 20 79 6F 75 72 20 6C 6F 63 61 6C 20 63 6F   ng your local co
270 : 6E 66 69 67 75 72 61 74 69 6F 6E 20 69 6E 66 6F   nfiguration info
280 : 72 6D 61 74 69 6F 6E 2E 0A 23 0A 23 20 54 68 65   rmation..#.# The
290 : 20 24 7B 72 63 5F 63 6F 6E 66 5F 66 69 6C 65 73    ${rc_conf_files
2a0 : 7D 20 66 69 6C 65 73 20 73 68 6F 75 6C 64 20 6F   } files should o
2b0 : 6E 6C 79 20 63 6F 6E 74 61 69 6E 20 76 61 6C 75   nly contain valu
2c0 : 65 73 20 77 68 69 63 68 20 6F 76 65 72 72 69 64   es which overrid
2d0 : 65 0A 23 20 76 61 6C 75 65 73 20 73 65 74 20 69   e.# values set i
2e0 : 6E 20 74 68 69 73 20 66 69 6C 65 2E 20 20 54 68   n this file.  Th
2f0 : 69 73 20 65 61 73 65 73 20 74 68 65 20 75 70 67   is eases the upg
300 : 72 61 64 65 20 70 61 74 68 20 77 68 65 6E 20 64   rade path when d
310 : 65 66 61 75 6C 74 73 0A 23 20 61 72 65 20 63 68   efaults.# are ch
320 : 61 6E 67 65 64 20 61 6E 64 20 6E 65 77 20 66 65   anged and new fe
330 : 61 74 75 72 65 73 20 61 72 65 20 61 64 64 65 64   atures are added
340 : 2E 0A 23 0A 23 20 41 6C 6C 20 61 72 67 75 6D 65   ..#.# All argume
350 : 6E 74 73 20 6D 75 73 74 20 62 65 20 69 6E 20 64   nts must be in d
360 : 6F 75 62 6C 65 20 6F 72 20 73 69 6E 67 6C 65 20   ouble or single
370 : 71 75 6F 74 65 73 2E 0A 23 0A 23 20 24 46 72 65   quotes..#.# $Fre
380 : 65 42 53 44 3A 20 73 72 63 2F 65 74 63 2F 64 65   eBSD: src/etc/de
390 : 66 61 75 6C 74 73 2F 72 63 2E 63 6F 6E 66 2C 76   faults/rc.conf,v
3a0 : 20 31 2E 35 33 2E 32 2E 31 33 20 32 30 30 30 2F    1.53.2.13 2000/
3b0 : 31 31 2F 31 31 20 32 30 3A 33 33 3A 34 30 20 6A   11/11 20:33:40 j
3c0 : 6B 68 20 45 78 70 20 24 0A 0A 23 23 23 23 23 23   kh Exp $..######
3d0 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
3e0 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
3f0 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
400 : 23 23 23 23 23 23 23 23 0A 23 23 23 20 20 49 6D   ########.###  Im
410 : 70 6F 72 74 61 6E 74 20 69 6E 69 74 69 61 6C 20   portant initial
420 : 42 6F 6F 74 2D 74 69 6D 65 20 6F 70 74 69 6F 6E   Boot-time option
430 : 73 20 20 23 23 23 23 23 23 23 23 23 23 23 23 23   s  ##############
440 : 23 23 23 23 23 23 23 0A 23 23 23 23 23 23 23 23   #######.########
450 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
460 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
470 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23   ################
480 : 23 23 23 23 23 23 0A 0A 73 77 61 70 66 69 6C 65   ######..swapfile
490 : 3D 22 4E 4F 22 09 09 23 20 53 65 74 20 74 6F 20   ="NO"..# Set to
4a0 : 6E 61 6D 65 20 6F 66 20 73 77 61 70 66 69 6C 65   name of swapfile
4b0 : 20 69 66 20 61 75 78 20 73 77 61 70 66 69 6C 65    if aux swapfile
4c0 : 20 64 65 73 69 72 65 64 2E 0A 61 70 6D 5F 65 6E    desired..apm_en
4d0 : 61 62 6C 65 3D 22 4E 4F 22 09 09 23 20 53 65 74   able="NO"..# Set
4e0 : 20 74 6F 20 59 45 53 20 74 6F 20 65 6E 61 62 6C    to YES to enabl
4f0 : 65 20 41 50 4D 20 42 49 4F 53 20 66 75 6E 63 74   e APM BIOS funct
500 : 69 6F 6E 73 20 28 6F 72 20 4E 4F 29 2E 0A 61 70   ions (or NO)..ap
510 : 6D 64 5F 65 6E 61 62 6C 65 3D 22 4E 4F 22 09 23   md_enable="NO".#
520 : 20 52 75 6E 20 61 70 6D 64 20 74 6F 20 68 61 6E    Run apmd to han
530 : 64 6C 65 20 41 50 4D 20 65 76 65 6E 74 20 66 72   dle APM event fr
```

```
540 : 6F 6D 20 75 73 65 72 6C 61 6E 64 2E 0A 61 70 6D   om userland..apm
550 : 64 5F 66 6C 61 67 73 3D 22 22 09 09 23 20 46 6C   d_flags=""..# Fl
560 : 61 67 73 20 74 6F 20 61 70 6D 64 20 28 69 66 20   ags to apmd (if
570 : 65 6E 61 62 6C 65 64 29 2E 0A 70 63 63 61 72 64   enabled)..pccard
580 : 5F 65 6E 61 62 6C 65 3D 22 4E 4F 22 09 23 20 53   _enable="NO".# S
590 : 65 74 20 74 6F 20 59 45 53 20 69 66 20 79 6F 75   et to YES if you
5a0 : 20 77 61 6E 74 20 74 6F 20 63 6F 6E 66 69 67 75    want to configu
5b0 : 72 65 20 50                                       re P

[**] IDS181/shellcode-x86-nops [**]
02/16-19:23:50.591032 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:896 IpLen:20 DgmLen:1500 DF
***AP*** Seq: 0x9C28AEF7  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 67 0E 05 08 D8 DA BF BF 01 00 00 00 EB 1B 90 90   g...............
010 : 16 1F 66 6A 00 51 50 06 53 31 C0 88 F0 50 6A 10   ..fj.QP.S1...Pj.
020 : 89 E5 E8 C7 00 8D 66 10 CB FC 31 C9 8E C1 8E D9   ......f...1.....
030 : 8E D1 BC 00 7C 89 E6 BF 00 07 FE C5 F3 A5 BE EE   ....|...........
040 : 7D 80 FA 80 72 2C B6 01 E8 67 00 B9 01 00 BE BE   }...r,...g......
050 : 8D B6 01 80 7C 04 A5 75 07 E3 19 F6 04 80 75 14   ....|..u......u.
060 : 83 C6 10 FE C6 80 FE 05 72 E9 49 E3 E1 BE 8B 7D   ........r.I....}
070 : EB 52 31 D2 89 16 00 09 B6 10 E8 35 00 BB 00 90   .R1........5....
080 : 8B 77 0A 01 DE BF 00 B0 B9 00 AC 29 F1 F3 A4 29   .w.........)...)
090 : F9 30 C0 F3 AA E8 03 00 E9 81 13 FA E4 64 A8 02   .0...........d..
0a0 : 75 FA B0 D1 E6 64 E4 64 A8 02 75 FA B0 DF E6 60   u....d.d..u....`
0b0 : FB C3 BB 00 8C 8B 44 08 8B 4C 0A 0E E8 53 FF 73   ......D..L...S.s
0c0 : 2A BE 86 7D E8 1C 00 BE 90 7D E8 16 00 30 E4 CD   *..}.....}...0..
0d0 : 16 C7 06 72 04 34 12 EA 00 00 FF FF BB 07 00 B4   ...r.4..........
0e0 : 0E CD 10 AC 84 C0 75 F4 B4 01 F9 C3 52 B4 08 CD   ......u.....R...
0f0 : 13 88 F5 5A 72 F5 80 E1 3F 74 ED FA 66 8B 46 08   ...Zr...?t..f.F.
100 : 52 66 0F B6 D9 66 31 D2 66 F7 F3 88 EB 88 D5 43   Rf...f1.f......C
110 : 30 D2 66 F7 F3 88 D7 5A 66 3D FF 03 00 00 FB 77   0.f....Zf=.....w
120 : 44 86 C4 C0 C8 02 08 E8 40 91 88 FE 28 E0 8A 66   D.......@...(..f
130 : 02 38 E0 72 02 88 E0 BF 05 00 C4 5E 04 50 B4 02   .8.r.......^.P..
140 : CD 13 5B 73 0A 4F 74 1C 30 E4 CD 13 93 EB EB 0F   ..[s.Ot.0.......
150 : B6 C3 01 46 08 73 03 FF 46 0A D0 E3 00 5E 05 28   ...F.s..F....^.(
160 : 46 02 77 88 C3 2E F6 06 99 08 80 0F 84 79 FF BB   F.w.........y..
170 : AA 55 52 B4 41 CD 13 5A 0F 82 6F FF 81 FB 55 AA   .UR.A..Z..o...U.
180 : 0F 85 64 FF F6 C1 01 0F 84 5D FF 89 EE B4 42 CD   ..d......]....B.
190 : 13 C3 52 65 61 64 00 42 6F 6F 74 00 20 65 72 72   ..Read.Boot. err
1a0 : 6F 72 0D 0A 00 80 90 90 90 90 90 90 90 90 90 90   or..............
1b0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
1c0 : 90 90 90 90 90 90 90 90 90 90 00 00 00 00 00 00   ................
1d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1f0 : 00 00 00 00 00 00 00 00 00 00 80 00 01 00 A5 FF   ................
200 : FF FF 00 00 00 00 50 C3 00 00 55 AA 57 45 56 82   ......P...U.WEV.
210 : 00 00 00 00 6D 69 6E 69 6D 75 6D 32 00 00 00 00   ....minimum2....
220 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
230 : 00 00 00 00 00 02 00 00 80 16 00 00 01 00 00 00   ................
240 : 01 00 00 00 80 16 00 00 80 16 00 00 00 00 00 00   ................
250 : 00 00 00 00 2C 01 01 00 00 00 00 00 00 00 00 00   ....,...........
260 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
270 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
280 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
290 : 57 45 56 82 AC 52 03 00 00 20 00 00 00 20 00 00   WEV..R... ... ..
2a0 : 80 16 00 00 00 00 00 00 00 02 00 00 00 08 00 00   ................
2b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2c0 : 80 16 00 00 00 00 00 00 00 02 00 00 07 08 06 00   ................
2d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
300 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
310 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
320 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
330 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
340 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
350 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
360 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
370 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
380 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
390 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
400 : 00 00 00 00 00 00 00 00 00 00 00 00 EB 0E 42 54   ..............BT
410 : 58 01 01 80 F6 0F 50 07 00 10 00 00 FA 31 C0 8E   X.....P......1..
420 : D0 BC 00 18 8E C0 8E D8 66 6A 02 66 9D BF 00 1E   ........fj.f....
430 : B9 00 39 57 F3 AB 5F BE B2 96 AC 98 91 E3 1D AC   ..9W.._.........
440 : 92 AD 93 AD B6 08 D1 EB 73 0B 89 05 88 75 02 88   ........s....u..
450 : 55 05 83 C0 04 8D 7D 08 E2 EC EB DE C6 45 05 18   U.....}......E..
460 : C6 45 08 10 C6 45 0D 1E C6 45 66 68 BB 20 28 E8   .E...E...Efh. (.
470 : A9 00 0F 01 1E A6 96 0F 01 16 A0 96 0F 20 C0 66   ............. .f
480 : 83 C8 01 0F 22 C0 EA 7F 90 08 00 31 C9 B1 10 8E   ....".. ...1....
490 : D1 B1 38 0F 00 D9 BA 00 A0 00 00 36 0F B7 05 13   ..8........6....
4a0 : 04 00 00 C1 E0 0A 2D 00 10 00 00 29 D0 B1 33 51   ......-....)..3Q
4b0 : 50 68 02 02 00 00 6A 2B FF 35 0C 90 00 00 51 51   Ph....j+.5....QQ
4c0 : 51 51 52 B1 07 6A 00 E2 FC 61 07 1F 0F A1 0F A9   QQR..j...a......
4d0 : CF FA BC 00 18 00 00 0F 20 C0 31 C9 66 EA D6 90   ........ .1.f...
4e0 : 18 00 B1 20 8E D1 8E D9 8E C1 8E E1 8E E9 48 0F   ... ..........H.
4f0 : 22 C0 EA EB 90 00 00 31 C0 8E D0 8E D8 BB 08 70   ".......1.......p
500 : E8 18 00 0F 01 1E AC 96 FB F6 06 07 90 01 74 FE   ..............t.
510 : C7 06 72 04 34 12 EA 00 00 FF FF E4 21 50 E4 A1   ..r.4.......!P..
520 : 50 B0 11 E6 20 E6 A0 88 D8 E6 21 88 F8 E6 A1 B0   P... ......!.....
530 : 04 E6 21 B0 02 E6 A1 B0 01 E6 21 E6 A1 58 E6 A1   ..!.......!..X..
540 : 58 E6 21 C3 F4 6A 00 EB 40 6A 01 EB 3C 6A 03 EB   X.!..j..@j..<j..
550 : 38 6A 04 EB 34 6A 05 EB 30 6A 06 EB 2C 6A 07 EB   8j..4j..0j..,j..
560 : 28 6A 08 EB 2C 6A 0A EB 28 6A 0B EB 24 6A 0C EB   (j..,j..(j..$j..
570 : 20 6A 0D EB 08 6A 0E EB 18 6A 10 EB 0C F6 44 24    j...j...j....D$
580 : 12 02 74 0D E9 C2 00 00 00 FF 34 24 C6 44 24 04   ..t.......4$.D$.
590 : 00 FC 1E 06 60 B0 06 F6 44 24 3A 02 75 18 0F A8   ....`...D$:.u...
5a0 : 0F A0 1E 06 B0 02 66 83 7C 24 44 08 75 08 16 8D   ......f.|$D.u...
5b0 : 44 24 50 50                                       D$PP
```

```
[**] IDS181/shellcode-x86-nops [**]
02/16-19:23:52.618134 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:1049 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9C297C47  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20
```

```
length = 1460

000 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
010 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
020 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
060 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
070 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
080 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
090 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0b0 : 00 00 00 00 00 00 00 00 00 00 00 00 EB 1B 90 90   ................
0c0 : 16 1F 66 6A 00 51 50 06 53 31 C0 88 F0 50 6A 10   ..fj.QP.S1...Pj.
0d0 : 89 E5 E8 C7 00 8D 66 10 CB FC 31 C9 8E C1 8E D9   ......f...1.....
0e0 : 8E D1 BC 00 7C 89 E6 BF 00 07 FE C5 F3 A5 BE EE   ....|...........
0f0 : 7D 80 FA 80 72 2C B6 01 E8 67 00 B9 01 00 BE BE   }...r,...g......
100 : 8D B6 01 80 7C 04 A5 75 07 E3 19 F6 04 80 75 14   ....|..u......u.
110 : 83 C6 10 FE C6 80 FE 05 72 E9 49 E3 E1 BE 8B 7D   ........r.I....}
120 : EB 52 31 D2 89 16 00 09 B6 10 E8 35 00 BB 00 90   .R1........5....
130 : 8B 77 0A 01 DE BF 00 B0 B9 00 AC 29 F1 F3 A4 29   .w.........)...)
140 : F9 30 C0 F3 AA E8 03 00 E9 81 13 FA E4 64 A8 02   .0...........d..
150 : 75 FA B0 D1 E6 64 E4 64 A8 02 75 FA B0 DF E6 60   u....d.d..u....`
160 : FB C3 BB 00 8C 8B 44 08 8B 4C 0A 0E E8 53 FF 73   ......D..L...S.s
170 : 2A BE 86 7D E8 1C 00 BE 90 7D E8 16 00 30 E4 CD   *..}.....}...0..
180 : 16 C7 06 72 04 34 12 EA 00 00 FF FF BB 07 00 B4   ...r.4..........
190 : 0E CD 10 AC 84 C0 75 F4 B4 01 F9 C3 52 B4 08 CD   ......u.....R...
1a0 : 13 88 F5 5A 72 F5 80 E1 3F 74 ED FA 66 8B 46 08   ...Zr...?t..f.F.
1b0 : 52 66 0F B6 D9 66 31 D2 66 F7 F3 88 EB 88 D5 43   Rf...f1.f......C
1c0 : 30 D2 66 F7 F3 88 D7 5A 66 3D FF 03 00 00 FB 77   0.f....Zf=.....w
1d0 : 44 86 C4 C0 C8 02 08 E8 40 91 88 FE 28 E0 8A 66   D.......@...(..f
1e0 : 02 38 E0 72 02 88 E0 BF 05 00 C4 5E 04 50 B4 02   .8.r.......^.P..
1f0 : CD 13 5B 73 0A 4F 74 1C 30 E4 CD 13 93 EB EB 0F   ..[s.Ot.0.......
200 : B6 C3 01 46 08 73 03 FF 46 0A D0 E3 00 5E 05 28   ...F.s..F....^.(
210 : 46 02 77 88 C3 2E F6 06 99 08 80 0F 84 79 FF BB   F.w..........y..
220 : AA 55 52 B4 41 CD 13 5A 0F 82 6F FF 81 FB 55 AA   .UR.A..Z..o...U.
230 : 0F 85 64 FF F6 C1 01 0F 84 5D FF 89 EE B4 42 CD   ..d......]....B.
240 : 13 C3 52 65 61 64 00 42 6F 6F 74 00 20 65 72 72   ..Read.Boot. err
250 : 6F 72 0D 0A 00 80 90 90 90 90 90 90 90 90 90 90   or..............
260 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
270 : 90 90 90 90 90 90 90 90 90 90 00 00 00 00 00 00   ................
280 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
290 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2a0 : 00 00 00 00 00 00 00 00 00 00 80 00 01 00 A5 FF   ................
2b0 : FF FF 00 00 00 00 50 C3 00 00 55 AA C8 02 00 00   ......P...U.....
2c0 : D0 02 00 00 D8 02 00 00 E0 02 00 00 E8 02 00 00   ................
2d0 : F0 02 00 00 F8 02 00 00 00 03 00 00 08 03 00 00   ................
2e0 : 10 03 00 00 18 03 00 00 20 03 00 00 28 03 00 00   ........ ...(...
2f0 : 30 03 00 00 38 03 00 00 40 03 00 00 48 03 00 00   0...8...@...H...
300 : 50 03 00 00 58 03 00 00 60 03 00 00 68 03 00 00   P...X...`...h...
310 : 70 03 00 00 78 03 00 00 80 03 00 00 88 03 00 00   p...x...........
320 : 90 03 00 00 98 03 00 00 A0 03 00 00 A8 03 00 00   ................
330 : B0 03 00 00 B8 03 00 00 C0 03 00 00 C8 03 00 00   ................
340 : D0 03 00 00 D8 03 00 00 E0 03 00 00 E8 03 00 00   ................
350 : F0 03 00 00 F8 03 00 00 00 04 00 00 08 04 00 00   ................
```

