



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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



SANS GIAC Certified Intrusion Detection Analyst Practical Assignment

Prepared by Wayne Veilleux

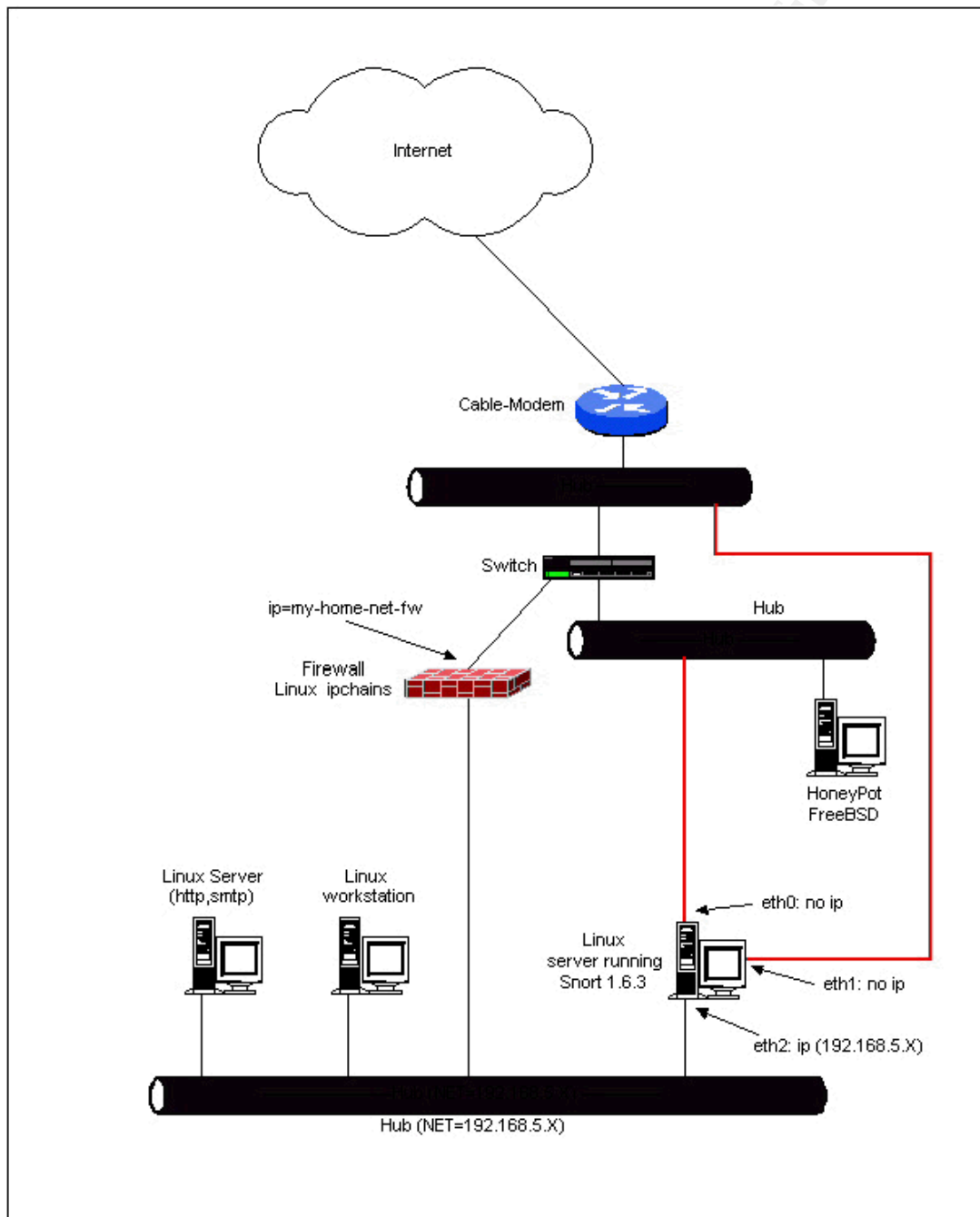
© SANS Institute 2000 - 2005, Author retains full rights.

TABLE OF CONTENTS

Introduction	1
Assignment 1 – 4 Network Detects:	2
1.1 Detect 1	2
1.2 Detect 2	20
1.3 Detect 3	21
1.4 Detect 4	23
Assignment 2 – Evaluate an Attack – WinGate attempt:	24
Assignment 3 – “Analyze This” Scenario :	27
3.1 Introduction	27
3.2 Analysis:	27
3.2.1 Suspected Compromises systems with recommendation:	27
3.2.2 Malicious Traffic by date	30
3.2.3 Conclusion and final recommendation:	31
3.2.4 Detect in detail:	31
3.2.4.1 Summary of the possible exploit from the Snort Alerts:	31
3.2.4.2 Happy 99 Virus summary:	32
3.2.4.3 Possible wu-ftpd exploit and site exec - GIAC000623:	32
3.2.4.4 site exec - Possible wu-ftpd exploit - GIAC000623:	33
3.2.4.5 TCP SMTP Source Port traffic:	34
3.2.4.6 Tiny Fragments - Possible Hostile Activity:	34
3.2.4.7 External RPC call:	35
3.2.4.8 Queso(Unix scan tool) fingerprint:	35
3.2.4.9 Probable NMAP(Unix scan tool) fingerprint attempt:	36
3.2.4.10 SUNRPC highport access:	37
3.2.4.11 NMAP TCP ping:	38
3.2.4.12 Null scan:	39
3.2.4.13 SMB Name Wildcard (scan for smb services; MS or Samba):	42
3.2.4.14 SNMP public access:	43
3.2.4.15 Attempted Sun RPC High port access:	44
3.2.4.16 Watchlist 000220 IL-ISDNNET-990517:	44
3.2.4.17 SynFin scan:	45
3.2.4.18 WinGate 1080 Attempt:	47
3.2.4.19 Watchlist 000222 NET-NCFC (The Computer Network Center Chinese Academy of Sciences):	51
3.2.4.20 Summary of the possible exploit from the Snort Scan Report:	53
3.2.4.21 UDP Scan Report:	54
3.2.4.22 Summary of the possible alert from the raw Snort log file (SOOS*.txt):	55
Assignment 4 – “Analysis Process :	55

Introduction

This is the practical assignment required for GCIA (GIAC Certified Intrusion Detection Analyst) certification Level 2. The assignment 1 contain 4 detects that I got from my home network using Snort 1.6.3. The assignment 2 describe in-depth an attack. The assignment 3 analyse data collect files from a sinister site and give some recommendation. And, assignment 4 describe how I did the assignment 3. Here is a small drawing of the setup I'm using to protect my internal network and from which I got the trace for assignment 1:



Assignment 1 – 4 Network Detects:

NOTE: Due to issues surrounding the legality of providing information about the behavior of another companies IP addresses, both the source and destination IP addresses have been sanitized. The monitored networks IP addresses have been replaced by my-home-net-fw. IP addresses categorized as "intruder" have the last two octets of the IP address sanitized.