```
360 : 10 04 00 00 18 04 00 00 20 04 00 00 28 04 00 00   ........ ...(...
370 : 30 04 00 00 38 04 00 00 40 04 00 00 48 04 00 00   0...8...@...H...
380 : 50 04 00 00 58 04 00 00 60 04 00 00 68 04 00 00   P...X...`...h...
390 : 70 04 00 00 78 04 00 00 80 04 00 00 88 04 00 00   p...x...........
3a0 : 90 04 00 00 98 04 00 00 A0 04 00 00 A8 04 00 00   ................
3b0 : B0 04 00 00 B8 04 00 00 C0 04 00 00 C8 04 00 00   ................
3c0 : D0 04 00 00 D8 04 00 00 E0 04 00 00 E8 04 00 00   ................
3d0 : F0 04 00 00 F8 04 00 00 00 05 00 00 08 05 00 00   ................
3e0 : 10 05 00 00 18 05 00 00 20 05 00 00 28 05 00 00   ........ ...(...
3f0 : 30 05 00 00 38 05 00 00 40 05 00 00 48 05 00 00   0...8...@...H...
400 : 50 05 00 00 58 05 00 00 60 05 00 00 68 05 00 00   P...X...`...h...
410 : 70 05 00 00 78 05 00 00 80 05 00 00 88 05 00 00   p...x...........
420 : 90 05 00 00 98 05 00 00 A0 05 00 00 A8 05 00 00   ................
430 : B0 05 00 00 B8 05 00 00 C0 05 00 00 C8 05 00 00   ................
440 : D0 05 00 00 D8 05 00 00 E0 05 00 00 E8 05 00 00   ................
450 : F0 05 00 00 F8 05 00 00 00 06 00 00 08 06 00 00   ................
460 : 10 06 00 00 18 06 00 00 20 06 00 00 28 06 00 00   ........ ...(...
470 : 30 06 00 00 38 06 00 00 40 06 00 00 48 06 00 00   0...8...@...H...
480 : 50 06 00 00 58 06 00 00 60 06 00 00 68 06 00 00   P...X...`...h...
490 : 70 06 00 00 78 06 00 00 80 06 00 00 88 06 00 00   p...x...........
4a0 : 90 06 00 00 98 06 00 00 A0 06 00 00 A8 06 00 00   ................
4b0 : B0 06 00 00 B8 06 00 00 C0 06 00 00 C8 06 00 00   ................
4c0 : D0 06 00 00 D8 06 00 00 E0 06 00 00 E8 06 00 00   ................
4d0 : F0 06 00 00 F8 06 00 00 00 07 00 00 08 07 00 00   ................
4e0 : 10 07 00 00 18 07 00 00 20 07 00 00 28 07 00 00   ........ ...(...
4f0 : 30 07 00 00 38 07 00 00 40 07 00 00 48 07 00 00   0...8...@...H...
500 : 50 07 00 00 58 07 00 00 60 07 00 00 68 07 00 00   P...X...`...h...
510 : 70 07 00 00 78 07 00 00 80 07 00 00 88 07 00 00   p...x...........
520 : 90 07 00 00 98 07 00 00 A0 07 00 00 A8 07 00 00   ................
530 : B0 07 00 00 B8 07 00 00 C0 07 00 00 C8 07 00 00   ................
540 : D0 07 00 00 D8 07 00 00 E0 07 00 00 E8 07 00 00   ................
550 : F0 07 00 00 F8 07 00 00 00 08 00 00 08 08 00 00   ................
560 : 10 08 00 00 18 08 00 00 20 08 00 00 28 08 00 00   ........ ...(...
570 : 30 08 00 00 38 08 00 00 40 08 00 00 48 08 00 00   0...8...@...H...
580 : 50 08 00 00 58 08 00 00 60 08 00 00 68 08 00 00   P...X...`...h...
590 : 70 08 00 00 78 08 00 00 80 08 00 00 88 08 00 00   p...x...........
5a0 : 90 08 00 00 98 08 00 00 A0 08 00 00 A8 08 00 00   ................
5b0 : B0 08 00 00

[**] IDS181/shellcode-x86-nops [**]
02/16-19:24:45.619343 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:6153 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9C55D573  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 01 00 00 00 7C D9 BF BF 36 00 08 28 EF 06 0B 28   ....|...6..(...(
010 : D6 05 79 0A 00 22 09 28 78 D9 BF BF 01 00 00 00   ..y.".(x.......
020 : 00 22 09 28 7C D9 BF BF 16 00 08 28 EF 06 0B 28   ."."(|......(...(
030 : 90 D9 BF BF 94 D9 BF BF EA FF 07 28 C8 F2 08 28   ...........(...(
040 : 00 22 09 28 E4 7A 12 28 BD 1E 08 28 C8 F2 08 28   ."."(.z.(...(...(
050 : 00 22 09 28 CC D9 BF BF 1C E3 0A 28 C8 F2 08 01   ."."(.......(....
060 : 00 20 09 28 AC D9 BF BF 6E F9 07 28 40 40 09 28   . .(....n..(@@.(
070 : 00 22 09 28 A8 D9 BF BF 01 00 00 00 A8 73 12 28   ."."(.........s.(
080 : A9 26 32 30 30 30 00 28 D0 D9 BF BF D1 E1 06 08   .&2000.(........
090 : 9C E1 06 08 CC D9 BF BF E0 26 12 28 FC D9 BF BF   .........&.(....
0a0 : 60 0E 00 00 D3 26 12 28 80 86 13 28 E0 26 12 28   `....&.(...(.&.(
```

```
0b0 : 12 02 00 00 D9 86 13 28 20 DA BF BF A7 36 10 28   .......( ....6.(
0c0 : C0 86 13 28 E0 26 12 28 A9 26 12 28 D3 26 12 28   ...(.&.(.&.(.&.(
0d0 : 16 00 00 00 03 00 00 00 27 00 00 00 18 00 00 00   ........'.......
0e0 : D0 07 00 00 50 DA BF BF 29 F3 07 28 3A 36 10 28   ....P...)..(:6.(
0f0 : A8 73 12 28 00 00 00 00 D8 E2 BF BF C0 86 13 28   .s.(...........(
100 : 97 02 00 00 00 22 09 28 50 DA BF BF 25 36 10 28   .....".(P...%6.(
110 : 80 86 13 28 C0 86 13 28 29 F3 07 28 0C 36 10 28   ...(...()..(.6.(
120 : A8 73 12 28 00 00 00 00 80 86 13 28 80 86 13 28   .s.(.......(...(
130 : 06 02 00 00 00 22 09 28 90 DA BF BF D3 2C 10 28   .....".(.....,.(
140 : 80 86 13 28 24 E6 09 08 E0 DD BF BF 82 45 0A 08   ...($........E..
150 : 00 22 09 28 D8 E2 BF BF 29 F3 07 28 B8 2C 10 28   .".(....)..(.,.(
160 : A4 D8 07 08 00 00 00 00 6C D8 BF BF 3C F9 BF BF   ........l...<...
170 : DC DA BF BF AD 0D 05 08 DC DA BF BF C0 86 13 28   ...............(
180 : D8 E2 BF BF 67 0E 05 08 D8 DA BF BF 01 00 00 00   ....g...........
190 : EB 1B 90 90 16 1F 66 6A 00 51 50 06 53 31 C0 88   ......fj.QP.S1..
1a0 : F0 50 6A 10 89 E5 E8 C7 00 8D 66 10 CB FC 31 C9   .Pj.......f...1.
1b0 : 8E C1 8E D9 8E D1 BC 00 7C 89 E6 BF 00 07 FE C5   ........|.......
1c0 : F3 A5 BE EE 7D 80 FA 80 72 2C B6 01 E8 67 00 B9   ....}...r,...g..
1d0 : 01 00 BE BE 8D B6 01 80 7C 04 A5 75 07 E3 19 F6   ........|..u....
1e0 : 04 80 75 14 83 C6 10 FE C6 80 FE 05 72 E9 49 E3   ..u.........r.I.
1f0 : E1 BE 8B 7D EB 52 31 D2 89 16 00 09 B6 10 E8 35   ...}.R1........5
200 : 00 BB 00 90 8B 77 0A 01 DE BF 00 B0 B9 00 AC 29   .....w.........)
210 : F1 F3 A4 29 F9 30 C0 F3 AA E8 03 00 E9 81 13 FA   ...).0..........
220 : E4 64 A8 02 75 FA B0 D1 E6 64 E4 64 A8 02 75 FA   .d..u....d.d..u.
230 : B0 DF E6 60 FB C3 BB 00 8C 8B 44 08 8B 4C 0A 0E   ...`......D..L..
240 : E8 53 FF 73 2A BE 86 7D E8 1C 00 BE 90 7D E8 16   .S.s*..}.....}..
250 : 00 30 E4 CD 16 C7 06 72 04 34 12 EA 00 00 FF FF   .0.....r.4......
260 : BB 07 00 B4 0E CD 10 AC 84 C0 75 F4 B4 01 F9 C3   ..........u.....
270 : 52 B4 08 CD 13 88 F5 5A 72 F5 80 E1 3F 74 ED FA   R......Zr...?t..
280 : 66 8B 46 08 52 66 0F B6 D9 66 31 D2 66 F7 F3 88   f.F.Rf...f1.f...
290 : EB 88 D5 43 30 D2 66 F7 F3 88 D7 5A 66 3D FF 03   ...C0.f....Zf=..
2a0 : 00 00 FB 77 44 86 C4 C0 C8 02 08 E8 40 91 88 FE   ...wD.......@...
2b0 : 28 E0 8A 66 02 38 E0 72 02 88 E0 BF 05 00 C4 5E   (..f.8.r.......^
2c0 : 04 50 B4 02 CD 13 5B 73 0A 4F 74 1C 30 E4 CD 13   .P....[s.Ot.0...
2d0 : 93 EB EB 0F B6 C3 01 46 08 73 03 FF 46 0A D0 E3   .......F.s..F...
2e0 : 00 5E 05 28 46 02 77 88 C3 2E F6 06 99 08 80 0F   .^.(F.w.........
2f0 : 84 79 FF BB AA 55 52 B4 41 CD 13 5A 0F 82 6F FF   .y...UR.A..Z..o.
300 : 81 FB 55 AA 0F 85 64 FF F6 C1 01 0F 84 5D FF 89   ..U...d......]..
310 : EE B4 42 CD 13 C3 52 65 61 64 00 42 6F 6F 74 00   ..B...Read.Boot.
320 : 20 65 72 72 6F 72 0D 0A 00 80 90 90 90 90 90 90    error..........
330 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
340 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 00 00   ................
350 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
360 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
370 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00   ................
380 : 01 00 A5 FF FF FF 00 00 00 00 50 C3 00 00 55 AA   ..........P...U.
390 : 57 45 56 82 00 00 00 00 66 64 31 34 34 30 00 00   WEV.....fd1440..
3a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3b0 : 00 00 00 00 00 00 00 00 00 02 00 00 12 00 00 00   ................
3c0 : 02 00 00 00 50 00 00 00 24 00 00 00 40 0B 00 00   ....P...$...@...
3d0 : 00 00 00 00 00 00 00 00 2C 01 01 00 00 00 00 00   ........,.......
3e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
400 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
410 : 00 00 00 00 57 45 56 82 28 69 03 00 00 20 00 00   ....WEV.(i... ..
420 : 00 20 00 00 40 0B 00 00 00 00 00 00 00 02 00 00   . ..@...........
430 : 00 08 00 00 40 0B 00 00 00 00 00 00 00 02 00 00   ....@...........
```

```
440 : 00 08 00 00 40 0B 00 00 00 00 00 00 00 02 00 00   ....@...........
450 : 07 08 06 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
460 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
470 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
480 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
490 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
4f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
500 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
510 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
520 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
530 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
540 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
550 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
560 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
570 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
580 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
590 : EB 0E 42 54 58 01 01 80 F6 0F 50 07 00 10 00 00   ..BTX.....P.....
5a0 : FA 31 C0 8E D0 BC 00 18 8E C0 8E D8 66 6A 02 66   .1..........fj.f
5b0 : 9D BF 00 1E
```

```
[**] IDS181/shellcode-x86-nops [**]
02/16-19:25:17.878055 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:8347 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9C6C5357  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
010 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
020 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
030 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
040 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
050 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
060 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
070 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
080 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
090 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
100 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
110 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
120 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
130 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
140 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
150 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
160 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
170 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
180 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
190 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
200 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
210 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
220 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
230 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
240 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
250 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
260 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
270 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
280 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
290 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
300 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
310 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
320 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
330 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
340 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
350 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
360 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
370 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
380 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
390 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3a0 : 00 00 00 00 00 00 00 00 00 00 00 00 EB 1B 90 90   ................
3b0 : 16 1F 66 6A 00 51 50 06 53 31 C0 88 F0 50 6A 10   ..fj.QP.S1...Pj.
3c0 : 89 E5 E8 C7 00 8D 66 10 CB FC 31 C9 8E C1 8E D9   ......f...1.....
3d0 : 8E D1 BC 00 7C 89 E6 BF 00 07 FE C5 F3 A5 BE EE   ....|...........
3e0 : 7D 80 FA 80 72 2C B6 01 E8 67 00 B9 01 00 BE BE   }...r,...g......
3f0 : 8D B6 01 80 7C 04 A5 75 07 E3 19 F6 04 80 75 14   ....|..u......u.
400 : 83 C6 10 FE C6 80 FE 05 72 E9 49 E3 E1 BE 8B 7D   ........r.I....}
410 : EB 52 31 D2 89 16 00 09 B6 10 E8 35 00 BB 00 90   .R1........5....
420 : 8B 77 0A 01 DE BF 00 B0 B9 00 AC 29 F1 F3 A4 29   .w.........)...)
430 : F9 30 C0 F3 AA E8 03 00 E9 81 13 FA E4 64 A8 02   .0...........d..
440 : 75 FA B0 D1 E6 64 E4 64 A8 02 75 FA B0 DF E6 60   u....d.d..u....`
450 : FB C3 BB 00 8C 8B 44 08 8B 4C 0A 0E E8 53 FF 73   ......D..L...S.s
460 : 2A BE 86 7D E8 1C 00 BE 90 7D E8 16 00 30 E4 CD   *..}.....}...0..
470 : 16 C7 06 72 04 34 12 EA 00 00 FF FF BB 07 00 B4   ...r.4..........
480 : 0E CD 10 AC 84 C0 75 F4 B4 01 F9 C3 52 B4 08 CD   ......u.....R...
490 : 13 88 F5 5A 72 F5 80 E1 3F 74 ED FA 66 8B 46 08   ...Zr...?t..f.F.
4a0 : 52 66 0F B6 D9 66 31 D2 66 F7 F3 88 EB 88 D5 43   Rf...f1.f......C
4b0 : 30 D2 66 F7 F3 88 D7 5A 66 3D FF 03 00 00 FB 77   0.f....Zf=.....w
4c0 : 44 86 C4 C0 C8 02 08 E8 40 91 88 FE 28 E0 8A 66   D.......@...(..f
4d0 : 02 38 E0 72 02 88 E0 BF 05 00 C4 5E 04 50 B4 02   .8.r.......^.P..
4e0 : CD 13 5B 73 0A 4F 74 1C 30 E4 CD 13 93 EB EB 0F   ..[s.Ot.0.......
4f0 : B6 C3 01 46 08 73 03 FF 46 0A D0 E3 00 5E 05 28   ...F.s..F....^.(
500 : 46 02 77 88 C3 2E F6 06 99 08 80 0F 84 79 FF BB   F.w.........y..
```

```
510 : AA 55 52 B4 41 CD 13 5A 0F 82 6F FF 81 FB 55 AA   .UR.A..Z..o...U.
520 : 0F 85 64 FF F6 C1 01 0F 84 5D FF 89 EE B4 42 CD   ..d......]....B.
530 : 13 C3 52 65 61 64 00 42 6F 6F 74 00 20 65 72 72   ..Read.Boot. err
540 : 6F 72 0D 0A 00 80 90 90 90 90 90 90 90 90 90 90   or..............
550 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
560 : 90 90 90 90 90 90 90 90 90 90 00 00 00 00 00 00   ................
570 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
580 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
590 : 00 00 00 00 00 00 00 00 00 00 80 00 01 00 A5 FF   ................
5a0 : FF FF 00 00 00 00 50 C3 00 00 55 AA 57 45 56 82   ......P...U.WEV.
5b0 : 00 00 00 00

[**] IDS181/shellcode-x86-nops [**]
02/16-19:25:18.429251 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:8399 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x9C6D153F  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20
length = 1460

000 : E8 67 00 B9 01 00 BE BE 8D B6 01 80 7C 04 A5 75   .g..........|..u
010 : 07 E3 19 F6 04 80 75 14 83 C6 10 FE C6 80 FE 05   ......u.........
020 : 72 E9 49 E3 E1 BE 8B 7D EB 52 31 D2 89 16 00 09   r.I....}.R1.....
030 : B6 10 E8 35 00 BB 00 90 8B 77 0A 01 DE BF 00 B0   ...5.....w......
040 : B9 00 AC 29 F1 F3 A4 29 F9 30 C0 F3 AA E8 03 00   ...)...).0......
050 : E9 81 13 FA E4 64 A8 02 75 FA B0 D1 E6 64 E4 64   .....d..u....d.d
060 : A8 02 75 FA B0 DF E6 60 FB C3 BB 00 8C 8B 44 08   ..u....`......D.
070 : 8B 4C 0A 0E E8 53 FF 73 2A BE 86 7D E8 1C 00 BE   .L...S.s*..}....
080 : 90 7D E8 16 00 30 E4 CD 16 C7 06 72 04 34 12 EA   .}...0.....r.4..
090 : 00 00 FF FF BB 07 00 B4 0E CD 10 AC 84 C0 75 F4   ..............u.
0a0 : B4 01 F9 C3 52 B4 08 CD 13 88 F5 5A 72 F5 80 E1   ....R......Zr...
0b0 : 3F 74 ED FA 66 8B 46 08 52 66 0F B6 D9 66 31 D2   ?t..f.F.Rf...f1.
0c0 : 66 F7 F3 88 EB 88 D5 43 30 D2 66 F7 F3 88 D7 5A   f......C0.f....Z
0d0 : 66 3D FF 03 00 00 FB 77 44 86 C4 C0 C8 02 08 E8   f=.....wD.......
0e0 : 40 91 88 FE 28 E0 8A 66 02 38 E0 72 02 88 E0 BF   @...(..f.8.r....
0f0 : 05 00 C4 5E 04 50 B4 02 CD 13 5B 73 0A 4F 74 1C   ...^.P....[s.Ot.
100 : 30 E4 CD 13 93 EB EB 0F B6 C3 01 46 08 73 03 FF   0..........F.s..
110 : 46 0A D0 E3 00 5E 05 28 46 02 77 88 C3 2E F6 06   F....^.(F.w.....
120 : 99 08 80 0F 84 79 FF BB AA 55 52 B4 41 CD 13 5A   .....y...UR.A..Z
130 : 0F 82 6F FF 81 FB 55 AA 0F 85 64 FF F6 C1 01 0F   ..o...U...d.....
140 : 84 5D FF 89 EE B4 42 CD 13 C3 52 65 61 64 00 42   .]....B...Read.B
150 : 6F 6F 74 00 20 65 72 72 6F 72 0D 0A 00 80 90 90   oot. error......
160 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
170 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
180 : 90 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
190 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1b0 : 00 00 80 00 01 00 A5 FF FF FF 00 00 00 00 50 C3   ..............P.
1c0 : 00 00 55 AA C0 02 00 00 C8 02 00 00 D0 02 00 00   ..U.............
1d0 : D8 02 00 00 E0 02 00 00 E8 02 00 00 F0 02 00 00   ................
1e0 : F8 02 00 00 00 03 00 00 08 03 00 00 10 03 00 00   ................
1f0 : 18 03 00 00 20 03 00 00 28 03 00 00 30 03 00 00   .... ...(...0...
200 : 38 03 00 00 40 03 00 00 48 03 00 00 50 03 00 00   8...@...H...P...
210 : 58 03 00 00 60 03 00 00 68 03 00 00 70 03 00 00   X...`...h...p...
220 : 78 03 00 00 80 03 00 00 88 03 00 00 90 03 00 00   x...............
230 : 98 03 00 00 A0 03 00 00 A8 03 00 00 B0 03 00 00   ................
240 : B8 03 00 00 C0 03 00 00 C8 03 00 00 D0 03 00 00   ................
250 : D8 03 00 00 E0 03 00 00 E8 03 00 00 F0 03 00 00   ................
260 : F8 03 00 00 00 04 00 00 08 04 00 00 10 04 00 00   ................
```

```
270 : 18 04 00 00 20 04 00 00 28 04 00 00 30 04 00 00   .... ...(...0...
280 : 38 04 00 00 40 04 00 00 48 04 00 00 50 04 00 00   8...@...H...P...
290 : 58 04 00 00 60 04 00 00 68 04 00 00 70 04 00 00   X...`...h...p...
2a0 : 78 04 00 00 80 04 00 00 88 04 00 00 90 04 00 00   x...............
2b0 : 98 04 00 00 A0 04 00 00 A8 04 00 00 B0 04 00 00   ................
2c0 : B8 04 00 00 C0 04 00 00 C8 04 00 00 D0 04 00 00   ................
2d0 : D8 04 00 00 E0 04 00 00 E8 04 00 00 F0 04 00 00   ................
2e0 : F8 04 00 00 00 05 00 00 08 05 00 00 10 05 00 00   ................
2f0 : 18 05 00 00 20 05 00 00 28 05 00 00 30 05 00 00   .... ...(...0...
300 : 38 05 00 00 40 05 00 00 48 05 00 00 50 05 00 00   8...@...H...P...
310 : 58 05 00 00 60 05 00 00 68 05 00 00 70 05 00 00   X...`...h...p...
320 : 78 05 00 00 80 05 00 00 88 05 00 00 90 05 00 00   x...............
330 : 98 05 00 00 A0 05 00 00 A8 05 00 00 B0 05 00 00   ................
340 : B8 05 00 00 C0 05 00 00 C8 05 00 00 D0 05 00 00   ................
350 : D8 05 00 00 E0 05 00 00 E8 05 00 00 F0 05 00 00   ................
360 : F8 05 00 00 00 06 00 00 08 06 00 00 10 06 00 00   ................
370 : 18 06 00 00 20 06 00 00 28 06 00 00 30 06 00 00   .... ...(...0...
380 : 38 06 00 00 40 06 00 00 48 06 00 00 50 06 00 00   8...@...H...P...
390 : 58 06 00 00 60 06 00 00 68 06 00 00 70 06 00 00   X...`...h...p...
3a0 : 78 06 00 00 80 06 00 00 88 06 00 00 90 06 00 00   x...............
3b0 : 98 06 00 00 A0 06 00 00 A8 06 00 00 B0 06 00 00   ................
3c0 : B8 06 00 00 C0 06 00 00 C8 06 00 00 D0 06 00 00   ................
3d0 : D8 06 00 00 E0 06 00 00 E8 06 00 00 F0 06 00 00   ................
3e0 : F8 06 00 00 00 07 00 00 08 07 00 00 10 07 00 00   ................
3f0 : 18 07 00 00 20 07 00 00 28 07 00 00 30 07 00 00   .... ...(...0...
400 : 38 07 00 00 40 07 00 00 48 07 00 00 50 07 00 00   8...@...H...P...
410 : 58 07 00 00 60 07 00 00 68 07 00 00 70 07 00 00   X...`...h...p...
420 : 78 07 00 00 80 07 00 00 88 07 00 00 90 07 00 00   x...............
430 : 98 07 00 00 A0 07 00 00 A8 07 00 00 B0 07 00 00   ................
440 : B8 07 00 00 C0 07 00 00 C8 07 00 00 D0 07 00 00   ................
450 : D8 07 00 00 E0 07 00 00 E8 07 00 00 F0 07 00 00   ................
460 : F8 07 00 00 00 08 00 00 08 08 00 00 10 08 00 00   ................
470 : 18 08 00 00 20 08 00 00 28 08 00 00 30 08 00 00   .... ...(...0...
480 : 38 08 00 00 40 08 00 00 48 08 00 00 50 08 00 00   8...@...H...P...
490 : 58 08 00 00 60 08 00 00 68 08 00 00 70 08 00 00   X...`...h...p...
4a0 : 78 08 00 00 80 08 00 00 88 08 00 00 90 08 00 00   x...............
4b0 : 98 08 00 00 A0 08 00 00 A8 08 00 00 B0 08 00 00   ................
4c0 : B8 08 00 00 C0 08 00 00 C8 08 00 00 D0 08 00 00   ................
4d0 : D8 08 00 00 E0 08 00 00 E8 08 00 00 F0 08 00 00   ................
4e0 : F8 08 00 00 00 09 00 00 08 09 00 00 10 09 00 00   ................
4f0 : 18 09 00 00 20 09 00 00 28 09 00 00 30 09 00 00   .... ...(...0...
500 : 38 09 00 00 40 09 00 00 48 09 00 00 50 09 00 00   8...@...H...P...
510 : 58 09 00 00 60 09 00 00 68 09 00 00 70 09 00 00   X...`...h...p...
520 : 78 09 00 00 80 09 00 00 88 09 00 00 90 09 00 00   x...............
530 : 98 09 00 00 A0 09 00 00 A8 09 00 00 B0 09 00 00   ................
540 : B8 09 00 00 C0 09 00 00 C8 09 00 00 D0 09 00 00   ................
550 : D8 09 00 00 E0 09 00 00 E8 09 00 00 F0 09 00 00   ................
560 : F8 09 00 00 00 0A 00 00 08 0A 00 00 10 0A 00 00   ................
570 : 18 0A 00 00 20 0A 00 00 28 0A 00 00 30 0A 00 00   .... ...(...0...
580 : 38 0A 00 00 40 0A 00 00 48 0A 00 00 50 0A 00 00   8...@...H...P...
590 : 58 0A 00 00 60 0A 00 00 68 0A 00 00 70 0A 00 00   X...`...h...p...
5a0 : 78 0A 00 00 80 0A 00 00 88 0A 00 00 90 0A 00 00   x...............
5b0 : 98 0A 00 00

[**] IDS181/shellcode-x86-nops [**]
02/16-19:25:44.749473 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:10151 IpLen:20 DgmLen:1500 DF
```

```
***A**** Seq: 0x9C82D73B  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 72 2C B6 01 E8 67 00 B9 01 00 BE BE 8D B6 01 80   r,...g..........
010 : 7C 04 A5 75 07 E3 19 F6 04 80 75 14 83 C6 10 FE   |..u......u.....
020 : C6 80 FE 05 72 E9 49 E3 E1 BE 8B 7D EB 52 31 D2   ....r.I....}.R1.
030 : 89 16 00 09 B6 10 E8 35 00 BB 00 90 8B 77 0A 01   .......5.....w..
040 : DE BF 00 B0 B9 00 AC 29 F1 F3 A4 29 F9 30 C0 F3   .......)...).0..
050 : AA E8 03 00 E9 81 13 FA E4 64 A8 02 75 FA B0 D1   .........d..u...
060 : E6 64 E4 64 A8 02 75 FA B0 DF E6 60 FB C3 BB 00   .d.d..u....`....
070 : 8C 8B 44 08 8B 4C 0A 0E E8 53 FF 73 2A BE 86 7D   ..D..L...S.s*..}
080 : E8 1C 00 BE 90 7D E8 16 00 30 E4 CD 16 C7 06 72   .....}...0.....r
090 : 04 34 12 EA 00 00 FF FF BB 07 00 B4 0E CD 10 AC   .4..............
0a0 : 84 C0 75 F4 B4 01 F9 C3 52 B4 08 CD 13 88 F5 5A   ..u.....R......Z
0b0 : 72 F5 80 E1 3F 74 ED FA 66 8B 46 08 52 66 0F B6   r...?t..f.F.Rf..
0c0 : D9 66 31 D2 66 F7 F3 88 EB 88 D5 43 30 D2 66 F7   .f1.f......C0.f.
0d0 : F3 88 D7 5A 66 3D FF 03 00 00 FB 77 44 86 C4 C0   ...Zf=.....wD...
0e0 : C8 02 08 E8 40 91 88 FE 28 E0 8A 66 02 38 E0 72   ....@...(..f.8.r
0f0 : 02 88 E0 BF 05 00 C4 5E 04 50 B4 02 CD 13 5B 73   .......^.P....[s
100 : 0A 4F 74 1C 30 E4 CD 13 93 EB EB 0F B6 C3 01 46   .Ot.0..........F
110 : 08 73 03 FF 46 0A D0 E3 00 5E 05 28 46 02 77 88   .s..F....^.(F.w.
120 : C3 2E F6 06 99 08 80 0F 84 79 FF BB AA 55 52 B4   .........y...UR.
130 : 41 CD 13 5A 0F 82 6F FF 81 FB 55 AA 0F 85 64 FF   A..Z..o...U...d.
140 : F6 C1 01 0F 84 5D FF 89 EE B4 42 CD 13 C3 52 65   .....]....B...Re
150 : 61 64 00 42 6F 6F 74 00 20 65 72 72 6F 72 0D 0A   ad.Boot. error..
160 : 00 80 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
170 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
180 : 90 90 90 90 90 90 00 00 00 00 00 00 00 00 00 00   ................
190 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1b0 : 00 00 00 00 00 00 80 00 01 00 A5 FF FF FF 00 00   ................
1c0 : 00 00 50 C3 00 00 55 AA 57 45 56 82 00 00 00 00   ..P...U.WEV.....
1d0 : 66 64 31 34 34 30 00 00 00 00 00 00 00 00 00 00   fd1440..........
1e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1f0 : 00 02 00 00 12 00 00 00 02 00 00 00 50 00 00 00   ............P...
200 : 24 00 00 00 40 0B 00 00 00 00 00 00 00 00 00 00   $...@...........
210 : 2C 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
220 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
230 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
240 : 00 00 00 00 00 00 00 00 00 00 00 00 57 45 56 82   ............WEV.
250 : 28 69 03 00 00 20 00 00 00 20 00 00 40 0B 00 00   (i... ... ..@...
260 : 00 00 00 00 00 02 00 00 00 08 00 00 40 0B 00 00   ............@...
270 : 00 00 00 00 00 02 00 00 00 08 00 00 40 0B 00 00   ............@...
280 : 00 00 00 00 00 02 00 00 07 08 06 00 00 00 00 00   ................
290 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
2f0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
300 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
310 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
320 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
330 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
340 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
350 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
360 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
370 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
380 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
390 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3a0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
3c0 : 00 00 00 00 00 00 00 00 EB 0E 42 54 58 01 01 80   ..........BTX...
3d0 : F6 0F 50 07 00 10 00 00 FA 31 C0 8E D0 BC 00 18   ..P......1......
3e0 : 8E C0 8E D8 66 6A 02 66 9D BF 00 1E B9 00 39 57   ....fj.f......9W
3f0 : F3 AB 5F BE B2 96 AC 98 91 E3 1D AC 92 AD 93 AD   .._.............
400 : B6 08 D1 EB 73 0B 89 05 88 75 02 88 55 05 83 C0   ....s....u..U...
410 : 04 8D 7D 08 E2 EC EB DE C6 45 05 18 C6 45 08 10   ..}......E...E..
420 : C6 45 0D 1E C6 45 66 68 BB 20 28 E8 A9 00 0F 01   .E...Efh. (.....
430 : 1E A6 96 0F 01 16 A0 96 0F 20 C0 66 83 C8 01 0F   ......... .f....
440 : 22 C0 EA 7F 90 08 00 31 C9 B1 10 8E D1 B1 38 0F   ".. ...1......8.
450 : 00 D9 BA 00 A0 00 00 36 0F B7 05 13 04 00 00 C1   .......6........
460 : E0 0A 2D 00 10 00 00 29 D0 B1 33 51 50 68 02 02   ..-....)..3QPh..
470 : 00 00 6A 2B FF 35 0C 90 00 00 51 51 51 51 52 B1   ..j+.5....QQQQR.
480 : 07 6A 00 E2 FC 61 07 1F 0F A1 0F A9 CF FA BC 00   .j...a..........
490 : 18 00 00 0F 20 C0 31 C9 66 EA D6 90 18 00 B1 20   .... .1.f...... 
4a0 : 8E D1 8E D9 8E C1 8E E1 8E E9 48 0F 22 C0 EA EB   ..........H."...
4b0 : 90 00 00 31 C0 8E D0 8E D8 BB 08 70 E8 18 00 0F   ...1.......p....
4c0 : 01 1E AC 96 FB F6 06 07 90 01 74 FE C7 06 72 04   ..........t...r.
4d0 : 34 12 EA 00 00 FF FF E4 21 50 E4 A1 50 B0 11 E6   4.......!P..P...
4e0 : 20 E6 A0 88 D8 E6 21 88 F8 E6 A1 B0 04 E6 21 B0    .....!.......!.
4f0 : 02 E6 A1 B0 01 E6 21 E6 A1 58 E6 A1 58 E6 21 C3   ......!..X..X.!.
500 : F4 6A 00 EB 40 6A 01 EB 3C 6A 03 EB 38 6A 04 EB   .j..@j..<j..8j..
510 : 34 6A 05 EB 30 6A 06 EB 2C 6A 07 EB 28 6A 08 EB   4j..0j..,j..(j..
520 : 2C 6A 0A EB 28 6A 0B EB 24 6A 0C EB 20 6A 0D EB   ,j..(j..$j.. j..
530 : 08 6A 0E EB 18 6A 10 EB 0C F6 44 24 12 02 74 0D   .j...j....D$..t.
540 : E9 C2 00 00 00 FF 34 24 C6 44 24 04 00 FC 1E 06   ......4$.D$.....
550 : 60 B0 06 F6 44 24 3A 02 75 18 0F A8 0F A0 1E 06   `...D$:.u.......
560 : B0 02 66 83 7C 24 44 08 75 08 16 8D 44 24 50 50   ..f.|$D.u...D$PP
570 : EB 08 FF 74 24 50 FE C8 75 F8 6A 10 1F 1E 07 89   ...t$P..u.j.....
580 : E3 BE D1 96 00 00 BF 00 18 00 00 57 E8 8C 03 00   ...........W....
590 : 00 5E E8 24 04 00 00 8D 64 24 18 61 07 1F 80 3C   .^.$....d$.a...<
5a0 : 24 03 74 05 E9 E4 FE FF FF 8D 64 24 08 CF FC 1E   $.t.......d$....
5b0 : 07 8D 55 3C                                       ..U<