Example:

My subnet = my.home.net.fw

Intruder = the.intruder.x.x

1.1 Detect 1

From Snort Alert:

Date: 1 November 2000/11/24

Time: 19:50 to 19:54

Only headers:

[illegible]


```

B8 08 00 8B 0E 1E 00 49 BA FF FF CD 31 B8 00 01 .....I....1...
BB 00 0F CD 31 73 10 3D 08 00 0F 85 65 01 B8 00 ....1s.=....e...
01 CD 31 0F 82 5C 01 A3 1C 06 89 16 1E 06 C1 E3 ..1..\.....
04 89 1E 20 06 66 8B 36 08 06 66 8B 3E FB 07 66 ... .f.6..f.>..f
8B 0E FF 07 E8 49 00 66 8B 36 0C 06 66 8B 3E 23 .....I.f.6..f.>#
08 66 8B 0E 27 08 E8 37 00 8E 06 16 06 66 8B 3E .f..'..7.....f.>
4B 08 66 8B 0E 4F 08 66 31 C0 66 C1 E9 02 67 F3 K.f..O.fl.f...g.
66 AB B4 3E 8B 1E 06 06 CD 21 B8 01 01 8B 16 1E f..>.....!.....
06 CD 31 1E 0F A1 8E 1E 16 06 66 64 FF 2E 10 06 ..1.....fd....
66 89 F0 66 25 FF 01 00 00 66 01 C1 29 C6 66 29 f..f%....f..)f)
C7 66 89 0E 26 06 66 89 3E 22 06 E8 FE 00 89 36 .f..&.f.>".....6
3E 06 66 C1 EE 10 89 36 42 06 8B 1E 06 06 89 1E >.f....6B.....
3A 06 C7 06 46 06 00 42 E8 F2 00 A1 1C 06 A3 4E :...F..B.....N
06 C7 06 3E 06 00 00 C6 06 47 06 3F A1 28 06 09 ...>.....G.?.(..
C0 75 09 A1 26 06 3B 06 20 06 76 03 A1 20 06 A3 .u..&.;. .v. . .
42 06 E8 C8 00 66 31 C9 8B 0E 46 06 66 8B 3E 22 B....f1...F.f.>"
06 66 01 0E 22 06 66 29 0E 26 06 66 31 F6 C1 E9 .f.."f).&.f1...
02 1E 06 8E 06 16 06 8E 1E 1E 06 67 F3 66 A5 07 .....g.f..
1F 66 03 0E 26 06 75 AF C3 3C 3A 74 06 3C 2F 74 .f..&.u..<:t.</t
02 3C 5C C3 BE 64 07 89 F3 26 8A 05 47 88 04 38 .<\..d..&..G..8
E0 74 0E 08 C0 74 0A 46 E8 DE FF 75 EC 89 F3 74 .t...t.F...u...t
E8 C3 BA 25 05 EB 08 BA 33 05 EB 03 BA 3D 05 52 ...%....3....=R
8B 1E 62 07 C6 07 24 BB 64 07 EB 1E E8 ED 00 BA ..b...$.d.....
77 05 EB 12 BA 90 05 EB 0D BA A2 05 EB 08 BA B4 w.....
05 EB 03 BA 77 05 52 BB 18 05 E8 14 00 5B E8 10 ....w.R.....[..
00 BB 41 04 E8 0A 00 B8 FF 4C CD 21 43 B4 02 CD ..A.....L.!C...
21 8A 17 80 FA 24 75 F4 C3 0D 0A 24 50 51 57 31 !....$u....$PQWl
C0 BF 2A 06 B9 19 00 F3 AB 5F 59 58 C3 B8 00 03 ..*.....YX....
BB 21 00 31 C9 66 BF 2A 06 00 00 CD 31 C3 00 00 .!1.f.*....1...
30 E4 E8 5F FF 89 DE 8B 3E 66 04 EB 18 B4 3B E8 0..._....>f....;
52 FF 81 FE 64 07 74 13 8A 84 FF FF E8 3A FF 74 R...d.t.....:t
04 C6 04 5C 46 E8 03 00 72 E3 C3 E8 36 00 BB 44 ...F...r...6..D
00 8A 07 88 04 43 46 08 C0 75 F6 06 57 1E 07 E8 .....CF...u..W...
9A FF BB 2A 06 8C 9F 04 00 89 9F 02 00 BA 64 07 ...*.....d.
B8 00 4B CD 21 5F 07 72 09 B4 4D CD 21 2D 00 03 ..K.!_r..M.!-...
F7 D8 EB 28 80 3E 69 08 05 72 20 B8 00 58 CD 21 ...(>i..r ..X.!
A2 67 08 B8 02 58 CD 21 A2 68 08 B8 01 58 BB 80 .g...X.!h...X..
00 CD 21 B8 03 58 BB 01 00 CD 21 C3 9C 80 3E 69 ..!...X....!...>i
08 05 72 1A 50 53 B8 03 58 8A 1E 68 08 30 FF CD ..r.PS..X..h.0..
21 B8 01 58 8A 1E 67 08 30 FF CD 21 5B 58 9D C3 !..X..g.0...[X..
4C 6F 61 64 20 65 72 72 6F 72 3A 20 24 3A 20 63 Load error: $: c
61 6E 6E 6F 74 20 6F 70 65 6E 24 3A 20 6E 6F 74 annot open$: not
20 45 58 45 24 3A 20 6E 6F 74 20 43 4F 46 46 20 EXE$: not COFF
28 43 68 65 63 6B 20 66 6F 72 20 76 69 72 75 73 (Check for virus
65 73 29 24 6E 6F 20 44 50 4D 49 20 2D 20 47 65 es)$no DPMI - Ge
74 20 63 73 64 70 6D 69 2A 62 2E 7A 69 70 24 6E t csdpmi*b.zip$n
6F 20 44 4F 53 20 6D 65 6D 6F 72 79 24 6E 65 65 o DOS memory$nee
64 20 44 4F 53 20 33 24 63 61 6E 27 74 20 73 77 d DOS 3$can't sw
69 74 63 68 20 6D 6F 64 65 24 6E 6F 20 44 50 4D itch mode$no DPM
49 20 73 65 6C 65 63 74 6F 72 73 24 6E 6F 20 44 I selectors$no D
50 4D 49 20 6D 65 6D 6F 72 79 24 90 90 90 90 90 PMI memory$.....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 4C 01 03 00 00 00 00 00 .....L.....
00 00 00 00 00 00 00 00 1C 00 0F 01 0B 01 00 00 .....
58 3D 01 00 00 18 00 00 00 4A 00 00 A8 10 00 00 X=.....J.....
A8 10 00 00 00 4E 01 00 2E 74 65 78 74 00 00 00 .....N...text...

```

[illegible]

Prepared by Wayne Veilleux

```

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] OVERFLOW-NOOP-X86 [**]
11/01-19:54:29.407122 the.intruder.x.x:59008 -> my.home.net.fw:61570
TCP TTL:44 TOS:0x0 ID:0 DF
*****PA* Seq: 0x96E1F37A Ack: 0x97F3E2C4 Win: 0xF928
TCP Options => NOP NOP TS: 1091630378 45176319
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....

```

.....

```

90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....

```

```

==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+
[**] OVERFLOW-NOOP-X86 [**]
11/01-19:54:29.431838 the.intruder.x.x:59008 -> my.home.net.fw:61570
TCP TTL:44 TOS:0x0 ID:0 DF
*****PA* Seq: 0x96E20A1A Ack: 0x97F3E2C4 Win: 0xF928
TCP Options => NOP NOP TS: 1091630381 45176322
80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 .....
80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 .....
80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 .....
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB .....
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB .....
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB .....
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB .....
AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB AB .....
AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC .....
AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC .....
AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC .....
AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC AC .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 84 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 85 .....
86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 .....
86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 .....
86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 .....
86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 86 .....
87 87 87 87 87 87 87 87 87 87 87 87 87 87 87 87 .....
87 87 87 87 87 87 87 87 87 87 87 87 87 87 87 87 .....