[**] IDS181/shellcode-x86-nops [**]
02/16-22:11:45.900400 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:37727 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xB7574763  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 6C 6E 57 B7 11 D5 F1 2C 37 DE 82 4A 70 E6 8A D5   lnW....,7..Jp...
010 : 87 C8 20 9F BF 3C 77 22 17 4E 6E EB 18 54 35 C7   .. ..<w".Nn..T5.
020 : 70 61 60 74 60 EB E8 3D 7E 0C 1B 3F E9 8D 0C 4F   pa`t`..=~..?...O
030 : B8 3D C8 36 80 4D 34 D2 8F C9 44 1B BB 27 0B A1   .=.6.M4...D..'..
040 : 7C 20 E2 30 02 A3 CC 81 C1 FA FC 4B 7E 55 9E 61   | .0.......K~U.a
050 : BE B9 D0 33 26 C6 B8 47 F5 3C 59 02 59 AC DC 2C   ...3&..G.<Y.Y..,
060 : ED 5A E3 7D F3 C0 B3 B9 41 B3 34 77 FA 5D F7 4D   .Z.}....A.4w.].M
070 : 71 6C 86 C6 42 3C 3A C3 2B 1F 21 DD 42 AD 71 89   ql..B<:.+.!.B.q.
080 : 6A B7 B0 FC FC F3 CB E7 D9 1C 9B 5B 8C 27 F5 01   j..........[.'..
```

```
090 : BF C1 9F 73 EE 9E 9B E6 FE 02 E5 65 97 2E B1 EC   ...s.......e....
0a0 : 62 F4 C8 B3 0E 1F D2 EA 45 C6 07 D5 F7 CF A3 EE   b.......E.......
0b0 : E7 FF 81 FD 35 34 3B A4 B4 47 CB E8 20 32 6F 5D   ....54;..G.. 2o]
0c0 : 07 67 10 DD 59 A2 4B 1F 8C 8F E9 81 FE BF 2C 3F   .g..Y.K.......,?
0d0 : B2 8D B1 52 4E C5 A2 52 A1 50 E2 27 82 AB 79 E9   ...RN..R.P.'..y.
0e0 : FF 7B 28 78 FC 49 FC 89 97 47 13 89 C7 DE 4C 24   .{(x.I...G....L$
0f0 : 18 AE 7C 22 81 83 98 F9 4F E2 89 E0 CB A3 C1 E7   ..|"....O.......
100 : C7 F8 A7 7F BC 31 BF F6 A5 F1 AB 6F 07 25 85 67   ... .1....o.%.g
110 : 86 3F 74 3C F1 D1 39 6E 59 42 42 42 42 42 42 42   .?t<..9nYBBBBBBB
120 : 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42   BBBBBBBBBBBBBBBB
130 : 42 42 42 42 42 42 E2 87 82 C7 12 FF 9E F9 56 E6   BBBBBB........V.
140 : 9D CC 5B 99 37 E9 E7 C3 AE 8D 84 84 84 84 84 84   ..[.7...........
150 : 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84   ................
160 : 84 84 84 84 84 84 84 84 C4 FD 70 E6 0B 49 FE 39   ..........p..I.9
170 : D1 DD 6E FF 4C 70 D1 1C 9B AE D3 B5 CD 89 EB 7C   ..n.Lp.........|
180 : 78 35 93 90 90 90 90 90 90 90 90 90 90 90 90 90   x5..............
190 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
1a0 : 90 F8 A0 F0 DD FF 96 90 90 90 90 90 90 90 90 90   ................
1b0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
1c0 : 90 90 90 90 90 F8 A8 E3 50 B7 97 87 66 67 D9 9E   ........P...fg..
1d0 : 8C 96 F7 CD A1 61 8E 7B C6 9D 25 FA ED 03 8C 31   .....a.{..%....1
1e0 : C8 AA AA 56 28 B0 04 03 D4 53 9F C5 82 4A 60 AC   ...V(....S...J`.
1f0 : 94 53 8B AA 96 2B 14 4A 8C 65 0B D9 82 96 60 EA   .S...+.J.e....`.
200 : 07 58 87 77 85 E7 B8 BA CD 58 C2 B6 2C F7 41 E9   .X.w.....X..,.A.
210 : 8E FA 86 31 7C 18 15 7A C8 78 FC 49 9D FE 7F 34   ...1|..z.x.I.. 4
220 : 91 78 EC CD 44 82 E1 CA 27 12 89 47 12 FE 4F E2   .x..D...'..G..O.
230 : 89 04 FE 44 44 22 F1 31 FA F9 31 FA F9 71 FA F9   ...DD".1..1..q..
240 : 11 BA 57 A4 64 5F 41 A2 2F 8D 5F 7D 3B 28 E9 D1   ..W.d_A./._};(..
250 : E0 07 69 3F FE 30 5F E1 89 47 1E E6 D3 24 24 24   ..i?.0_..G...$$$
260 : 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24 24   $$$$$$$$$$$$$$$$
270 : 24 24 24 24 24 24 24 24 24 24 24 FE F7 E1 AB 8F   $$$$$$$$$$$.....
280 : 7C 27 F3 8F 99 BF CD FC 45 E6 8D CC EB 99 DF CA   |'......E.......
290 : FC 5A E6 17 32 3F 9F 79 2D 73 98 79 39 63 66 5E   .Z..2?.y-s.y9cf^
2a0 : CC EC 64 1A 99 B5 4C 21 73 3E 33 9B 79 32 F3 78   ..d...L!s>3.y2.x
2b0 : E6 BF D2 FF 91 FE 97 F4 3B E9 B7 D2 7F 93 FE F3   ........;... ...
2c0 : F4 9F A6 DF 48 BF 9E FE DD F4 6F A7 7F 23 FD 95   ....H.....o. #..
2d0 : F4 2F A6 3F 9F FE 99 B4 93 1E A4 3B E9 9B E9 46   ./.?.......;...F
2e0 : 7A 2D 7D 39 5D 4E E7 D3 E7 D2 67 D3 4F A6 3F 99   z-}9]N....g.O.?.
2f0 : 4E A4 BF 3D FB 0F B3 DF 9C FD CB D9 3F 99 FD A3   N..=........?...
300 : D9 DF 9B FD D5 D9 2F CF BE 36 7B 38 FB E2 EC F6   ....../..6{8....
310 : EC A5 D9 CA EC A7 67 A7 66 1F 9D FD F6 CC DB 33   ......g.f......3
320 : 7F 3D F3 87 33 BF 33 F3 CB 33 5F 9E 79 6D E6 CE    =..3.3..3_.ym..
330 : CC 4B 33 3B 33 9F 9B D1 66 1E 9F 49 CC BC 33 FD   .K3;3...f..I..3.
340 : 77 D3 5F 9F 7E 7D FA D7 A7 7F 65 FA 0B D3 3F 3B   w._.~}... e...?;
350 : 7D 7B BA 33 9D 9B 5E 9C FE D4 F4 8F 4E FF EB D4   }{.3..^.....N...
360 : 3F 4F FD D5 D4 9B 53 BF 3F F5 B5 A9 9F 9B 7A 65   ?O....S.?.....ze
370 : AA 3B F5 D2 D4 F5 A9 2B 53 3F 31 F5 A9 A9 E4 D4   .;.....+S?1.....
380 : C7 A7 BE 9B FA 4E EA DF 52 DF 4A FD 7D EA 1B A9   .....N..R.J.}...
390 : 3F 4B BD 91 7A 3D F5 B5 D4 6F A6 BE 9A FA A5 D4   ?K..z=...o......
3a0 : 17 53 9F 4F BD 9A F2 52 56 EA 20 75 33 B5 95 AA   .S.O...RV. u3...
3b0 : A5 56 53 97 52 C5 D4 52 EA E9 14 4B 9D 49 7D 32   .VS.R..R...K.I}2
3c0 : F5 44 EA 91 D4 7F 9E F9 A7 33 DF 3C F3 D6 99 6F   .D... ...3.<...o
3d0 : 9C 79 F3 CC 1F 9F F9 FA 99 3F F8 1F F6 BE 3C 3C   .y.......?....<<
3e0 : 8A 2A 6B 3F 2C E9 AE AE 5E D2 7B F5 92 74 0B C2   .*k?,...^.{..t..
3f0 : 28 60 C5 DE D2 49 70 23 90 C8 22 9B 49 50 50 31   (`...Ip#..".IPP1
400 : 56 3A 4D D2 A4 D3 1D 7A 49 08 8A 0B 28 8A 0B AE   V:M....zI...(...
410 : 28 2A 2A 2A 0E B8 8C 88 E2 BE AF A8 28 A0 8E A2   (***........(...
```

```
420 : A2 A2 B8 A0 83 8A 8A DB B8 7E F7 9C 7B AA 13 9C   .........~..{...
430 : 79 1C E7 9B EF F9 CD EF 8F 14 3C CF B9 EF 7B 6E   y.........<...{n
440 : 57 DD DA EE 3D 75 CE 3D 37 AE 07 5C 77 BA 56 BB   W...=u.=7..\w.V.
450 : 56 BA 2E 73 9D EF 5A E4 5A E0 CA B9 92 AE B8 6B   V..s..Z.Z......k
460 : B6 EB 18 D7 54 D7 78 D7 11 AE 2A 57 C0 35 CC 55   ....T.x...*W.5.U
470 : EA B2 B8 74 AE 9F A5 6F A4 4F A4 F7 A4 D7 A4 CD   ...t...o.O......
480 : D2 46 E9 51 E9 3E E9 0E E9 56 E9 46 E9 1A 69 B9   .F.Q.>...V.F..i.
490 : 74 A1 74 B6 B4 58 3A 59 CA 4B 1D 52 4C 3A 5E 9A   t.t..X:Y.K.RL:^.
4a0 : 2E 4D 90 0E 97 A2 52 50 1A 21 0D 97 CA 24 97 64   .M....RP.!...$.d
4b0 : 96 04 A9 48 FA D9 F9 8D 73 B7 F3 7D E7 DB CE 57   ...H....s..}...W
4c0 : 9D 9B 9D CF 38 9F 70 3E E0 5C EF BC D9 B9 DA B9   ....8.p>.\......
4d0 : D2 79 85 F3 42 E7 39 CE D3 9D A7 38 73 CE 0E 67   .y..B.9....8s..g
4e0 : DC D9 EC 3C CE 59 EF 9C E4 1C E3 AC 72 1E E4 1C   ...<.Y......r...
4f0 : E6 F4 38 AD 4E BD 73 90 F3 27 C7 D7 8E CF 1D 1F   ..8.N.s..'......
500 : 39 3E 74 BC ED 78 C5 B1 C9 F1 94 E3 21 C7 3D 8E   9>t..x......!.=.
510 : DB 1D 6B 1D AB 1C 57 39 2E 71 5C E0 38 CB 71 AA   ..k...W9.q\.8.q.
520 : A3 CB D1 E9 68 73 C4 1C C7 3B A6 3B 26 38 8E 70   ....hs...;.;&8.p
530 : 54 3A 0E 76 1C E0 D8 CF E1 72 98 1C 1A C7 AF F6   T:.v.....r......
540 : EF EC 5F D8 3F B6 EF B0 6F B3 BF 6C 7F DE FE B4   .._.?...o..l ...
550 : FD 61 FB 06 FB 6D F6 6B ED 97 DB 2F B4 9F 6D 3F   .a...m.k.../..m?
560 : C3 DE 63 EF B4 B7 D9 15 FB 2C 7B A3 7D B2 FD 48   ..c......,{.}..H
570 : FB E1 F6 6A 7B D0 7E A0 7D 3F BB CB 6E B6 EB ED   ...j{.~.}?..n...
580 : 83 EC 3F D9 BE B6 ED B1 ED B2 ED B4 BD 69 7B D5   ..?..........i{.
590 : F6 A2 ED 69 DB C3 B6 BB 6C B7 DA 56 DB 56 DA 2E   ...i....l..V.V..
5a0 : B3 9D 6F 5B 64 5B 60 CB D8 E6 DA 9A 6C C7 DA 8E   ..o[d[`.....l...
5b0 : B6 4D B4 1D
```

```
[**] IDS181/shellcode-x86-nops [**]
02/16-23:37:10.802794 205.149.189.91:6810 -> Target IP:1355
TCP TTL:50 TOS:0x10 ID:36039 IpLen:20 DgmLen:1500 DF
***AP*** Seq: 0xC12E07F7  Ack: 0x3EFAC928  Win: 0x4470  TcpLen: 20

length = 1460

000 : 7D 61 61 A1 AA 4D 3D AA DA A3 24 50 98 BF 50 55   }aa..M=...$P..PU
010 : 17 2E 28 2A 02 ED 79 45 AA 9A 67 2F 5A 58 20 D4   ..(*..yE..g/ZX .
020 : 71 99 32 24 FC 95 49 1A 68 1F 2F DF 58 FE 6F 29   q.2$..I.h./.X.o)
030 : C2 EB C0 E4 CD 81 1A AF 67 BB B3 B5 3B 37 2D 9C   ........g...;7-.
040 : 27 6D 2D 99 F9 63 71 1D 4E EF 3C 95 BE 1B 42 79   'm-..cq.N.<...By
050 : 9D 5E 6D CE DF E6 9E EE 6D 1E EF E2 E1 80 2A A7   .^m.....m.....*.
060 : A7 D3 D5 A6 AE CF 55 D7 6C 43 88 67 A7 BA 94 DE   ......U.lC.g....
070 : 97 E8 ED 6C CD 6D EB 69 E9 6C CE F5 F5 2C 1F 29   ...l.m.i.l...,.)
080 : BD B4 AD CD A5 4F BD AB CD 1F DC DC DD BA CD E9   .....O..........
090 : 53 DB BD 9E 8E 91 12 57 3B 5D 3B 3C 6A 5D EB 36   S......W;];<j].6
0a0 : AF C7 D9 E6 F4 8E 04 97 3B 7D AE AD E1 76 6C 70   ........;}...vlp
0b0 : B6 E4 74 34 FB BA 9D 86 B6 54 6E F5 78 23 5A E2   ..t4.....Tn.x#Z.
0c0 : 71 B7 39 5A DC 3D 4E 9F 49 5B 2E F6 5A 91 90 90   q.9Z.=N.I[..Z...
0d0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0e0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0f0 : 90 F8 D3 70 36 14 0A 9D 8D F1 5E 9B 84 84 84 44   ...p6.....^....D
100 : 43 F5 9A EA 75 1B AA D5 0A AF D7 73 AE DF A9 FB   C...u......s....
110 : 73 C1 12 43 4A 48 48 48 48 48 48 48 48 48 48 48   s..CJHHHHHHHHHHH
120 : 48 48 48 48 48 48 48 48 48 48 48 48 48 48 48 48   HHHHHHHHHHHHHHHH
130 : 48 48 48 48 48 48 48 48 48 48 48 48 48 48 48 48   HHHHHHHHHHHHHHHH
140 : 48 48 48 48 48 5C 18 D0 FB 1B 4B BF 67 53 4A C1   HHHHH\....K.gSJ.
150 : 0A B0 0A BC 11 DC 00 DE 0C 7A 6F ED D5 FF 53 66   .........zo...Sf
```

```
160 : BF D0 3F 66 15 10 42 FB B0 4B 13 A8 0A 7D 7A 7C   ..?f..B..K...}z|
170 : 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09   ................
180 : 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09   ................
190 : 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09 09   ................
1a0 : 09 09 09 09 09 09 09 09 09 09 09 09 09 89 FF 27   ...............'
1b0 : B8 79 0C BF 63 E1 ED B3 7D E5 9B 57 6D CB BD A5   .y..c...}..Wm...
1c0 : 31 BF 76 66 4B D1 CA F5 B3 EC D7 DD B8 B3 66 DD   1.vfK.........f.
1d0 : 72 67 CE 82 1B 3A 9A 6F 6E E8 EA AD F2 CE A9 BE   rg...:.on.......
1e0 : B5 7D 7A E7 4D AB D7 B8 77 6F DD 31 FF 7B 33 96   .}z.M...wo.1.{3.
1f0 : 6E 6C 2B 6E DD E5 99 96 B7 6C 5E 65 F7 A6 8A 2D   nl+n.....l^e...-
200 : 4D 73 5D 3D 1B 4A BF 5F 5F B0 A2 EE B6 B5 25 DB   Ms]=.J._______%.
210 : 17 15 96 DD 71 FD FC 44 DA 77 57 AF 4D A1 F7 FD   ....q..D.wW.M...
220 : 7F 02 99 04 F9 30 64 32 E4 63 90 13 20 9F 81 4C    ....0d2.c.. ..L
230 : 81 3C 0C 99 0A F9 32 A4 15 F2 28 A4 02 F9 26 E4   .<....2...(...&.
240 : 44 C8 F7 20 D3 20 FF 00 99 0E F9 39 A4 0D 72 10   D.. . .....9..r.
250 : 72 31 E4 10 E4 12 AA 70 97 4D 59 0D 31 11 B2 22   r1.....p.MY.1.."
260 : C1 3E 3C DC 6E 55 6E 77 59 15 65 BB 55 09 40 D6   .><.nUnwY.e.U.@.
270 : 90 DC 01 42 2A 90 EE 6D B0 41 DA DD 56 A5 17 4C   ...B*..m.A..V..L
280 : B0 58 09 09 89 31 B0 EE 76 9B 52 07 6E 00 37 83   .X...1..v.R.n.7.
290 : 8D 60 2B B8 15 DC 01 7A 40 1F 78 2B B8 1B A4 98   .`+....z@.x+....
2a0 : A3 E0 C6 37 AD CA 71 50 79 C3 AA 84 C6 F8 86 75   ...7..qPy......u
2b0 : A0 44 08 55 15 22 0B DC 3B 53 88 09 90 49 E0 1B   .D.U."..;S...I..
2c0 : 39 BA A4 E3 D2 F3 38 A8 24 D9 C1 A0 10 DE DF 27   9.....8.$......'
2d0 : 8B A4 FE 4C 91 84 C0 E7 7F B7 47 24 F9 91 F6 4F   ...L.... .G$...O
2e0 : 15 67 AE 5F 82 FC 3E F0 23 31 54 E2 48 68 F9 02   .g._..>.#1T.Hh..
2f0 : 7B 84 E8 07 83 E0 00 38 08 0E 81 A1 58 0C 11 93   {......8....X...
300 : C1 4C B0 04 DC C3 E9 A9 F0 2F 01 7D E0 47 A0 43   .L......./.}.G.C
310 : CB 9F 50 1B C2 CB 8F B2 F7 FA 85 28 1F 4C 16 D3   ..P........(.L..
320 : 92 92 C4 64 4B 92 F8 EB 81 24 71 03 7A 60 4E 0D   ...dK....$q.z`N.
330 : 48 F2 59 92 42 CC 41 BE 39 CB 92 91 CE 04 97 8B   H.Y.B.A.9.......
340 : 39 9F 0F 41 0E 26 83 D6 FF 63 EF 5C E0 9B A8 F2   9..A.&...c.\....
350 : 3D 3E 49 08 09 29 10 54 52 58 5E 2D AF 52 52 A0   =>I..).TRX^-.RR.
360 : 05 04 CA E3 DA BA 2A D0 D2 C5 2E ED 10 50 34 82   ......*......P4.
370 : 20 8F 05 8A BC 05 AE 09 2F 2B F2 90 F2 50 51 D1    ......../+...PQ.
380 : AC A0 C4 89 10 DE E2 E3 6E B2 80 4B 01 41 40 7B   ........n..K.A@{
390 : 41 3F A8 A9 C8 E3 D6 2B C6 2B BD 0D 25 9D 73 CF   A?.....+.+..%.s.
3a0 : 63 92 26 99 C9 CC C9 EE 67 77 3F 77 CD DF ED 92   c.&.....gw?w....
3b0 : 69 E7 97 EF 9C F3 FF 9F FF FF 9C 33 93 D6 FC 51   i..........3...Q
3c0 : 80 E9 C3 04 54 99 CC 7E 4D 6E 5D 3F 5D 3A D3 A5   ....T..~Mn]?]:..
3d0 : A5 0F 68 9A C8 B6 1F A8 98 00 FC 0A 02 1D C3 C3   ..h.............
3e0 : 2F 40 FD 15 EA 07 80 BE 34 F0 4B 27 BC 56 01 F0   /@......4.K'.V..
3f0 : BE 26 08 06 E9 82 A0 47 4B 3F D0 35 81 5F 22 FE   .&.....GK?.5._".
400 : AF E5 6F 05 D3 B7 13 06 32 F9 97 5E 12 10 24 5E   ..o.....2..^..$^
410 : 7A 09 74 59 82 12 FB 3F 42 E2 5B 09 80 9A 48 D2   z.tY...?B.[...H.
420 : 29 25 7C 39 B0 69 89 A4 98 4E E1 05 46 00 0C E4   )%|9.i...N..F...
430 : 65 67 3A 89 1F A4 85 29 BF A7 95 E4 85 29 E9 B4   eg:....).....)..
440 : 12 1B 0F 08 C5 47 F9 FB 93 FC 00 F0 02 C5 47 D9   .....G........G.
450 : 16 1F CA C7 26 F2 F2 AE 04 24 29 04 98 38 25 D8   ....&....$)..8%.
460 : 86 4E E2 45 92 2C FC 92 EF 95 80 84 50 78 A5 A9   .N.E.,......Px..
470 : 36 36 A0 6B A4 D8 97 0E A3 42 18 B1 C4 82 0F 9E   66.k.....B......
480 : BE 45 21 81 D1 62 0F 53 7C 8B 6B 28 24 01 90 67   .E!..b.S|.k($..g
490 : 0F 53 02 8B AB 28 06 0C 0F 6C 58 82 E7 F9 C3 82   .S...(...lX.....
4a0 : 9C 46 51 81 4E 6F A4 74 5A D6 5A 9C 8F 63 0D B9   .FQ.No.tZ.Z..c..
4b0 : 51 8D 24 6E 74 A4 7B 56 DF 49 51 12 80 67 6B 91   Q.$nt.{V.IQ..gk.
4c0 : C4 0A 0F BC 9A 85 AD 3B 28 4A 82 F0 6C 43 88 E2   .......;(J..lC..
4d0 : 53 2D 31 E4 2A 4A B0 E3 79 44 81 5D E5 67 16 99   S-1.*J..yD.].g..
4e0 : E6 28 29 70 CB 53 78 38 5E 3C F0 68 8E 7D A9 C1   .()p.Sx8^<.h.}..
```

```
4f0 : 47 25 81 94 06 4C 69 EB 7D C6 E4 55 EA 65 E2 78   G%...Li.}..U.e.x
500 : 1E DC 01 1E 98 C8 5A FA 6E EB ED 42 2F F3 C6 F8   ......Z.n..B/...
510 : 6D 69 00 A6 20 A8 45 14 BB EA DC E2 D6 0C 39 D5   mi.. .E.......9.
520 : 1B CA 9F 52 92 3B C0 1C 04 3F 20 8A 57 75 23 A0   ...R.;...? .Wu#.
530 : 67 88 63 60 3E 88 17 3A A8 B3 D8 20 A8 02 16 15   g.c`>..:... ....
540 : F3 04 33 1F 52 48 F8 07 D0 7C 26 BE 04 52 5C 1E   ..3.RH...|&..R\.
550 : 4E CD E4 32 5D 72 0D 4C 00 7F 3F 08 24 4A 39 32   N..2]r.L. ?.$J92
560 : 1F 76 A5 25 00 2C 16 56 0B 2F A9 2F A4 F8 9B 09   .v.%.,.V././....
570 : 6F 25 DD FE 80 0A 49 B2 03 20 CB 09 29 BA F4 56   o%....I.. ..)..V
580 : 90 E2 53 93 36 82 34 49 49 50 83 62 2C 0F 52 8A   ..S.6.4IIP.b,.R.
590 : 59 AD 5D D3 4A 9F DB 9A F1 6A 05 89 74 97 F1 1A   Y.].J....j..t...
5a0 : 3F 72 8C 1F 98 1D 1C EC 30 7D F3 61 30 69 A2 8C   ?r......0}.a0i..
5b0 : 66 8F 3B 3B                                       f.;;
```

```
Registrant:
HackerDome, Inc. (RDY-DOM)
   707 Continental circle, #1634
   Mountain View, CA 94040  US

   Domain Name: RDY.COM

   Administrative Contact, Technical Contact, Billing Contact:
      Ruban, Dima  (DR7362)  dima@RDY.COM
      Ruban Consulting, Inc.
      707 Continental circle, #1634
      Mountain View,, CA 94040
      (415) 730-0648
```

```
02/18/01 19:42:49 dns ftp4.freebsd.org
Canonical name: burka.rdy.com
Aliases:
  ftp4.freebsd.org
Addresses:
  205.149.189.91
```

ANALYSIS

1. **Source of trace**
   Source of trace was from my home network (DSL/Fixed IP).

2. **Detection Generator**
   Snort IDS with ACID (Analysis Console for Intrusion Databases) interface. Main alert is generated from the raw Snort Alert log, payload data lifted from the ACID interface. Using ArachNIDS ruleset downloaded on 14 Feb 2001.

3. **Probability that the source was spoofed.**
   Low. This type of exploit would require a three-way handshake for data to be transferred. If the source were spoofed, it would near impossible to receive replies from the victim computer.

4. Description of Attack

This attack is a buffer overflow attack not aimed at any specific port. This attack has the signature of the "shellcode-x86-nops" exploit, it has no CVE # (GENERIC-MAP-NOMATCH), it does have a signature ID from Whitehats.com of IDS181.

5. Attack Mechanism

The Attack attempts to "pad" data with a long series of "no-op"'s resulting in a large piece of data that overloads the buffer. If the system is susceptible to buffer overflows, the data in the packet may be passed on to the system with root privileges. This could allow the attacker to take control of the system by replacing key system files with modified versions. It may also allow the attacker to execute commands that require root access to call.

6. Correlations

This particular detect was found out to be a false positive after investigating. The packet dump did not match any dump I'd seen previously at the SANS conference or any I'd looked up on various security sites. When first seeing the packet dump of the detect it appeared as though someone had attempted to upload a new rc.conf file to the system.. If this were true, the attacker could take control by reconfiguring the system the next time rc.conf was called. The target port (1355) was not listed on any port knowledge base so the only thing I could suspect was that an attacker had previously compromised the system and was listening on this port. When looking up the suspect address it came back with a name of HackerDome, Inc. Though the company the IP was registered to was interesting, I thought that it was improbable that my system would be the target of such a unique attack. I decided to investigate a little more. Fortunately my network is quite small and that allowed me to consider what was happening at the time of the detect. Unfortunately my firewall box had just had FreeBSD installed and configured with minimal logging (see section 9) so I was unable to see where the packet when after it had passed the IDS. I inquired with one of the people on the network at the time and he had indicated that he started an FTP download of a FreeBSD ISO (CD Image) from ftp4.freebsd.org. This was particularly interesting because when I used a search engine to investigate the ISP, I discovered that the Administrative Contact was listed as a FreeBSD developer. At this point I definitely had something a little more than a "coincidence" and there were only two options. Option one was that somehow a redirect had been done and the image was being downloaded via the suspect IP. Option two was that the "attacker" was monitoring traffic on ftp4.freebsd.org and was able to figure out what port numbers and ack #'s to use to feed in malicious traffic. Option two was definitely more interesting but not likely. After some digging on the net, I discovered that the suspect IP had an alias of ftp4.freebsd.org. Conclusion: False Positive.

One interesting note: All nine of the alert packets had the same ACK#.

This particular signature was compared against another signature from another system on a different network and matched. Their system connected to ftp4.freebsd.org to download the same file and received the same Snort alerts as I had.

7. Evidence of Active Targeting

This particular detect was definitely targeting the intended host.

8. Severity
(5+5)-(4+4)=+2
Criticality=5, This machine is the firewall and file server for the network.
Lethality=5, If successful, attacker could gain root access and "own" the system.
System Countermeasures=4, Latest stable version of FreeBSD running with no Telnet. External access via FTP, SSH, HTTP, and SSL-HTTP(Apache). Minimal logging enabled.
Network Countermeasures=4, Restrictive firewall that was in the process of being validated. There is only one way in or out.

9. Defensive Recommendation
Although this detect turned out to be a false positive, the machine in question had just undergone a total installation and configuration of FreeBSD. At the time IPFilter was enabled, rules were written to allow certain types of traffic. All traffic not specifically allowed was rejected. Although this was a good thing, the system was not configured to log denied packets, nor was it configured to record incoming and outgoing connections. This degraded the ability to find out what actually happened since the only log's available were Snort logs. Had logging been turned on, it would have been much easier to find out who was doing what. Fortunately logging was enabled on the machine that initiated the FTP transfer and the person remembered quite well what he was doing at the time. Had this been a very large network, it would have been very difficult and time consuming to find out who was doing what.

Recommend firewall logging be enabled for all traffic.

10. Multiple Choice Question
The purpose of including many NOP(No-Operation) bytes in a packet is to:
A) Increase the chances of getting malicious traffic past a firewall
B) Cause a DoS by flooding the system with so many No Operation bytes that the system effectively does nothing for a period of time.
C) Probe the system and compare return information to signatures for a system fingerprint.
D) Trick the system into listing services that are running.

Answer: A) Increase the chances of getting malicious traffic past a firewall

Detect 2 Analysis

```
[**] IDS277/named-probe-iquery [**]
02/10-10:24:30.417031 131.109.3.11:53 -> Target IP:53
UDP TTL:51 TOS:0x0 ID:8257 IpLen:20 DgmLen:55
Len: 35

length = 27
000 : E8 EC 09 80 00 00 00 01 00 00 00 00 00 00 01 00  ................
010 : 01 00 00 7A 69 00 04 04 03 02 01                 ...zi.....

[**] IDS278/named-version probe [**]
02/10-10:24:30.636386 131.109.3.11:53 -> Target IP:53
```

```
UDP TTL:49 TOS:0x0 ID:64707
Len: 38

Length = 30
000 : 3C FC 01 80 00 01 00 00 00 00 00 00 07 76 65 72          <.............ver
010 : 73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03                sion.bind.....


[**] IDS277/named-probe-iquery [**]
03/05-18:28:51.265497 131.109.3.11:1932 -> Target IP:53
UDP TTL:46 TOS:0x0 ID:36135 IpLen:20 DgmLen:493
Len: 473

length = 465
000 : 42 6F 09 80 00 00 00 01 00 00 00 00 3E 41 41 41  Bo.........>AAA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
030 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
040 : 41 41 41 41 41 41 41 41 41 41 41 3E 42 42 42 42  AAAAAAAAAAA>BBBB
050 : 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
060 : 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
070 : 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
080 : 42 42 42 42 42 42 42 42 42 42 3E 43 43 43 43 43  BBBBBBBBBB>CCCCC
090 : 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
0a0 : 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
0b0 : 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 43  CCCCCCCCCCCCCCCC
0c0 : 43 43 43 43 43 43 43 43 43 3E 00 01 02 03 04 05  CCCCCCCCC>......
0d0 : 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15  ................
0e0 : 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25  .......... !"#$%
0f0 : 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35  &'()*+,./012345
100 : 36 37 38 39 3A 3B 3C 3D 3E 45 45 45 45 45 45 45  6789:;<=>EEEEEEE
110 : 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45  EEEEEEEEEEEEEEEE
120 : 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45  EEEEEEEEEEEEEEEE
130 : 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45  EEEEEEEEEEEEEEEE
140 : 45 45 45 45 45 45 45 3E 46 46 46 46 46 46 46 46  EEEEEEE>FFFFFFFF
150 : 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46  FFFFFFFFFFFFFFFF
160 : 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46  FFFFFFFFFFFFFFFF
170 : 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 46  FFFFFFFFFFFFFFFF
180 : 46 46 46 46 46 46 3D 47 47 47 47 47 47 47 47 47  FFFFFF=GGGGGGGGG
190 : 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
1a0 : 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
1b0 : 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 47  GGGGGGGGGGGGGGGG
1c0 : 47 47 47 47 00 00 01 00 01 00 00 00 01 00 FF 40  GGGG...........@
1d0 : 66                                               f
```

ANALYSIS

1. Source of trace

Source of trace was from my home network (DSL/Fixed IP).

2. Detection Generator

Snort IDS with ACID (Analysis Console for Intrusion Databases) interface. Main alert is generated from the raw Snort Alert log, payload data lifted from the ACID interface. Using ArachNIDS ruleset downloaded on 08 Feb 2001.

3. Probability that the source was spoofed.
Very unlikely. The purpose of a DNS query and version query is to gain information about the victim system. Information cannot be sent back if the IP is spoofed.

4. Description of Attack
The attacker started by sending a DNS iquery to the victim machine. A follow up version bind request was sent to try and gain the version of bind the DNS server is running.

What is amusing about this particular attack is that the machine targeted is not running DNS and will not reply to a DNS request. That didn't seem to matter to the attacker. They initially send an iquery probe and followed up with a version inquiry even though they didn't get a reply. I'm surprised they didn't try to upload Ramen.

Even stranger, the last packet is a packet that was sent a month later. I haven't been able to figure out what the purpose of it was.

5. Attack Mechanism
The attack is supposed to check to see if DNS will return an inverse DNS query. This lets the attacker know if DNS is running. A follow up packet is sent requesting to see what version of BIND the DNS server is running. If the DNS server is running a vulnerable version, the attacker can compromise the system.

6. Correlations
Packet dump matches the packet of a packet trace on whitehats.com.
http://www.whitehats.com/IDS/277

7. Evidence of Active Targeting
This particular detect was targeting the particular host but most likely on a random scan. It is odd that the same IP scanned this machine over a month prior.

8. Severity

(5+0)-(5+5)= -5
Criticality=5 This machine is the firewall and file server for the network
Lethality=0 This machine is not running DNS.
System Countermeasures=5, Latest stable version of FreeBSD running with no Telnet or FTP. External access via FTP, SSH, HTTP, and SSL-HTTP(Apache)
Network Countermeasures=5 Firewall is the only way to enter/exit the network. Snort NIDS installed along with restrictive IP Filter rules.

9. Defensive Recommendation

Defenses are fine, attack was blocked by the firewall.

10. Multiple Choice Question

Certain versions of BIND are vulnerable to _____ attacks:

A) Session hijacking
B) Amplifying Denial of Service (DoS) attacks (ie Smurf)
C) Brute Force cryptanalysis
D) Buffer Overflow

Answer: D) Buffer Overflow

Detect 3 Analysis

```
[**] IDS177/netbios-name-query [**]
02/26-03:01:24.326077 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:29798 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 34 00 10 00 01 00 00 00 00 00 20 43 4B 41   ^4.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAA..!
030 : 00 01                                          ..