```



```

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
[**] OVERFLOW-NOOP-X86 [**]
11/01-19:54:29.440013 the.intruder.x.x:59008 -> my.home.net.fw:61570
TCP TTL:44 TOS:0x0 ID:0 DF
*****PA* Seq: 0x96E21B12 Ack: 0x97F3E2C4 Win: 0xF928
TCP Options => NOP NOP TS: 1091630381 45176323
7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D }}}}}}}}}}}}}}}}}}}
7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D }}}}}}}}}}}}}}}}}}}
7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D 7D }}}}}}}}}}}}}}}}}}}
7D 7D 7D 7D 7D 7D 7D 7D 7E 7E 7E 7E 7E 7E 7E }}}}}}}}}~::~::~::
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E ~::~::~::~::~::~
7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E 7E ~::~::~::~::~::~
7E 7E 7E 7E 7E 7E 7E 7E 8C 8C 8C 8C 8C 8C 8C ~::~::~~.....
8C 8C 8C 8C 8C 8C 8C 8C 8C 8C 8C 8C 8C 8C 8C .....
8C 8C 8C 8C 8C 8C 8C 8C 8D 8D 8D 8D 8D 8D 8D .....
8D 8D 8D 8D 8D 8D 8D 8D 8D 8D 8D 8D 8D 8D 8D .....
8D 8D 8D 8D 8D 8D 8D 8D 8E 8E 8E 8E 8E 8E 8E .....
8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E .....
8E 8E 8E 8E 8E 8E 8E 8E 8F 8F 8F 8F 8F 8F 8F .....
8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F 8F .....
8F 8F 8F 8F 8F 8F 8F 8F 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 91 91 91 91 91 91 91 .....
91 91 91 91 91 91 91 91 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 6A 6A 6A 6A 6A 6A 6A .....jjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A 6A jjjjjjjjjjjjjjjjjjjj
6A 6A 6A 6A 6A 6A 6A 6A 10 11 00 00 00 00 07 07 jjjjjjjjjj.....
07 07 00 00 06 06 06 06 07 07 00 00 00 00 00 .....
07 07 00 00 06 06 06 06 06 06 06 06 00 00 07 07 .....
00 00 00 00 00 00 07 07 07 07 00 00 00 00 00 .....
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
07 07 00 00 12 13 07 07 07 07 00 00 00 00 07 07 .....
00 00 00 00 06 06 06 06 06 06 06 06 00 00 14 00 .....
00 15 16 17 18 19 07 07 04 04 04 04 04 04 04 .....

```

```

04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 .....
04 04 04 04 04 04 04 04 05 05 05 05 05 05 05 .....
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
06 06 06 06 06 06 06 06 04 04 04 04 04 04 04 .....
04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 .....
04 04 04 04 04 04 04 04 06 06 06 06 06 06 06 .....
05 05 05 05 05 05 05 05 04 04 04 04 04 04 04 .....
04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 .....
04 04 04 04 04 04 04 04 1A 1B 1C 00 00 1D 07 07 .....
00 1E 1F 20 00 21 07 07 07 07 22 00 23 24 25 00 ... !...".#$%.
00 26 27 28 06 06 06 06 06 06 06 06 00 29 2A 00 .&' (.....)*.
00 2B 2C 00 2D 2E 07 07 07 07 2F 30 31 32 33 00 .+,-...../0123.
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
06 06 06 06 06 06 06 06 06 06 06 06 07 07 07 .....
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
07 07 07 07 06 06 06 06 05 05 05 05 05 05 05 .....
05 05 05 05 05 05 05 05 1A 1B 1C 00 00 1D 07 07 .....
00 1E 1F 20 00 21 07 07 07 07 22 00 23 24 25 00 ... !...".#$%.
00 26 27 28 06 06 06 06 06 06 06 06 00 29 2A 00 .&' (.....)*.
00 2B 2C 00 2D 2E 07 07 07 07 2F 30 31 32 33 00 .+,-...../0123.
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
06 06 06 06 06 06 06 06 06 06 06 06 07 07 07 .....
05 05 05 05 05 05 05 05 05 05 05 05 05 05 05 .....
07 07 07 07 06 06 06 06 05 05 05 05 05 05 05 .....
05 05 05 05 05 05 05 05 34 35 36 00 37 38 39 00 .....456.789.
00 3A 3B 3C 3D 3E 07 07 07 07 3F 40 41 42 43 00 .:;<=>....?@ABC.
00 44 45 46 06 06 06 06 06 06 06 06 07 07 07 07 .DEF.....
07 07 00 00 06 06 06 06 06 06 06 06 00 00 07 07 .....
06 06 06 06 06 06 06 06 34 35 36 00 37 38 39 00 .....456.789.
00 3A 3B 3C 3D 3E 07 07 07 07 3F 40 41 42 43 00 .:;<=>....?@ABC.
00 44 45 46 06 06 06 06 06 06 06 06 07 07 07 07 .DEF.....
07 07 00 00 06 06 06 06 06 06 06 06 00 00 07 07 .....
06 06 06 06 06 06 06 06 34 35 36 00 37 38 39 00 .....456.789.
00 3A 3B 3C 3D 3E 07 07 07 07 3F 40 41 42 43 00 .:;<=>....?@ABC.
00 44 45 46 06 06 06 06 06 06 06 06 07 07 07 07 .DEF.....
07 07 00 00 06 06 06 06 06 06 06 06 00 00 07 07 .....
06 06 06 06 06 06 06 06 47 48 49 4A 4B 4C 4D 00 .....GHIJKLM.
00 4E 4F 50 51 52 07 07 07 07 00 00 00 53 07 07 .NOPQR.....S..
07 07 54 00 07 07 07 07 47 48 49 4A 4B 4C 4D 00 ..T.....GHIJKLM.
00 4E 4F 50 51 52 07 07 07 07 00 00 00 53 07 07 .NOPQR.....S..
07 07 54 00 07 07 07 07 47 48 49 4A 4B 4C 4D 00 ..T.....GHIJKLM.
00 4E 4F 50 51 52 07 07 07 07 00 00 00 53 07 07 .NOPQR.....S..
07 07 54 00 07 07 07 07 47 48 49 4A 4B 4C 4D 00 ..T.....GHIJKLM.
00 4E 4F 50 51 52 07 07 .....NOPQR..

```

```

==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+==+
[**] OVERFLOW-NOOP-X86 [**]
11/01-19:54:45.716453 the.intruder.x.x:59008 -> my.home.net.fw:61570
TCP TTL:44 TOS:0x0 ID:0 DF
*****PA* Seq: 0x96FC331A Ack: 0x97F3E2C4 Win: 0xF928
TCP Options => NOP NOP TS: 1091632010 45177951
D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 D1 .....
7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C |||||
7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C |||||

```

Page 14
Author retains full rights.

[illegible]

.....

```
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
  
++++++  
y.home.net.fw:6157  
0xF928
```

```

+++++
ay.home.net.fw:6157
0xF928
}}}}}}}}}}}}}}}}}}
}}}}}}}}}}}}}}}}}}
}}}}}}}}}}}}}}}}}}
}}}}}}}}}}}}}}}}}}
~::~::~::~::~::~::~
~::~::~::~::~::~::~
~::~::~::~::~::~::~

```

```

7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 94 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 95 .....
00 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 .....
D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 .....
D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 .....
D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 D2 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 .....
C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 .....
C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 .....
C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 .....
C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 C5 .....
C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 .....
C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 C8 .....
C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 .....
C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 C9 .....
CA CA CA CA CA CA CA CA CA CA CA CA CA CA CA CA .....
CA CA CA CA CA CA CA CA CA CA CA CA CA CA CA CA .....
CB CB CB CB CB CB CB CB CB CB CB CB CB CB CB .....
CB CB CB CB CB CB CB CB CB CB CB CB CB CB CB .....
CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC .....
CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC .....
CD CD CD CD CD CD CD CD CD CD CD CD CD CD CD .....
CD CD CD CD CD CD CD CD CD CD CD CD CD CD CD .....
C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 .....
C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 .....
C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 .....
C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 C6 .....
C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 .....
C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 .....
C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 C7 .....

```

```

+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
[**] OVERFLOW-NOOP-X86 [**]
11/01-19:54:45.875729 the.intruder.x.x:59008 -> my.home.net.fw:61570
TCP TTL:44 TOS:0x0 ID:0 DF
*****PA* Seq: 0x96FCA43A Ack: 0x97F3E2C4 Win: 0xF928

```


[illegible]

5. Attack mechanism:

The purpose of this frame is to create a buffer overflow in the program listening to the TCP port 61570 on the my.home.net.fw firewall. Then, once the buffer is overflowed, it should execute a command with the privilege level of root or administrator of the workstation. In that case, it is not very easy to find the program that the hacker want to use for the exploit. In the payload of the first packet, we see in the decode ASCII field that it seems to be referred to some memory anti-virus program. The hex 90's would be interpreted by a intel x86 processor machine language interpreter as a noop which would cause the processor to go to the next instruction until it finds executable code. This is helpful if unsure of the exact location of the stack pointer.

6. Correlation's:

This particular detect has never been seen before and the TCP port 61570 being use for that attack as well.

7. Evidence of active targeting:

2 possible reasons:

- Because the firewall is configured as a packet-filter with ipchains on Linux, it shows all the TCP and UDP port as **filtered**(with nmap) when hackers scan port with a normal SYN pattern. For that particular hacker, tcp-port 61570 most mean something to him and he tried his root-kit exploit program on my firewall.
- Misconfigured program with wrong IP address.

8. Severity:

Severity = (criticality + lethality) – (system + net) = (5+1) – (1+5) = 0

Criticality = 5: The Firewall was the target.

Lethality = 1: No application on tcp-port 61570 is running on the firewall and that port is also block.

System = 1: It is a well configured firewall with the latest Linux OS patch.

Net = 5: It is a well configured firewall with the latest Linux OS patch.

9. Defensive recommendation:

The attack is a false positive. No defensive measures required.

10. Multiple choice test question:

Scanning a specific port with “nmap -sT” on a Linux ipchains firewall blocking the port (DENY) will show port state as ?

- a) closed
- b) filtered
- c) unfiltered
- d) none of the above

Answer is 'b'.

1.2 Detect 2

From Snort Alert:

Date: 17 November 2000

Time: 08:34

```
[**] SNMP public access [**]  
11/17-08:34:15.562528 the.intruder.x.x:1026 -> my.home.net.fw:161  
UDP TTL:31 TOS:0x0 ID:10752
```

Prepared by Wayne Veilleux

```

Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 .....0.0....+.
01 04 01 0B 02 04 03 0A 06 00 05 00 .....

```

1. Source of trace

My home subnet accessing the Internet using a cable-modem.

2. Detect was generated by:

Snort version 1.6.3

3. Probability the source address was spoofed

It was a PC trying to open the udp port 161. The IP address was not spoofed.

4. Description of attack:

SNMP public access – The attacker is trying to see if an snmp daemon is running on the firewall with a misconfigured default community string of “public”.

5. Attack mechanism:

There is a lot of tool out there to check if an snmp daemon is listening on port udp/161. Almost every Linux system come with ucd-snmp-utilities which include a “snmp-get-next” tool called snmpwalk. You can use that tool to “dump” the whole MIBS variable like this if you want:

- `snmpwalk my.home.net.fw public (snmpwalk <hostname> <community-string>)`

Or being more specific on a MIBS tree variables (this one will tell you all the running process on the machine with there pid number):

- `snmpwalk my.home.net.fw public host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunPath`

6. Correlation's:

The **Common Vulnerabilities and Exposures** web page indicates that this type of detect is commun and active:

[CAN-1999-0517](#) An SNMP community name is the default (e.g. public), null, or missing.

7. Evidence of active targeting:

Intruder was targeting the firewall to find if snmpd is running. On the market, a lot of firewall and routers have snmp services running by default (server or daemon) for diagnostic purpose (mostly use for snmp-traps). No logging information from Snort or from the syslog firewall logging show that the intruder did a scan port on the firewall before.

8. Severity:

Severity = (criticality + lethality) – (system + net) = (5+3) – (1+5) = 2

Criticality = 5: The Firewall was the target.

Lethality = 3: snmpd is running on the firewall but only to send snmp-traps to the management console.
Udp port 161 and 162 are block as input on the outside(Internet) interface

System = 1: It is a well configured firewall with the latest Linux OS patch.

Net = 5: It is a well configured firewall with the latest Linux OS patch.

9. Defensive recommendation:

The attack is a false positive. If you run snmp services on a firewall you must well configure the rules to make it un-accessible from the Internet. Also, please, change the *public* default community string with

10. Multiple choice test question:

What is the port that the snmp-trap service use ?

- a) Tcp/162
- b) Udp/162
- c) Tcp/161
- d) Udp/161

Answer is 'b'.

1.3 Detect 3

From Snort Alert:

Date: 26 October 2000

Time: 03:54 and 22:33

[illegible]

1. Source of trace

My home subnet accessing the Internet using a cable-modem.

2. Detect was generated by:

Snort version 1.6.3

3. Probability the source address was spoofed

This is classic information gathering. IP address was most likely not spoofed.

4. Description of attack:

SCAN-SYN FIN – Triggers when a series of TCP packets with both the SYN and FIN flags set have been sent to the same destination port on a number of different hosts. Illegal flag set, SYN-FIN, is looking here for port 9704. A vulnerability exists in the rpc.statd program which use that tcp port and it is part of the nfs-utils packages, distributed with a number of popular Linux distributions. Because of a format string vulnerability when calling the syslog() function a malicious remote user can execute code as root. The rpc.statd server is an RPC server that implements the Network Status and Monitor RPC protocol. It's a component of the Network File System (NFS) architecture. The logging code in rpc.statd uses the syslog() function passing it as the format string user supplied data. A malicious user can construct a format string that injects executable code into the process address space and overwrites a function's return address, thus forcing the program to execute the code. rpc.statd requires root privileges for opening its network socket, but fails to drop these privileges later on. Thus code executed by the malicious user will execute with root privileges. Debian, Red Hat and Connectiva have all released advisories on this matter. Presumably, any Linux distribution which runs the statd process is vulnerable, unless patched for the problem. In our case, the attacker did a scan to know if the system is running

rpc.statd.

5. Attack mechanism:

Illegal flag set, SYN-FIN, looking for port tcp/9704. This detect might come from a port scanning tool or maybe more from a root-kit tool like those you can find on the net:

- statd-toy.c
- rpc-statd-xpl.c
- statdx.c

This intruder is looking for UNIX machines and specially Linux systems, using a SYN-FIN probe to port 9704. If it is a true positive attack, attackers may now try there a buffer-overflow tool to gain root access.

6. Correlation's:

- The CERT/CC Current Activity web page indicates that this type of probe is common and active: **CERT® Advisory [CA-2000-17](#), Input Validation Problem in rpc.statd**
- The **Common Vulnerabilities and Exposures** web page also indicates that this type is common and active:
The MITRE Corporation [CVE-2000-0666](#)

7. Evidence of active targeting:

Intruder was targeting the firewall to find if nfsd or rpc.statd was running.