[**] IDS177/netbios-name-query [**]
02/26-03:01:25.827974 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:30054 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 36 00 10 00 01 00 00 00 00 00 20 43 4B 41   ^6.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAA..!
030 : 00 01                                          ..

[**] IDS177/netbios-name-query [**]
02/26-03:01:27.328233 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:30310 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 38 00 10 00 01 00 00 00 00 00 20 43 4B 41   ^8.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAA..!
030 : 00 01                                          ..
```

```
[**] IDS177/netbios-name-query [**]
02/26-03:02:27.887748 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:43622 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 48 00 10 00 01 00 00 00 00 00 00 20 43 4B 41   ^H.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAAA..!
030 : 00 01                                             ..


[**] IDS177/netbios-name-query [**]
02/26-03:02:29.383126 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:43878 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 4A 00 10 00 01 00 00 00 00 00 00 20 43 4B 41   ^J.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAAA..!
030 : 00 01                                             ..


[**] IDS177/netbios-name-query [**]
02/26-03:02:30.883061 63.106.48.202:137 -> Target IP:137
UDP TTL:118 TOS:0x0 ID:44134 IpLen:20 DgmLen:78
Len: 58
length = 50
000 : 5E 4C 00 10 00 01 00 00 00 00 00 00 20 43 4B 41   ^L.......... CKA
010 : 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41   AAAAAAAAAAAAAAAA
020 : 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21   AAAAAAAAAAAAA..!
030 : 00 01
```

ANALYSIS

11. Source of trace
Source of trace was from my home network (DSL/Fixed IP).

12. Detection Generator
Snort IDS with ACID (Analysis Console for Intrusion Databases) interface. Main alert is generated from the raw Snort Alert log, payload data lifted from the ACID interface. Using ArachNIDS ruleset downloaded on 20 Feb 2001.

13. Probability that the source was spoofed.
Low. To extract the desired information, the source IP would need to be provided.

14. Description of Attack
This attack is aimed at machines running Microsoft NetBIOS (or Samba) on Port 137 for a name table query. This would give the attacker useful information on the system such as

workstation name, domain, and users logged in. This attack has a CVE number of CAN-1999-0621, it also has been identified on Whitehats.com with an IDS key of IDS177.

15. Attack Mechanism

This attack works by querying the victim computer for NetBIOS information if a machine is running with Microsoft File and Print Sharing enabled. On a protected network or computer, an attacker should not be able to access this.

16. Correlations

A normal NetBIOS name query looks like this:

```
12/30-02:28:32.282973 source:1057 -> target:137
UDP TTL:64 TOS:0x0 ID:62089 Len: 58
24 C0 00 00 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 packet normally is transmitted three times with the same payload each time.
If you look at the suspect NetBIOS queries, you will see that they appear to be crafted. Each packet contains a similar code but the first two characters change. Each packet sent appears to be using a control character as the first character. I have not seen this particular signature before which is why I flagged it as suspect. I can only theorize that the attacker was attempting to get a firewall or OS to "hiccup" and/or pass the packet. The attacker may also have been attempting to cause the system to crash by introducing odd combinations of characters.

17. Evidence of Active Targeting
This particular detect was targeting the particular host. I suspect an automated scan

18. Severity
(5+2)-(5+5)= -3
Criticality=5, This machine is the firewall and file server(Samba) for the network
Lethality=2, Attacker could glean important information on the target. System is running Samba.
System Countermeasures=5, Latest stable version of FreeBSD running with no Telnet or FTP. External access via FTP, SSH, HTTP, and SSL-HTTP(Apache).
Network Countermeasures=5, Firewall is the only way to enter/exit the network. Snort NIDS installed along with restrictive IP Filter rules.

19. Defensive Recommendation

Defenses are adequate, attack was blocked by the firewall.

20. Multiple Choice Question

A NetBIOS Name Query is considered to be:

A. Rare attack against older Microsoft operating systems.
B. Background noise on the network.
C. A buffer overflow attack.
D. A Denial of Service Attack.

B. Background noise on the network.

Detect 4 Analysis

```
[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:36.743113 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:43564 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:37.762182 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:51451 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:38.767778 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:38230 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:39.781120 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:58797 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:40.793430 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:38704 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:41.794634 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:19663 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:33:42.811461 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:31290 IpLen:20 DgmLen:40 MF
Frag Offset: 0x0   Frag Size: 0x14

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:34:00.489425 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:37828 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:34:01.502314 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:37235 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:34:02.522610 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:29230 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:34:03.541639 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:43621 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34
```

```
[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:34:04.541178 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:52552 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:40:21.842685 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:45073 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:40:22.846411 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:8164 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:40:23.872569 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:9235 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:40:24.866765 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:40270 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34

[**] Tiny Fragments - Possible Hostile Activity [**]
03/17-10:40:25.876266 211.105.164.24 -> Target IP
TCP TTL:53 TOS:0x0 ID:43013 IpLen:20 DgmLen:72 MF
Frag Offset: 0x0   Frag Size: 0x34
```

```
inetnum:     211.104.0.0 - 211.119.255.255
netname:     KRNIC-KR-25
descr:       KRNIC
descr:       Korea Network Information Center
country:     KR
admin-c:     WK1-AP
tech-c:      SL119-AP
remarks:     KRNIC Allocation Block
remarks:     Authoritative Information regarding assignments and
remarks:     allocations made from within this block can also be
remarks:     queried at whois.nic.or.kr
mnt-by:      APNIC-HM
mnt-lower:   MNT-KRNIC-AP
changed:     hostmaster@apnic.net 20000414
source:      APNIC
```


ANALYSIS

1. **Source of trace**

Source of trace was from my home network (DSL/Fixed IP).

2. **Detection Generator**

Snort IDS with ACID (Analysis Console for Intrusion Databases) interface. Main alert is generated from the raw Snort Alert log, payload data lifted from the ACID interface (in this case, there is no payload data to examine). Using ArachNIDS ruleset downloaded on 16 Mar 2001.

3. **Probability that the source was spoofed.**

Possible. This is a very strange set of packets. If this was a DoS attempt, the source IP received spoofed packets with my IP. If it was a fingerprint attempt, it is unlikely the source was spoofed since the attacker could not get the needed response to their stimulus.

4. Description of Attack

This attack is very strange. The attacker sent 17 "tiny fragment" packets over about 7 minutes. These packets indicated a fragment size of 32 bytes with no offset. It's not clear to me what the attacker is trying to do at this point. If the attacker were attempting a buffer overflow, the offsets would change so the entire buffer would fill. These packets are all using an offset of 0, which would continue to overwrite the same space in the buffer.

5. Attack Mechanism

This attack works by making fragments very small. On some firewall systems, it is possible to sneak packets past the firewall by using small packets. There are two explanations that I can come up with.

One is that this was a denial of service (DoS) attempt. Each packet ID is different and each one has the MF flag set. If a large number of these were sent, the firewall could continue to hold these in its buffer waiting for the rest of the packets to arrive. Since no follow up packets are sent, the firewall may run out of memory and accept no more connections until the firewall "expires" the connections. The probability that this is a DoS attack is low since a total of 17 packets were sent. I suspect if this were a true DoS attempt, many more packets would have been sent.

The other explanation is that this was some sort of fingerprint attack. The firewall that is running on this network is programmed to deny all connections on all ports except FTP, SSH, HTTP, and SSL-HTTP. The attacker may have been attempting to fingerprint the system by analyzing the response to a tiny fragment sent to port 0.

6. Correlations

This particular scan does not match any packets that I can find. After these packets were discovered the firewall logs were inspected and nothing was found. This is troubling because it seems that the packets entered the system. They should have been rejected.

7. Evidence of Active Targeting

17 packets were fired at this system. One group of 10 was fired, followed approximately six minutes later by an additional 6 packets. This would seem to indicate that this system was being directly targeted.

8. Severity
(5+3)-(5+2)= +1
Criticality=5, This machine is the firewall and file server(Samba) for the network
Lethality=3, Attacker could glean important information on the target. Since I am not sure what the attacker was trying to do, I would rank this as suspicious.
System Countermeasures=5, Latest stable version of FreeBSD running with no Telnet. External access via SSH, HTTP, SSL-HTTP(Apache) only.
Network Countermeasures=2, Firewall is the only way to enter/exit the network. Snort NIDS installed along with restrictive IP Filter rules. Since the firewall did not block these packets, the network countermeasures will be ranked lower.

9. Defensive Recommendation

Upon inspection of firewall rules it was found that the suspect packets were not rejected (Deny). It was determined that the packets we passed because the following IPFilter rule was written:

Pass fragments
${fwcmd} add pass all from any to any frag

This would allow an attacker to send packets through the firewall as long as there is a fragment ID and offset.

Recommend rule change to the following:

Pass fragments
${fwcmd} add pass all from any to any frag established

This would make sure that a connection was established before fragmented packets could be sent. Unsolicited fragmented packets would be denied.

Also recommend this IP block be "blacklisted". We have no reason to connect to Korea. Blocking this would be a prudent step to take since I am not sure what the attacker was attempting to do.

10. Multiple Choice Question

Packets are normally fragmented to:
A) Decrease the time spent in the firewall packet inspection queue.
B) Traverse a network with an MTU smaller than the packet size.
C) Increase the chance of delivery.

D) Send time critical data (such as video or audio).

Answer: B) Traverse a network with an MTU smaller than the packet size.

Detect 5 Analysis

http://www.sans.org/y2k/032201-1500.htm

```
[**] IDS247/dos-large-udp [**]
03/14-11:01:17.450391 193.113.133.154:500 -> a.b.20.2:500
UDP TTL:112 TOS:0x0 ID:46267
Len: 864
E2 A5 3B 06 B8 49 D0 CE 00 00 00 00 00 00 00 00      ..;..I..........
01 10 02 00 00 00 00 00 00 00 03 58 0D 00 03 24      ...........X...$
00 00 00 01 00 00 00 01 00 00 03 18 01 01 00 0C      ................
03 00 00 24 01 01 00 00 80 01 00 05 80 02 00 02      ...$............
80 04 00 02 80 03 00 03 80 0B 00 01 00 0C 00 04      ................
00 00 70 80 03 00 00 24 02 01 00 00 80 01 00 05      ..p....$........
80 02 00 01 80 04 00 02 80 03 00 03 80 0B 00 01      ................
00 0C 00 04 00 00 70 80 03 00 00 24 03 01 00 00      ......p....$....
80 01 00 01 80 02 00 02 80 04 00 01 80 03 00 03      ................
80 0B 00 01 00 0C 00 04 00 00 70 80 03 00 00 24      ..........p....$
04 01 00 00 80 01 00 01 80 02 00 01 80 04 00 01      ................
80 03 00 03 80 0B 00 01 00 0C 00 04 00 00 70 80      ..............p.
03 00 00 50 05 01 00 00 80 01 00 05 80 02 00 02      ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04      ................
00 00 70 80 7D 01 00 28 77 00 32 00 30 00 30 00      ..p.}..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00      0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00      F.L...L.O.C.A.L.
03 00 00 50 06 01 00 00 80 01 00 05 80 02 00 02      ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04      ................
00 00 70 80 40 00 00 28 77 00 32 00 30 00 30 00      ..p.@..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00      0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00      F.L...L.O.C.A.L.
03 00 00 50 07 01 00 00 80 01 00 05 80 02 00 01      ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04      ................

[**] IDS247/dos-large-udp [**]
03/14-11:01:18.497383 193.113.133.154:500 -> a.b.20.2:500
UDP TTL:112 TOS:0x0 ID:46272
Len: 864
E2 A5 3B 06 B8 49 D0 CE 00 00 00 00 00 00 00 00  ..;..I..........
01 10 02 00 00 00 00 00 00 00 03 58 0D 00 03 24  ...........X...$
00 00 00 01 00 00 00 01 00 00 03 18 01 01 00 0C  ................
03 00 00 24 01 01 00 00 80 01 00 05 80 02 00 02  ...$............
80 04 00 02 80 03 00 03 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 03 00 00 24 02 01 00 00 80 01 00 05  ..p....$........
80 02 00 01 80 04 00 02 80 03 00 03 80 0B 00 01  ................
00 0C 00 04 00 00 70 80 03 00 00 24 03 01 00 00  ......p....$....
80 01 00 01 80 02 00 02 80 04 00 01 80 03 00 03  ................
80 0B 00 01 00 0C 00 04 00 00 70 80 03 00 00 24  ..........p....$
04 01 00 00 80 01 00 01 80 02 00 01 80 04 00 01  ................
80 03 00 03 80 0B 00 01 00 0C 00 04 00 00 70 80  ..............p.
```

```
03 00 00 50 05 01 00 00 80 01 00 05 80 02 00 02  ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 7D 01 00 28 77 00 32 00 30 00 30 00  ..p.}..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00  0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00  F.L...L.O.C.A.L.
03 00 00 50 06 01 00 00 80 01 00 05 80 02 00 02  ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 40 00 00 28 77 00 32 00 30 00 30 00  ..p.@..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00  0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00  F.L...L.O.C.A.L.
03 00 00 50 07 01 00 00 80 01 00 05 80 02 00 01  ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 7D 01 00 28 77 00 32 00 30 00 30 00  ..p.}..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00  0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00  F.L...L.O.C.A.L.
03 00 00 50 08 01 00 00 80 01 00 05 80 02 00 01  ...P............
80 04 00 02 80 03 FD E9 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 40 00 00 28 77 00 32 00 30 00 30 00  ..p.@..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00  0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00  F.L...L.O.C.A.L.
03 00 00 50 09 01 00 00 80 01 00 01 80 02 00 02  ...P............
80 04 00 01 80 03 FD E9 80 0B 00 01 00 0C 00 04  ................
00 00 70 80 7D 01 00 28 77 00 32 00 30 00 30 00  ..p.}..(w.2.0.0.
30 00 69 00 73 00 61 00 33 00 24 00 40 00 59 00  0.i.s.a.3.$.@.Y.
46 00 4C 00 2E 00 4C 00 4F 00 43 00 41 00 4C 00  F.L...L.O.C.A.L.
03 00 00 50 0A 01 00 00 80 01 00 01 80 02 00 02  ...P............
```

ANALYSIS

1. Source of trace

Source of trace was the SANS current detects page on March 22, 2001
http://www.sans.org/y2k/032201-1500.htm

2. Detection Generator

Snort IDS logs. Unknown ruleset.

3. **Probability that the source was spoofed.**

Not likely. The detect appears to be a response from a system that was queried.