8. Severity:

Severity = (criticality + lethality) – (system + net) = (5+1) – (1+5) = 0

Criticality = 5: The Firewall was the target.

Lethality = 1: No application on tcp-port 9704 is running on the firewall and that port is also block.

System = 1: It is a well configured firewall with the latest Linux OS patch.

Net = 5: It is a well configured firewall with the latest Linux OS patch.

9. Defensive recommendation:

The attack is a false positive. No defensive measures required.

10. Multiple choice test question:

What is a normal response from a SynFin packet to an IP stack ?

- a) Ack packet
- b) Ack/Fin packet
- c) No packet at all
- d) Fin packet

Answer is 'c'.

1.4 Detect 4

From Snort Alert:

Date: 17 November 2000

Time: 08:34

```
[**] Possible NetSphere access [**]
```

Prepared by Wayne Veilleux

```
615 -> my.home.net.fw:30100
0x2000
+++++
odem.
ost likely not spoofed.
```

1. Source of trace

My home subnet accessing the Internet using a cable-modem.

2. Detect was generated by:

Snort version 1.6.3

3. Probability the source address was spoofed

This is classic information gathering. IP address was most likely not spoofed.

4. Description of attack:

NetSphere is a backdoor that performs the standard backdoor functions, including logging keystrokes, setting up a port redirector, capturing screenshots, and several functions to operate with Mirabilis ICQ. NetSphere works on Windows 95, 98, and Windows NT. NetSphere uses TCP ports 30100 and 30102. To determine if NetSphere is running on a machine, telnet to port 30100. If you connect, NetSphere will send a banner similar to the following:

```
<NetSphere|v1.30|0><Access|1><SysPath|C:\WINDOWS\system><Secure|0><SRes|1024|768  
|24><Dv|a|2|removable disk><Dv|c|1|fixed disk><Dv|d|1|fixed disk><Dv|e|1|fixed  
disk><Dv|f|1|fixed disk><Dv|q|3|CD-ROM drive>
```

If you connect to port 30102, you will see this banner:

220 NetSphere Capture FTP

5. Attack mechanism:

This was an attempt to discover the NetSphere trojan horse program. In our case here, due to the generated time of the 2 packets traces and also because they have the same sequence number, it has to be done by a scanning tool. With a TCP TTL of 109, it might come from a Sun Solaris 2.X workstation.

6. Correlation's:

7. Evidence of active targeting:

Intruder was targeting the firewall to see if Netsphere is running on it. “Unfortunately, it was not the case.

8. Severity:

$$\text{Severity} = (\text{criticality} + \text{lethality}) - (\text{system} + \text{net}) = (5+1) - (1+5) = 0$$

Criticality = 5: The Firewall was the target.

Lethality = 1: No application on tcp-port 9704 is running on the firewall and that port is also block.
System = 1: It is a well configured firewall with the latest Linux OS patch.
Net = 5: It is a well configured firewall with the latest Linux OS patch.

9. Defensive recommendation:

Multiple choice test question:

Which instant messaging system Netsphere usually use to be installed into system ?

- a) AOL
- b) Mirabillis/ICQ
- c) AIM
- d) InternetPhone

Answer is 'b'.

Assignment 2 – Evaluate an Attack – WinGate attempt:

In this assignment I will describe a detect trace targeting a server running WinGate. Wingate is a popular software package that allows a Local Area Network (LAN) to share a single Internet connection. The default configuration for WinGate allows an intruder to use a WinGate server to conceal his or her true location without the need to forge packets. In particular:

- WinGate enables all available network ports or services (this includes FTP, IRC, News,

Prepared by Wayne Veilleux

- WinGate does not log connections.

Because connections are not logged by default, and because WinGate will accept any incoming connections by default, intruders can use WinGate to effectively launder their IP addresses during an internet-based attack.

A victim of an attack using a WinGate server is only able to trace the connection back to the WinGate server. Additionally, a site running a vulnerable WinGate server may be implicated in a security incident when in fact an intruder has used the WinGate server to conceal his or her true location.

Here is some usefull URL links for WinGate that treat those kind of attempt:

- CERT Vulnerability Note VN-98.03: (http://www.cert.org/vul_notes/VN-98.03.WinGate.html)
- IDS-175 WhiteHats: (<http://www.whitehats.com/IDS/175>)
- CVE-1999-0290: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0290>)
- CVE-1999-0291: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0291>)
- CVE-1999-0441: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0441>)
- CVE-1999-0494: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0494>)
- CAN-1999-0657: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0657>)
- CAN-2000-1048: (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1048>)

Here is a trace that I got from my Snort IDS sitting in front of the firewall:

```

[**] MISC-WinGate-1080-Attempt [**]
11/05-16:23:35.373401 the.intruder.x.x:1738 -> my.home.net.fw:1080
TCP TTL:110 TOS:0x0 ID:47697 DF
**S***** Seq: 0x3CB828B Ack: 0x0 Win: 0x10C0
TCP Options => MSS: 536 NOP NOP SackOK
[**] MISC-WinGate-1080-Attempt [**]
11/05-16:23:38.412995 the.intruder.x.x:1738 -> my.home.net.fw:1080
TCP TTL:110 TOS:0x0 ID:11602 DF
**S***** Seq: 0x3CB828B Ack: 0x0 Win: 0x10C0
TCP Options => MSS: 536 NOP NOP SackOK

```

These kind of probes scan are very common. An attacker is usually interested in this service because they can use it to bounce their connections through the server, and make other connections that will then seem to come from the victim IP address. Port 1080 is usually use for SOCKS proxy services. SOCKS is a system that allows multiple machines to share a common Internet connection. Many products support SOCKS. A typical product for home and small business users is WinGate (<http://wingate.deerfield.com/>). WinGate is installed on a single machine that contains the actual Internet connection. All the other machines within the home connect to the Internet through the machine running WinGate.

Usually SOCKS services running on UNIX systems are well configured. But, the way WinGate implement SOCKS is that it isn't picky about the source and destination. Just as it allows internal machines access to the Internet, it possibly will allow Internet machines access the internal home network (oups!). Most importantly, it may allow a hacker access to other Internet machines through your system. This allows the hacker to hide his/her true location. The attacks against the victim appear to come from your machine, not from the real hacker. The ability to hide their tracks like this is important to hackers.

Therefore, hackers scour the Internet religiously looking for systems they can bounce their attacks through.

The version 3.0 (ver 4.1.0 is the current version and I did not found anything about the same kind of vulnerability) of WinGate has three very well-known vulnerabilities:

1. Read any file on the remote system:

The WinGate Log File service in the past has had holes where you can read any file on the system and the holes still seem to be there and some new ways of doing it have cropped up. For examples;

```
http://www.victim:8010/c:/ - NT/Win9x
http://www.victim.com:8010// - NT/Win9x
http://www.victim.com:8010/.../ - Win9x
```

will list all files on the remote machine. By default all WinGate services are set so that only 127.0.0.1 can use the service. However the use for the log file service is to let users remotely view the logs so therefore chances are people using the log file service are not going to be leaving it on 127.0.0.1. Also by default in the WinGate settings "Browse" is enabled.

2. DoS the WinGate service.

The Winsock Redirector Service sits on port 2080. When you connect to it and send 2000 characters and disconnect it will crash all WinGate services. Blue Panda (bluepanda@dwarf.box.sk) has discovered that a variation of the vulnerability exists also in recent versions (ver. 4.1 BetaC and above). Using escaped characters, one can achieve the same effect.

3. Decrypt WinGate passwords.

The registry keys where WinGate stores its passwords are insecure and let everyone read them (as we just saw). Therefore anyone can get the passwords and decrypt them. Here is the source C code to do it (thanks to ChrisA@eEye.com and Mike@eEye.com):

```
#include "stdafx.h"
#include <stdio.h>
#include <string.h>

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

    for(i = 0; i < strlen(argv[1]); i++)
        putchar(argv[1][i]^(char)((i + 1) << 1));
    return 0;
}
```

This intrusion signature above indicates that "the.intruder.x.x" scanned my.home.net.fw looking for SOCKS, but did not find it. I am pretty sure that come from a scan tool because of the time of the frame and also because the SEQ number are identical.

Remote attackers could also perform a denial of service in machines running WinGate using a buffer overflow in the Winsock Redirector Service.

Assignment 3 – "Analyze This" Scenario :

3.1 Introduction

This is a security analysis of the network (MY.NET) at GIAC Enterprise. The network was attack and compromised. Fortunately, the network was monitored with the Snort intrusion detection system (IDS). From time to time, the power has failed at this location, and maybe because the disk was full so we do not have data for all days. But, we do not have any network map of the site and neither configuration of routers. We don't even know if the whole network was protected by a firewall (but after looking at the trace, we are pretty sure that no firewall or any packet-filtering gateways were used to face the Internet. Our task is to analyze the data, and be especially alert for signs of compromised systems or network problems and produce an analysis report. The Snort reports were analyzed to assess the security of the network.

3.2 Analysis:

Network activity was monitored with the Snort IDS (<http://www.snort.org>). Snort is a free IDS used extensively by the network security community. In the data we have snort trace from August 11th to September 14th 2000. There were some gaps in the data collected, but the time periods covered are enough to do a first level assessment of the network activity from a security point of view. Here is the 3 different kind of information we had to analyse:

- **Alert Report (Files with extension SnortA*.txt):**
Those include trace of Snort with "full alert mode" enable. We counted about 68958 detects in those files.
- **Scan Report (Files with extension SnortS*.txt):**
Those have only one line of information per packet. They report all the scan. I counted about 250176 detects in those files.
- **Raw Snort Data (Files with extension SOOS*.txt):**
Those have raw snort trace without the alert header. I counted about 7506 detects in those files.

3.2.1 Suspected Compromises systems with recommendation:

1. Happy 99: Very important to scan a recent anti-virus to those machine; 131.195.179.80 and 131.195.6.35
2. Ftp server running wu-ftpd daemon: Those ftp server were probably compromised; 131.195.150.24, 131.195.202.202, 131.195.202.190 and 131.195.202.202. We suggest to reinstall all those systems.
3. Sun RPC highport: Here is summary of the malicious traffic:

Source IP	Nslookup	Whois	Flow	Destination IP
193.64.205.17	N/A	(SETA1) Sexual Equality Association; PO Box 55, SF-00531 Helsinki, FI	->	131.195.211.2

205.188.153.98	fes-d002.icq.aol.com	N/A	->	131.195.222.66 131.195.220.58 131.195.217.82
205.188.179.33	fes-d021.icq.aol.com	N/A	->	131.195.217.42
205.188.153.115	fes-d019.icq.aol.com	N/A	->	131.195.53.15 131.195.218.218
205.188.153.112	fes-d016.icq.aol.com	N/A	->	131.195.105.2
205.188.153.109	fes-d013.icq.aol.com	N/A	->	131.195.219.26
205.188.153.114	fes-d018.icq.aol.com	N/A	->	131.195.105.2 131.195.206.38
141.213.191.50	westquad-19150.reshall.umich.edu	University of Michigan (NET-UMNET3)	->	131.195.98.160

We most investigate in more deeply those servers, it is probably legitimate traffic or they are maybe compromised.

4. SMB vulnerability: Those server were hardly scan for smb services; 131.195.101.192, 131.195.100.165, and 131.195.6.7. Make sure that are intensively scan by a good and recent anti-virus. And, it is maybe safely to re-install them. They are maybe compromised.
5. SNMP public community string: It seems that all the SNMP alert that we have are from the inside. They are maybe justify traffic but the community strings they use are still the default which is public. We strongly recommend to change it for something more "original". The only server probed was 131.195.98.192 and those stations sent SNMP request; 131.195.98.172, 131.195.98.109, 131.195.97.217, 131.195.97.154, 131.195.97.206, 131.195.97.246, 131.195.98.114, 131.195.98.171, 131.195.98.191, 131.195.98.181, 131.195.98.159, 131.195.98.201, 131.195.98.148, 131.195.98.177 and 131.195.98.190.
6. SynFin Scanner: Here is the two major SynFin scanner:

Source IP	Nslookup	Whois	# of scans
210.61.144.125	N/A	(HINET8-144-TW) Abnet Information Co., Ltd; 6F. No.22-5; Ning Hsia Rd Taipei, Taiwan; TW	4784
213.25.136.60	server.roztozce.com.pl	N/A	663

7. Wingate attempt: Here is a list of possible host compromised by a WinGate attempt. First, check if WinGate is really running on those host. If it is the case, re-install the OS with the last version of WinGate if proxying functionality is still required. A well detailed explanation of WinGate is done in Assignment 2. 2156 host were hit by this attempt. If you want to check more host on that attempt, there is a more detail list farther. Host 168.187.26.157 (Kuwait Ministry of Communications (NET-MOC-KW))

Target IP	# of WinGate detect	# of detect on this host
131.195.60.11	177	363
131.195.60.8	139	195
131.195.100.2	91	91

131.195.60.16	39	39
131.195.222.198	33	34
131.195.98.111	31	32
131.195.98.124	31	32
131.195.97.192	22	22
131.195.98.185	21	23
131.195.98.162	20	20

Attacker (most)	nslookup/whois	# of WinGate attempt
168.187.26.157	N/A	4290
168.120.16.250	irc.au.ac.th	136
208.240.218.220	warpcore.provalue.net	111
208.47.92.164	owb.kellyandwilmore.com	64
204.117.70.5	security.enterthegame.com	61
216.179.0.37	services.gamesnet.net	61
207.126.106.118	mandarin.peopleweb.com	61

8. DNS server: It seems, because they were hardly scanned for udp port 53, that 131.195.1.3, 131.195.1.4 and 131.195.1.5 are DNS server. And they are probably composed, especially 131.195.1.4 and 131.195.1.5, because they also scanned a lot of there own network. So hackers had probably already installed there root-kit on it. We strongly recommend to re-install those 3 servers (OS and applications).