4. Description of Attack

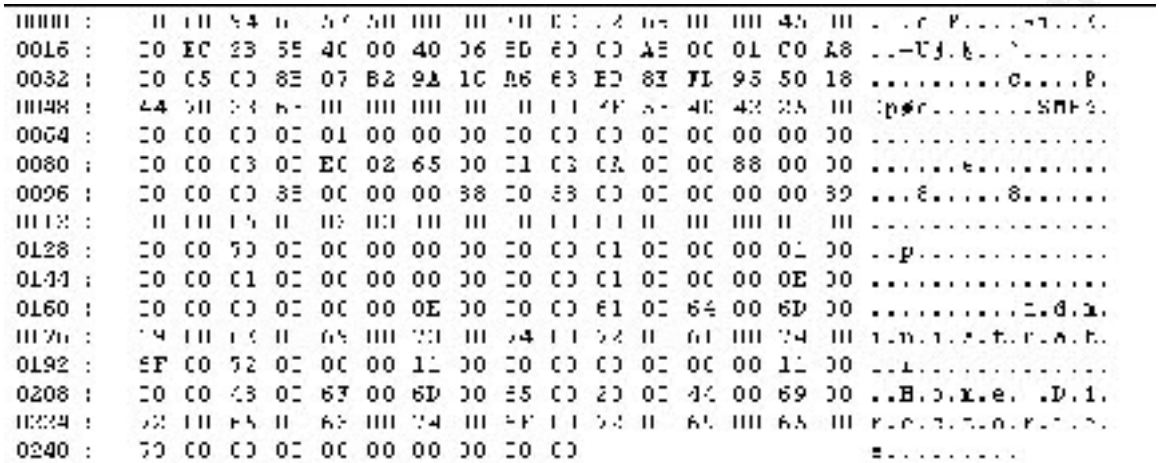
These packets were flagged as a "DOS Large UDP" attack.
Whitehats ID: IDS247

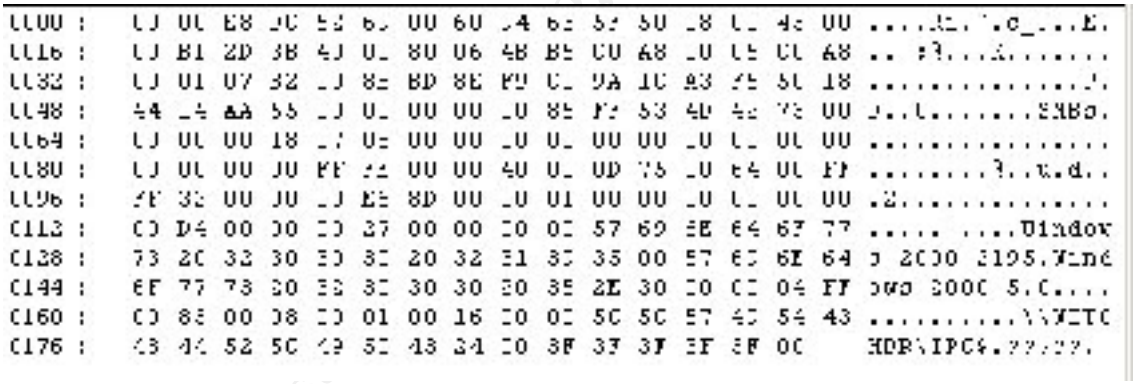
5. Attack Mechanism

If this were a malicious attack, the attacker could send unusually large UDP packets to the victim. Most UDP packets are small in size. The DoS occurs when large packets are sent to a firewall that does stateful packet inspection. Since it is inspecting large UDP packets, the firewall uses more resources than normal. If a number of large packets arrive very quickly, the firewall may run out of resources to use and suffer from DoS.

Other possibilities are that a "covert" channel exists and the attacker is using UDP packets to transmit the data or the machine is transmitting DDOS control traffic.

6. Correlations





After inspecting the packet dump of these packets I noticed that the packet looked very familiar. When inspecting NetBIOS packets a few weeks back I noticed a similar pattern. I decided to get a packet-sniffing device and capture some NetBIOS packets from my home network. What I viewed is pasted above (sorry for the picture, the sniffer does not like to import to text). What I viewed on my home network was a NetBIOS session setup and a NetBIOS reply. These two packets appear to be similar to the flagged packets

So now I'm pretty sure what I have are a few NetBIOS packets. This only explains some of the puzzle. The NetBIOS port that these packets should normally be seen on is Port 139. So why are these packets being seen on 500?

Port 500 is the standard port IPSEC/ISAKMP. Obviously these packets are not encrypted so again I scratched my head and wondered why. An initial whois indicated that the IP 193.113.133.154 belonged to British Telecom(BT). When I dug further into it I found that it

belongs to the IPSEC DEMO NET of BT. This would explain a lot. It's probable that these packets originate from a misconfigured IPSEC/VPN tunnel.

whois -h whois.ripe.net 193.113.133.154

inetnum: 193.113.133.144 - 193.113.133.159
netname: BT-CORPORATE
descr: IP_SEC_DEMO_NET_York
country: GB
admin-c: BCER1-RIPE
admin-c: BTCR1-RIPE
tech-c: BTCR3-RIPE
status: ASSIGNED PA
remarks: Please send abuse notification to btcertcc@bt.com

7. Evidence of Active Targeting

As explained in the previous section, these packets are most likely from a misconfigured VPN tunnel. Since I do not have information on the actual target IP (supplied IP is a.b.20.2) I can only speculate that the other end of the VPN tunnel contained an internal IP that matched the external IP of the target. If configured properly, the VPN tunnel would pass these packets from network to network. If configured improperly, one side may be passed in the clear. If the actual target contains IP's that are not private, those packets will go to the owner of this network.

Another possibility is that the target IP was conducting a VPN demo and failed to inform the system administrator.

8. Severity

Since there was little information given about the network this was detected on, I will evaluate this detect as if it was detected on my network.

(5+2)-(5+5)= -2

Criticality=5, This machine is the firewall and file server(Samba) for the network

Lethality=3, Attacker could glean important information on the target.

System Countermeasures=5, Latest stable version of FreeBSD running with no Telnet. External access via SSH, HTTP, SSL-HTTP(Apache) only.

Network Countermeasures=5, Firewall is the only way to enter/exit the network. Snort NIDS installed along with restrictive IP Filter rules. Port 500 is blocked.

9. Defensive Recommendation

Even though this detect appears to originate from a misconfigured VPN client, it would be wise to put this IP or IP block into a "watch list". Large UDP packets can conceal covert and DDOS control channels. If this IP/IP Block continues to appear, further investigation may be warranted.

10. Multiple Choice Question

Large UDP packets are not normally sent because:
A) It is quicker for the packet filter to process smaller packets
B) UDP is an unreliable protocol and sending large amounts of data is best sent via TCP to ensure data delivery
C) UDP has a Maximum Segment Size of 512 bytes
D) Many routers cannot handle large UDP packets

Answer: B) UDP is an unreliable protocol and sending large amounts of data is best sent via TCP to ensure data delivery

Assignment 2

Outsourcing IDS monitoring

Brian Varine
SANS GCIA New Orleans

It's early morning and you've just taken a seat at your desk - just like you do everyday. Firing up your trusty computer, you take a look at the morning news….only today something really catches your eye. One of the local companies in your area was hacked into yesterday and they've made the news. Unfortunately for them, the hackers obtained all of their credit card information from their database. Now the hackers are holding the data ransom. You take a gulp of coffee and say to co-workers; "Check out what happened to Acme!!" That's when you realize it could have been you.

Could it have been you? You have firewalls and check the logs periodically but would you even know what to look for? Maybe you need to look into an Intrusion Detection System (IDS). You're probably thinking that IDS's are complex and you don't even have the time to look at the firewall logs; so how are you going to check yet another system? This is where a new type of business may be worth looking into. Managed Security Monitoring services. In this paper I will describe what some of the benefits are to outsourcing your IDS monitoring (and why getting a GIAC cert is still a good idea).

What is Managed Security Monitoring (MSM)? In a nutshell, MSM is an IDS monitor akin to a burglar system (like ADT or Brinks) for your computer network. When suspicious activity is detected, an alert is generated. At this point, a live analyst will be notified and they can take a look at the event that triggered the alert. If the event is suspicious, it will be logged. If the event is serious enough, the analyst will call the appropriate personnel and inform them of what is going on. Presently, I could not find a firm that would actually take charge and attempt to repel the attack (i.e., shutdown a web server or write a firewall rule) but I suspect someone will probably offer this in the future.

There are many advantages to going with an outsourced MSM. Intrusion Detection requires a skilled person to analyze what is happening on the network. Unfortunately many companies do not have nearly enough people to go around so it is rare to find a person whose sole responsibility is to monitor the network for potential intrusions. Most security administrators have a variety of responsibilities along with being the "IDS guy". If they are lucky, they may get an hour or so of "quality" time with the IDS. With an outsourced MSM, the network is monitored 24 hours a day/7 days a week. This means that at 2am, your network is being monitored. Sunday? Monitored. IDS guy is on vacation? Monitored.

Another advantage is the fact that with an outsourced MSM, they get to figure out what is an alert and what is a false positive. IDS's generate a lot of alerts, especially when first installed.

This presents a problem for the security administrator. Management will certainly want their investment in an IDS to be working. This puts pressure on the security team to respond to the alerts that the IDS generates. It doesn't take very many "Ping Zero" alarms at 2am to cause the administrator to begin to either leave the pager at home or to disable a lot more alerts. Worse yet, if the administrator is continuously flooded with poor alerts, they may just turn the IDS off and never check it again! With an MSM, the call at 2am isn't going to happen unless a skilled person at the MSM thinks it's worth waking someone up for.

Advantage three is skill level. With an MSM, you have analysts that sit and monitor networks all day for signs of intrusion. Over time, this can have an enormous advantage. They get to see attacks on a variety of sources. They aren't limited to one network. This allows them to recognize attacks and patterns much better than a person who scans logs from one network for an hour each day.

The final advantage is the I&W advantage. I&W is used in the military to refer to *Indications and Warnings*. Those are things that lead up to an attack. Indications are things that, alone, seem benign but when coupled with other indicators, may indicate a possible attack. With the MSM monitoring a variety of networks, they may notice little things that an analyst on a single network would consider network noise or a random event. With the MSM, they can correlate these events and build a more comprehensive picture of what is happening. They may notice probing on ports that have typically been quiet. With that indicator they can investigate further and look for a reason why this is happening. If something is discovered, they can issue warnings. One would hope that these MSM companies would provide the rest of the world these warnings as well. The advantage to the subscriber would be an immediate notification vice having to wait to come into work and read it in E-mail….. six hours later.

Now that we have looked at some of the advantages, let's look at a few of the disadvantages are. The most obvious disadvantage is cost. MSM's are not cheap. Looking at a few MSM's (Brinks Internet Security and Counterpane) the cheapest price listed was in excess of $8000 per month (Brinks). Counterpane charges $12,000 per month. Obviously for some businesses this will be a considerable cost but for a small company this would not be a feasible option. Counterpane argues that the price is competitive with having your own in house monitoring. Looking at what a semi skilled administrator cost, they have a valid point, especially if you look at the fact that you have 24/7 monitoring. Still, for most companies, a recurring monthly cost of $12,000 may be a hard sell. Especially considering you still need to purchase an IDS (they monitor your IDS, they do not supply it).

Another caveat to look for in a MSM is who the company is. There are a few "MSM" services out there that claim to be an MSM but are merely a box they put on your network that sends out pages if something is detected (http://www.securityhome.com). This isn't any better than putting in your own IDS and having it send a page. The MSM you select needs to be a trusted partner. They will be the guardians to your network and you will trust them to protect your network. You can't be thinking about who is the cheapest solution, you need to think about who is the partner that you trust the most. For some organizations, no company will fit.

Some companies have gone to great lengths to ensure that they are a trusted entity. Counterpane has a secure facility where their operations center resides. They have video monitoring of every station and they make sure each analyst is bonded. If that isn't enough, they have two facilities on opposite coasts. Each facility can take over for the other in case it goes offline for any reason. It's clear they take the issue of trust very seriously.

Ok, so if MSM's are so great, why should I bother getting a SANS certification? Well, just like with Physical Security, you still need someone "on premises". MSM's may sound the alarm, but someone still needs to respond. It's going to help out your MSM and you a lot more if you both speak the same language. If your partner contacts you and says your network was just used as a Smurf attack amplifier, you need to know what a Smurf attack is. Sure the MSM's can take the time out to educate the administrator, but the response is going to be much quicker if the administrator knows how the attack works and what to look for. It will also help the administrator when dealing with the other administrators. It's probably not going to go over well with your DNS team if you come in and say "Hey, our MSM just said you guys got hacked by an TSIG overflow attack" and you don't know what that is.

Another good reason is that with the price of these services, it's unlikely that you will be monitoring all of your points of entry. It's similar to a home burglar alarm. Typically the front door and a few windows are monitored but what happens if the burglar enters from one of the windows that aren't monitored? The same thing applies to networks. Some companies have a lot of paths in and out of the network. If you can't afford to have the MSM monitor all of them, have them monitor the major ones. You can monitor the other points. In the worst-case scenario, you both monitor the same paths.

This is a basic overview of what Managed Security Monitoring is. If you think that this may be something for your organization, you need to consider a myriad of details before looking for a provider. I believe Managed Security Monitoring can be an asset to most companies should they decide to go with it.

IT World, November 13, 2000, "Outsourced Security: Consider it Carefully"
http://www2.itworld.com/cma/ett_content_article/0,2849,3412_3411,00.html

USA Today, April 3, 2000, "Net Security System Targets Cyburglars"
http://www.usatoday.com/life/cyber/tech/review/crh029.htm

Metases, "Intrusion Detection Systems: Proactive Security Management of the Network Enterprise" http://www.metases.com/files/IntruD.pdf

Computerworld, March 12, 2001, "Zen and the Art of Intrusion Detection"
http://computerworld.com/cwi/story/0,1199,NAV65-663_STO58458_NLTs,00.html

Counterpane, "Innovative E-Business Insurance Protection for Customers of Counterpane Internet Security" http://www.counterpane.com/pr-lloydswp.html

ZDNet, August 9, 1999, “Hack Attacks Drive Outsourced Security”
http://home.zdnet.com/eweek/stories/general/0,11011,411335,00.html

Assignment 3

Analyze This!
GIAC Enterprises

Overview:

Our organization has been given approximately a month worth of Snort logs for analysis and submit our findings to GIAC Enterprises. After careful analysis we have come up with a number of findings. We have also provided recommendations to make GIAC a more secure network.

Findings:

The network was subjected to a number of attack attempts over the course of a month. Some were more numerous than others but all should be taken seriously.

Summary of Attacks:

TCP SMTP Source Port traffic	100
SITE EXEC – Possible wu-ftpd exploit - GIAC000623	3
Null scan!	826
NMAP TCP ping!	558
DNS udp DoS attack described on unisog	16147 (!)
External RPC call	59
Watchlist 000222 NET-NCFC	2400
SYN-FIN scan!	51192
Happy 99 Virus	1
SMB Name Wildcard	515
SNMP public access	591
Back Orifice	77
SUNRPC highport access!	204
Queso fingerprint	710
WinGate 1080 Attempt	2240
connect to 515 from inside	160
STATDX UDP attack	1
connect to 515 from outside	4239
Watchlist 000220 IL-ISDNNET-990517	over 65,000
Attempted Sun RPC high port access	2054
Probable NMAP fingerprint attempt	8
Broadcast Ping to subnet 70	154
Russia Dynamo - SANS Flash 28-jul-00	546
Tiny Fragments - Possible Hostile Activity	5340

WU-FTPD Attacks:

11/26-17:30:50.939661	24.23.255.246:4507	->	MY.NET.130.98:21
12/21-15:26:29.595664	64.217.116.106:1684	->	MY.NET.97.162:21
12/16-12:21:46.219962	209.162.94.11:4584	->	MY.NET.156.127:21

The above servers should be checked **immediately** for signs of compromise. These servers may have been identified previously as running vulnerable versions of the WU-FTP daemon. The attack is a sign of complete compromise of a system. See CVE-1999-0080. Also see: http://www.cert.org/advisories/CA-2000-13.html

STATDX Attack:

01/06-06:39:35.583605	206.210.80.6:1074	->	MY.NET.6.15:32776

This machine should be checked **immediately** for signs of compromise. This machine may have been identified previously as running vulnerable rpc.statd service on Linux. The attack indicates complete compromise. See CVE-2000-0666. Also see http://www.cert.org/advisories/CA-2000-17.html

SNMP Attacks:

MY.NET.100.143:161
MY.NET.100.206:161
MY.NET.100.99:161
MY.NET.101.192:161
MY.NET.14.1:161
MY.NET.154.26:161
MY.NET.50.154:161

The above servers have SNMP running and were accessed by a large number of internal users.

01/11-18:12:07.868642	128.183.38.30:1032	->	MY.NET.154.26:161
01/12-09:31:41.697088	128.46.156.231:1030	->	MY.NET.100.206:161
01/12-09:32:04.134998	128.46.156.231:1094	->	MY.NET.100.143:161
01/12-09:32:10.408144	128.46.156.231:1096	->	MY.NET.100.99:161

The above external connections were made via the SNMP port. The four target servers should be inspected for signs of compromise. SNMP allows a remote console to manage a large number of devices. If an external device is allowed to connect to an internal machine using SNMP, they can control that machine as they see fit.

Denial Of Service Attack

One of the most aggressive attacks was a Denial of Service attack which occurred on 1/06. This attack originated from 209.67.50.203 (Exodus Comm) and targeted DNS servers on MY.NET.1.3/MY.NET.1.4/MY.NET.1.5. Over the course of 90 minutes, the three servers were hit with approximately 16150 hits. This averages out to 179 per minute, or 60 per minute per server.

The effect of this would have been to tie up all three DNS servers with lookups. Users attempting to use the DNS would have probably encountered slow or no response from the DNS server.

SMTP Attacks:

01/03-16:35:10.148560 165.112.79.25:25 -> MY.NET.253.42:25

You may want to inspect the machine listed above. On the date listed, it was sent 11 packets in one second. This machine may have been previously identified as a machine running an SMTP server and vulnerable to an overflow attack.