Attacker (most)	nslookup/whois	# of WinGate attempt
168.187.26.157	N/A	4290
168.120.16.250	irc.au.ac.th	136
208.240.218.220	warpcore.provalue.net	111
208.47.92.164	owb.kellyandwilmore.com	64
204.117.70.5	security.enterthegame.com	61
216.179.0.37	services.gamesnet.net	61
207.126.106.118	mandarin.peopleweb.com	61

Telnet and SSH server: A lot of host on network 131.195.208.0 (20) were scanned on tcp port 23 which is telnet. They were only scanned 1 time each by 24.180.134.156 (@Home Network (NETBLK-HOME-2BLK)HOME-2BLK). Also, 1 host (131.195.253.112) was hit 6 times by 151.196.73.119 (Bell Atlantic (NETBLK-BELL-ATLANTIC1)). We strongly suggest to look if those host are compromised:

Target Host IP	TCP Port
131.195.253.112	22
131.195.208.117	23
131.195.208.141	23
131.195.208.149	23
131.195.208.153	23
131.195.208.165	23

131.195.208.166	23
131.195.208.169	23
131.195.208.17	23
131.195.208.177	23
131.195.208.181	23
131.195.208.193	23
131.195.208.201	23
131.195.208.209	23
131.195.208.21	23
131.195.208.213	23
131.195.208.225	23
131.195.208.229	23
131.195.208.233	23
131.195.208.237	23
131.195.208.241	23
131.195.208.245	23
131.195.208.25	23
131.195.208.29	23
131.195.208.33	23
131.195.208.37	23
131.195.208.41	23
131.195.208.5	23
131.195.208.57	23

3.2.2 Malicious Traffic by date

For some circumstances, it is often interesting to see the number of “hits” per day. When we looked at that table, we see that there is a lot of UDP scan with Snort alert between the 15th and 19th of August. There was also a lot of activity between the 2nd and the 11th of September with almost everything (UDP scan, TCP scan and Snort Alerts). Here is a detail table and a total hit per day basis:

Date	# of SnortAlert (SnortA)	# of UDP Scan (SnortS)	# of TCP Scan (SOOS)	Total by day
08/15	3039	43298	0	46337
08/16	3019	26549	0	29568
08/17	3645	1810	0	5455
08/18	3224	1676	0	4900
08/19	3615	0	0	3615
08/20	7145	0	0	7145
08/21	148	0	0	148
08/22	0	0	0	0
08/23	0	0	0	0
08/24	0	0	0	0
08/25	0	0	0	0
08/26	0	0	0	0
08/27	0	0	0	0

08/28	0	1922	16	1938
08/29	0	0	18	18
08/30	0	0	0	0
08/31	0	0	31	31
09/01	0	0	73	73
09/02	2378	24356	25	26759
09/03	1620	9709	35	11364
09/04	0	1278	57	1335
09/05	615	1405	40	2060
09/06	1563	6317	31	7910
09/07	1430	1898	1061	4389
09/08	2018	48396	82	50469
09/09	2106	13150	9	15265
09/10	2234	17443	37	19714
09/11	14750	39691	5902	60343
09/12	8170	0	17	8187
09/13	1315	5553	34	1902
09/14	2236	5724	23	7983

3.2.3 Conclusion and final recommendation:

After looking to all those signature et detect, it is more than absolutely sure that there is no firewall on this network. So, first, a security architecture should be implemented to shield the internal network from external. The rules should be set up to permit only traffic required to support the organization's functions. All incoming traffic should be proxied with an application-level gateway firewall if possible. Once the firewall is in place, the internal network should be extensively scanned for listening host services (with tools like NMAP), particularly on trojan ports, and any suspicious findings noted and investigated. All hosts should have up-to-date anti-virus software installed and active. SMTP mail, along with HTTP and FTP traffic into and out of the network, should be scanned for virus signatures in realtime if possible.

Internal and external NIDS probe should be also installed (like Snort NIDS), along with systems logging facility like syslogd, to record network access and provide data to compare with the NIDS analysis if required.

All internal UNIX hosts should be protected with TCP wrappers or similar products to help protect against future scans and vulnerabilities, especially those hosts which use a portmapper service. All externally visible hosts, including proxy servers such as WinGate, should be hardened and all Operating System and Application security patches applied if possible.

3.2.4 Detect in detail:

With this amount of information we had to start with a summary. I used the tool SnortSnarf (<http://www.silicondefense.com/snortsnarf/>). This tool is a Perl program to take files of alerts from Snort and

produce HTML output intended for diagnostic inspection and tracking down problems. That will help to represent a summary before getting more deeper. Because of the amount of alert, I had to trunc sometime some signature that have no more that 2 alerts.

**Note: For the purpose of using SnortSnarf, I had tp replace the mask MY.NET by the Class B network address 131.195. So when you will see 131.195, it was MY.NET in the files.
I would also like to thanks the authors of SnortSnarf Jim Hoagland and Stuart Staniford at Silicon Defense. Without it I would still working on it.*

3.2.4.1 Summary of the possible exploit from the Snort Alerts:

40225 alerts found among the files:
Earliest alert at **00:33:44.374672** on 08/11
Latest alert at **23:21:39.338983** on 09/14

Signature	# Alerts	# Sources	# Destinations
<u>Happy 99 Virus</u>	2	2	2
<u>Possible wu-ftpd exploit - GIAC000623</u>	2	1	2
<u>site exec - Possible wu-ftpd exploit – GIAC000623</u>	6	1	4
<u>TCP SMTP Source Port traffic</u>	8	2	2
<u>Tiny Fragments – Possible Hostile Activity</u>	12	5	8
<u>External RPC call</u>	40	6	3
<u>Queso fingerprint</u>	54	11	23
<u>Probable NMAP fingerprint attempt</u>	64	7	28
<u>SUNRPC highport access!</u>	64	5	3
<u>NMAP TCP ping!</u>	138	10	42
<u>Null scan!</u>	181	63	73
<u>SMB Name Wildcard</u>	338	17	15
<u>SNMP public access</u>	922	16	1
<u>Attempted Sun RPC high port access</u>	1990	8	11
<u>Watchlist 000220 IL-ISDNNET-990517</u>	5276	19	21
<u>SYN-FIN scan!</u>	5457	6	3005
<u>WinGate 1080 Attempt</u>	6193	347	2156
<u>Watchlist 000222 NET-NCFC</u>	19478	45	19

3.2.4.2 Happy 99 Virus summary:

2 alerts with this signature among the files:
Earliest such alert at **14:36:46.954418** on 08/16
Latest such alert at **15:41:12.157972** on 08/20

Happy 99 Virus 2 sources 2 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>24.2.2.66</u>	1	1	1	1
<u>128.8.198.101</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.179.80	1	1	1	1
131.195.6.35	1	12	1	3

- CERT Incident Note IN-99-02: (http://www.cert.org/incident_notes/IN-99-02.html)

This is a very compromised attack. Once Happy99 is installed, every email and Usenet posting sent by an affected user triggers Happy99 to send a followup message containing Happy99.exe as a uuencoded attachment. Happy99 keeps track of who received the Trojan horse message in a file called LISTE.SKA in the system folder. Note that messages containing the Trojan horse will generally appear to come from someone you know.

3.2.4.3 Possible wu-ftpd exploit and site exec - GIAC000623:

2 alerts with this signature among the files:

Earliest such alert at **05:25:41.167678** on 09/08

Latest such alert at **05:59:04.191384** on 09/08

Possible wu-ftpd exploit - [1 sources](#) [2 destinations](#)
GIAC000623

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.17.189.83	2	8	2	4

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.150.24	1	2	1	1
131.195.202.202	1	3	1	1

3.2.4.4 site exec - Possible wu-ftpd exploit - GIAC000623:

6 alerts with this signature among the files:

Earliest such alert at **04:53:17.038845** on 09/08

Latest such alert at **05:59:04.271433** on 09/08

site exec - Possible wu-ftpd exploit - [1 sources](#) [4 destinations](#)
GIAC000623

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.17.189.83	6	8	4	4

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.202.190	2	2	1	1
131.195.202.202	2	3	1	1
131.195.99.104	1	1	1	1
131.195.150.24	1	2	1	1

- CERT® Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTPD:
(<http://www.cert.org/advisories/CA-1999-13.html>)
- CERT® Advisory CA-2000-13 Two Input Validation Problems In FTPD:
(<http://www.cert.org/advisories/CA-2000-13.html>)
- CVE-1999-0075 : PASV core dump in wu-ftpd daemon when attacker uses a QUOTE PASV command after specifying a username and password.
- CVE-1999-0080 : wu-ftp FTP server allows root access via "site exec" command.
- CVE-1999-0081 : wu-ftp allows files to be overwritten via the rnfr command.
- CVE-1999-0368 : Buffer overflows in wuarchive ftpd (wu-ftpd) and ProFTPD lead to remote root access, a.k.a. palmetto.
- CVE-1999-0720 : The pt_chown command in Linux allows local users to modify TTY terminal devices that belong to other users.
- CVE-1999-0878 : Buffer overflow in WU-FTPD and related FTP servers allows remote attackers to gain root privileges via MAPPING_CHDIR.
- CVE-1999-0879 : Buffer overflow in WU-FTPD and related FTP servers allows remote attackers to gain root privileges via macro variables in a message file.
- CVE-1999-0880 : Denial of service in WU-FTPD via the SITE NEWER command, which does not free memory properly.
- CVE-1999-0955 : Race condition in wu-ftpd and BSDI ftpd allows remote attackers gain root access via the SITE EXEC command.
- CVE-1999-0997 : wu-ftp with FTP conversion enabled allows an attacker to execute commands via a malformed file name that is interpreted as an argument to the program that does the conversion, e.g. tar or uncompress.
- CAN-1999-0076 : ** CANDIDATE (under review) ** Buffer overflow in wu-ftp from PASV command causes a core dump.
- CAN-1999-0156 : ** CANDIDATE (under review) ** wu-ftpd FTP daemon allows any user and password combination.
- CAN-1999-0661 : ** CANDIDATE (under review) ** A system is running a version of software that was replaced with a Trojan Horse at its distribution point, e.g. TCP Wrappers, wuftp, etc.
- CAN-1999-0911 : ** CANDIDATE (under review) ** Buffer overflow in ProFTPD, wu-ftpd, and beroftpd allows remote attackers to gain root access via a series of MKD and CWD commands that create nested directories.
- CAN-2000-0573 : ** CANDIDATE (under review) ** The lreply function in wu-ftpd 2.6.0 and earlier does not properly cleanse an untrusted format string, which allows remote attackers to execute arbitrary commands via the SITE EXEC command.

3.2.4.5 TCP SMTP Source Port traffic:

8 alerts with this signature among the files:

Earliest such alert at 00:06:16.011962 on 08/17

Latest such alert at 16:24:01.024055 on 09/10

TCP SMTP Source Port traffic 2 sources 2 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>206.46.170.21</u>	5	5	1	1
<u>156.40.66.2</u>	3	3	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
<u>131.195.97.181</u>	5	6	1	2
<u>131.195.253.53</u>	3	11	1	4

3.2.4.6 Tiny Fragments - Possible Hostile Activity:

12 alerts with this signature among the files:

Earliest such alert at 04:11:08.040731 on 08/19

Latest such alert at 19:15:29.350830 on 09/14

Tiny Fragments - Possible Hostile Activity 5 sources 8 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>24.68.58.96</u>	5	5	2	2
<u>62.76.42.18</u>	3	3	3	3
<u>213.132.131.201</u>	2	2	1	1
<u>212.160.15.85</u>	1	1	1	1
<u>62.76.42.17</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
<u>131.195.217.82</u>	4	178	1	2
<u>131.195.203.62</u>	2	2	1	1
<u>131.195.210.242</u>	1	1	1	1
<u>131.195.160.109</u>	1	1	1	1
<u>131.195.1.8</u>	1	39	1	5
<u>131.195.1.9</u>	1	5	1	3
<u>131.195.1.10</u>	1	7	1	3
<u>131.195.212.86</u>	1	3	1	2

3.2.4.7 External RPC call:

40 alerts with this signature among the files:

Earliest such alert at **06:10:13.484691** on 08/18

Latest such alert at **03:15:34.249462** on 09/10

External RPC call [6 sources](#) [3 destinations](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
18.116.0.75	11	14	1	3
209.160.238.215	10	10	3	3
141.223.124.31	10	10	2	2
161.31.208.237	5	5	1	1
210.100.199.219	3	3	2	2
210.101.101.110	1	3	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
131.195.6.15	35	45	6	9
131.195.100.130	4	10	3	6
131.195.15.127	1	4	1	3

3.2.4.8 Queso(Unix scan tool) fingerprint:

54 alerts with this signature among the files:

Earliest such alert at **15:30:15.258499** on 08/15

Latest such alert at **10:22:54.817324** on 09/14

Queso fingerprint [11 sources](#) [23 destinations](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
64.80.63.121	20	20	9	9
216.15.191.130	17	17	5	5
24.3.161.193	7	7	1	1
130.149.41.70	2	42	1	1
128.61.105.106	2	3	1	1
147.126.59.89	1	1	1	1
24.24.137.232	1	1	1	1
213.228.1.13	1	1	1	1
129.2.146.48	1	1	1	1
24.19.244.80	1	1	1	1
216.123.63.13	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
131.195.6.35	9	12	1	3
131.195.145.9	7	7	1	1

131.195.201.86	6	6	1	1
131.195.253.43	4	5419	1	20
131.195.217.46	2	86	1	9
131.195.218.202	2	5	1	2
131.195.209.130	2	2	1	1
131.195.223.42	2	4	1	3
131.195.210.194	2	2	1	1
131.195.204.214	2	2	1	1
131.195.6.34	2	8	1	4
131.195.224.34	2	4	1	3
131.195.208.26	2	2	1	1
131.195.201.146	1	1	1	1
131.195.253.24	1	2	1	2
131.195.219.0	1	1	1	1
131.195.253.41	1	4287	1	21
131.195.219.194	1	1	1	1
131.195.253.42	1	4416	1	23
131.195.162.200	1	1	1	1
131.195.217.26	1	3	1	2
131.195.217.182	1	1	1	1
131.195.75.106	1	1	1	1

3.2.4.9 Probable NMAP(Unix scan tool) fingerprint attempt:

64 alerts with this signature among the files:

Earliest such alert at **10:23:16.502216** on 08/15

Latest such alert at **05:18:51.570991** on 09/11

Probable NMAP fingerprint attempt 7 sources 28 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.180.134.156	46	206	23	51
130.149.41.70	11	42	1	1
151.196.73.119	2	9	1	1
207.151.147.201	2	11	1	1
24.23.198.174	1	32	1	1
216.181.188.154	1	1	1	1
63.226.208.41	1	3	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
131.195.217.46	12	86	2	9
131.195.208.117	2	4	1	1
131.195.253.112	2	17	1	3
131.195.208.241	2	8	1	1

<u>131.195.208.225</u>	2	8	1	1
<u>131.195.208.226</u>	2	13	1	2
<u>131.195.208.153</u>	2	6	1	1
<u>131.195.208.237</u>	2	8	1	1
<u>131.195.208.190</u>	2	3	1	2
<u>131.195.208.193</u>	2	6	1	1
<u>131.195.208.177</u>	2	2	1	1
<u>131.195.208.169</u>	2	6	1	1
<u>131.195.60.8</u>	2	195	1	43
<u>131.195.208.21</u>	2	6	1	1
<u>131.195.208.25</u>	2	8	1	1
<u>131.195.208.33</u>	2	6	1	1
<u>131.195.208.41</u>	2	8	1	1
<u>131.195.208.17</u>	2	4	1	1
<u>131.195.208.5</u>	2	6	1	1
<u>131.195.208.37</u>	2	4	1	1
<u>131.195.208.29</u>	2	2	1	1
<u>131.195.208.213</u>	2	6	1	1
<u>131.195.208.201</u>	2	6	1	1
<u>131.195.208.57</u>	2	4	1	1
<u>131.195.208.74</u>	2	2	1	1
<u>131.195.208.114</