The network was also scanned on 12/29 by 165.112.79.25 for possible SMTP servers running. This scan did not appear to scan the 253 subnet, which would indicate that the attack on MY.NET.253.42 used results from a previous scan. An interesting note is the domain belongs to the National Institutes of Health. This would indicate the source IP had been compromised.

Watchlist Detects:

MY.NET.6.47
MY.NET.6.7
MY.NET.6.34
MY.NET.6.35
MY.NET.253.53
MY.NET.5.29
MY.NET.253.52
MY.NET.253.51
MY.NET.253.41
MY.NET.253.42
MY.NET.253.43
MY.NET.145.9
MY.NET.145.18
MY.NET.110.150
MY.NET.100.230
MY.NET.1.2

The above listed machines are listed as having made connections to networks, which are on the "watchlist". The connections were made to Ports 25, 113, 143, 443. Are these mail servers?

SMB Name Wildcard Detects:

There were numerous machines that had NetBIOS name query attempts made on them. Over 65 machines were identified as having been queried. Below are the machines that drew the most traffic and should be investigated soon.

MY.NET.98.122:137
MY.NET.6.15:137
MY.NET.101.192:137
MY.NET.100.130:137

Broadcast Ping to Subnet 70:

12/01-19:11:20.273721	213.154.131.131:	->	MY.NET.70.255:
12/01-17:25:08.240600	193.231.220.137:	->	MY.NET.70.255:
11/24-21:54:56.975159	194.102.93.101:	->	MY.NET.70.255:

The above entries are significant because they show where an attacker has most likely performed a Smurf attack on another network. These machines were sent packets numerous times over a short period of time, which would indicate they were probably used as an amplifier for a denial of service attack. Your network routers allow broadcast pings to be sent from an external source. The problem with this is that an attacker can spoof broadcast ping packets. When the internal hosts receive this, they respond to the spoofed IP (the victim). An attacker can send many broadcast pings to different subnets. When the combined response from many subnets arrives at the victim network it becomes saturated causing a denial of service.

11/26-21:45:56.114233	193.231.169.166:	->	MY.NET.70.255:
01/15-07:58:25.750259	212.204.137.53:	->	MY.NET.70.255:
11/29-18:26:20.772161	151.21.208.42:	->	MY.NET.70.255:
11/29-19:38:24.779497	212.35.129.91:	->	MY.NET.70.255:
12/30-02:11:26.723709	211.33.158.136:	->	MY.NET.70.255:
12/30-06:08:30.357942	209.21.180.147:	->	MY.NET.70.255:
12/30-22:52:00.442649	213.97.215.87:	->	MY.NET.70.255:
12/29-16:26:01.298554	62.226.88.105:	->	MY.NET.70.255:
12/09-18:28:37.580861	62.98.69.17:	->	MY.NET.70.255:
01/01-11:30:23.281931	211.33.158.136:	->	MY.NET.70.255:
01/01-12:27:30.545037	203.106.43.141:	->	MY.NET.70.255:
01/01-16:29:42.641202	217.80.182.182:	->	MY.NET.70.255:
12/26-21:10:46.062791	213.154.130.64:	->	MY.NET.70.255:
12/28-11:52:58.292917	216.22.239.2:	->	MY.NET.70.255:
01/10-17:30:37.666932	195.159.0.162:	->	MY.NET.70.255:
12/01-18:16:15.632189	193.231.220.91:	->	MY.NET.70.255:
12/01-18:41:03.663963	193.231.220.214:	->	MY.NET.70.255:
12/01-18:51:29.743876	193.231.220.125:	->	MY.NET.70.255:
12/01-19:04:16.020754	193.231.220.91:	->	MY.NET.70.255:
12/01-19:07:31.789486	217.10.207.88:	->	MY.NET.70.255:

These machines received broadcast pings from external machines on one to five occasions. This was most likely a network-mapping attempt. By using the broadcast ping, the attacker can receive replies from all of the active machines. This gives the attacker a quick map of that subnet. By sending the packet a few times, the attacker can gain a more reliable map.

Printer Port Detects:

12/20-21:58:38.206581	MY.NET.163.17:2178	->	148.243.214.7:515
12/07-22:06:02.060089	MY.NET.179.78:4877	->	24.13.123.8:515
11/29-20:31:12.014245	MY.NET.219.122:50325	->	128.2.166.68:515
12/08-22:28:32.862899	MY.NET.219.194:2351	->	131.204.205.101:515
12/07-14:46:01.272485	MY.NET.253.12:34091	->	64.23.4.67:515
12/07-14:46:01.285319	MY.NET.253.12:34091	->	64.23.4.67:515
12/08-13:58:20.072019	MY.NET.253.12:61882	->	64.23.4.67:515
12/01-10:21:50.598369	MY.NET.60.16:1165	->	151.196.73.119:515
01/08-21:26:34.695216	MY.NET.60.38:513	->	128.8.3.106:515
01/08-21:26:39.785432	MY.NET.60.38:513	->	128.8.3.106:515
01/08-21:29:04.786541	MY.NET.60.38:513	->	128.8.3.106:515
12/20-23:22:47.929679	216.119.15.88:1040	->	MY.NET.130.86:515
12/20-23:22:47.250185	216.119.15.88:1032	->	MY.NET.100.209:515
12/20-23:38:34.311898	216.119.15.88:1035	->	MY.NET.214.166:515
12/20-23:22:47.250433	216.119.15.88:1036	->	MY.NET.99.104:515

The machines above are communicating to other networks on Port 515 which is the LPR (printer) port. Normally this traffic should be shielded from leaving the network. These machines may be sending print traffic to other networks. This means an attacker may be reading internal data and printing in on an external machine. It is also possible to compromise a print server and use that as a jump off point for additional attacks on the network.Of particular note is MY.NET.100.209:515, MY.NET.130.86:515, MY.NET.214.166:515, and MY.NET.99.104:515 During an approximate 60 minute period, an external machine attempted to connect to these machines numerous times. These machines were most likely identified as being vulnerable on previous scans. These four machines should be inspected as soon as possible.

Also note MY.NET.60.38. It appears to be sending back traffic from the Rlogin port, which could indicate an attacker has logged into that machine using the Rlogin service. Rlogin checks to see if incoming connections are coming from hosts in the '.rhosts' file, and should be coming from ports between 512-1023.

Back Orifice Detects:

MY.NET.202.94:31337
MY.NET.7.22:32771

These machines should be inspected for possible Back Orifice inspection. Inspecting the logs I found connection attempts to these two machines on separate occasions.

MY.NET.98.15:31337
MY.NET.98.157:31337
MY.NET.98.70:31337

Connection attempts were made on these machines but were not part of an overall scan.

Scans for Back Orifice were perfomed on:
11/26 and 12/09 by 209.94.199.143 (Telecommunications Services of Trinidad and Tobago).
12/01 by 62.136.71.93(Planet Online Ltd)

Happy 99 Virus:

12/22-20:25:10.840208 63.216.198.158:2239 -> MY.NET.6.47:25

This machine received the Happy99 virus from 63.216.198.158(Fanfiction Mailing List). This virus (actually it is a trojan/worm) propagates via E-mail so it would appear that the virus was not executed on your network. If it had been, there would be a number of outbound detects.

Attempted Sun RPC Detects:

MY.NET.213.158:32771
MY.NET.105.115:32771
MY.NET.98.192:32771
MY.NET.98.226:32771
MY.NET.97.245:32771
MY.NET.213.158:32771
MY.NET.223.106:32771
MY.NET.213.158:32771
MY.NET.221.130:32771
MY.NET.223.106:32771
MY.NET.97.74:32771
MY.NET.97.96:32771
MY.NET.98.238:32771
MY.NET.97.45:32771
MY.NET.97.208:32771
MY.NET.97.213:32771

The above machines are most likely users of ICQ, a popular "Instant Messaging" service. All of the detects for those IP's had source addresses belonging to AOL (parent company of ICQ)

12/15-00:36:43.676300 216.13.244.241:3456 -> MY.NET.221.130:32771

This detect may warrant further investigation. The listed machine attempted numerous connections to MY.NET.221.130. This may be an indication of a Sun machine running RPC. The attacker can attempt to overflow the RPC stack and gain control of the machine. See CVE-1999-0003

Dynamo Detects

12/08-15:36:30.735338	MY.NET.205.138:6699	->	194.87.6.38:2478
12/08-15:37:12.356256	194.87.6.38:2478	->	MY.NET.205.138:6699

This connection was flagged because it originated from a "significantly compromised" system in Russia that was the subject of a SANS flash bulletin. I could not locate the particular flash message but I was able to pull information from the SANS current detects page. Although this was identified in July, it still warrants further investigation. The source IP connected to a machine running Napster on your network.

Dynamo information→ http://www.sans.org/y2k/073000.htm

Tiny Fragments:

11/29-23:17:50.134801	MY.NET.219.122:	->	208.162.62.208:
01/05-03:50:50.679956	202.101.43.220:	->	MY.NET.1.10:
12/31-23:45:47.026613	202.205.5.10:	->	MY.NET.1.8:
11/28-04:27:52.346131	63.210.46.242:	->	MY.NET.1.9:
11/28-15:13:30.851379	63.210.46.242:	->	MY.NET.100.230:
01/03-15:13:10.388407	24.64.14.194:	->	MY.NET.201.14:
01/11-23:44:17.189538	65.4.87.43:	->	MY.NET.202.18:
12/16-15:25:14.319245	24.2.170.67:	->	MY.NET.215.106:
01/12-19:47:58.862156	65.4.87.43:	->	MY.NET.217.162:
11/26-15:14:03.090933	213.112.131.135:	->	MY.NET.219.46:
01/13-02:28:30.039894	8.8.8.8:	->	MY.NET.60.11:
01/13-02:32:44.810948	4.4.4.4:	->	MY.NET.60.11:
12/23-11:29:21.620703	210.159.220.160:	->	MY.NET.71.38:
12/15-18:26:28.461159	24.68.58.96:	->	MY.NET.98.123:

The above machines were sent tiny fragments. A few machines were sent these packets hundredes times.
MY.NET.1.8= 3165
MY.NET.1.10 = 1265
MY.NET.27.162= 870
MY.NET.60.11= 168

These tiny fragment packets were sent from a volume of IP's. It's possible that these fragments were sent as a Denial of Service attack. Other explainations are that a "covert" channel has been established on these machines. Right now it is unclear why these machines were sent these packets. The small number of machines affected would indicate that this was not part of a random scan.

Other scans:

There were numerous other types of scans that were performed on your network. These scans were not outright attacks but rather "surveillance". These scans are useful to the attacker because they give them useful information on the network. Information such as OS and services running are extremely useful to an attacker. Armed with this information the attacker can identify points of attack and execute them.

Scans:
Queso – Attempts to identify OS running on targeted machine
NMAP - Attempts to identify OS running on targeted machine, also identifies open ports. NMAP can use a variety of fingerprint tools like SYN-FIN, NULL, and XMAS packets.
SYN-FIN – This can identify a particular OS running or it can cause unknown errors to occur. Since a SYN-FIN is not supposed to happen, OS's respond differently upon receiving a SYN-FIN packet.
NULL – This scan sets no flags on the TCP header. It is similar to the SYN-FIN in that it is not supposed to happen.

Recommendations:

Firewalls and NAT
The first recommendation I have is to install a set of firewalls and to reduce your internet footprint by renumbering your internal addresses to non-routable addresses When I inspected the logs I found that there is nothing to prevent someone from another network from connecting to ALL of your internal machines. The network is wide open to the outside. This is akin to having an office building with all of the windows and doors removed. A firewall would be able to reduce this vulnerability considerably. Depending on the size, complexity, and bandwidth needs of your network, you may have to install a series of firewalls.

Firewalls have the benefit of rules to direct traffic. This will allow you to permit and deny traffic to your network. For instance, in the firewall you can write a rule that allows external SMTP traffic to go ONLY to the SMTP server. If someone attempts to connect to another machine on the SMTP port, the firewall will block that connection. Some firewalls (such as Symantec's Raptor Firewall) will actually do "stateful packet inspection" to make sure that only certain traffic can pass. For instance, an attacker may try to sneak out of your network using VNC (a popular Remote Control program) on Port 80. Since Port 80 is allowed out in most organizations, an attacker may be able to circumvent the firewall by operating on Port 80. With a firewall that does stateful packet inspection, ONLY http traffic would be allowed to pass and the attacker would be thwarted.

Renumbering your internal addresses to a 10.x.x.x or 192.168.x.x scheme will hide your internal network from the outside. The firewall will perform Network Address Translation (NAT), which will allow users on the network to access external sites. To an attacker, your network will no longer show up as a Class B address, but will show up as a few individual IP's. The Snort logs indicated that numerous scans were made on your network. Over 51,000 Syn-Fin packets alone were targeted against your internal network! These scans were looking for FTP, POP2, DNS, and

other servers running on your network. Once the attacker identifies which machines are vulnerable, they can return later to execute attacks.

There are also a number of connects from machines that are on a "watchlist". The watchlisted machines made numerous scans and connected to SMTP, IMAP, HTTPS ports. If these machines are on a watchlist, I would assume there is a reason for this. By using a firewall, you could block traffic from the suspect subnets.

One other benefit of having a firewall will be the logging capability available. With the Snort logs that were provided, it is difficult to determine if attacks were successful. By having a firewall, you can inspect the logs and correlate the firewall data with Snort data to see if the attack was passed through to the internal network.

There are many more benefits to using a firewall and NAT. If security dollars are tight, installing a firewall and using NAT will give you the most bang for your security buck.

Continue using Snort

Snort is basically your burglar alarm. While firewalls are very effective pieces for security, they don't tell you what attackers are trying to do. With Snort you can identify certain attacks that are being directed against your network. A firewall will only log that it allowed or denied the connection.

I would also recommend a Snort sensor on both sides of the firewall. The external sensor will tell you what has been attempted. The internal sensor will show you which of those attempts actually made it through the firewall. Internal sensors can also alert you to potential attacks from against your network from attackers inside the network.

Use Access Control Lists on Routers

Looking at the log files I found that routers could be used much more effectively. Currently the routers allow almost all traffic in and out. By utilizing Access Control Lists (ACL's) you can filter out simpler attacks such as broadcast pings and spoofed internal addresses

Establish a Security Policy

During analysis of your network it is clear that there are machines running all kinds of services. While most of these services are needed and necessary, there are a number of services that were not. I identified ICQ, AIM, Napster, and other services running on machines within your network. These services have little, if any, business reason to be on the networks. In the case of Napster, you are hosting servers that most likely illegally distribute music. Napster is also a notorious bandwidth hog. The security policy should establish what is allowed and what is not allowed on the network.

Also part of this policy should be something that requires all servers run only the necessary services needed. Most OS's install services by default that should not be running. If you are hosting

an SQL server, there is no reason why IIS should be running. Even printers run vulnerable services!

Your policy should not be limited to these! Security policy can cover a wide area!

Scan your own network

If the "bad guys" can use automated scanning tools to discover what is vulnerable on your system, then you should too. System administrators typically have a lot of work to do and it's not uncommon for them to leave a service turned on when it should be off. They may also not be aware of a particular vulnerability. By doing regular scans of your network you can discover things before the bad guys do. There are a number of tools that you can use to scan networks. These include NMAP, SAINT, Nessus, and CyberCop Security Scanner. Even better NMAP, SAINT, and Nessus are free!

Use a current virus scanner and E-mail "firewall"

The use of an anti-virus tool cannot be over emphasized. Many of the current vulnerabilities today are "backdoor" programs that typically come in via E-mail. Unsuspecting users kick off what they think is a cute program. This program runs and usually has something to amuse the receiver while in the background it installs the backdoor program and the machine is compromised. Current anti virus software is extremely successful but ONLY when it is updated regularly. Ensure that your organization has a plan for making sure anti virus software is updated regularly.

Anti virus software should also be installed on your mail servers. Since the mail servers are the first place in your network that infected E-mails will arrive, it makes sense to inspect them there. By inspecting the files before delivery to the user you eliminate the possibility that the file will be opened by an unsuspecting user (who probably disabled the anti virus scanner on their desktop). One thing to consider is the amount of resources this will take. If your current mail server is close to running out of processor power and memory, you will want to upgrade your servers before attaching anti virus software to them.

Firewalls are not magic shields. Although they do a great job of knocking down a lot of malicious traffic, they cannot block what you are allowing in. E-mail has to be let through the firewall! There is no way around this. A good security tool is a "firewall" for your E-mail traffic. Most vendors are calling this "content filtering". Tools such as *Mailsweeper* are put between your firewall and your mail server. These tools inspect all E-mails for things that you have defined. Upon discovery of an E-mail that meets the definition, it can be quarantined, deleted, or sent to a virus scanner for repair. This is a great tool for blocking things like .VBS attachments, which are attached to E-mails. Not only can these tools block incoming mail, they can block outgoing mail as well. This is particularly useful if a user in your network becomes infected with a virus such as Melissa or the I Love You virus. This prevents your network from sending infected files to other networks.

Looking at the Snort logs, it appears that your network is doing an adequate job of containing these. One instance of Happy99 was detected. If your anti virus defense had been inadequate, there would have been many more cases of the virus leaving the network.

Still, there appeared to be a few instances of Back Orifice running so it's still a good idea to review your use of anti virus products.

Last Updated: May 28th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Boston SEC503	Boston, MA	Oct 09, 2017 - Oct 14, 2017	Community SANS
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced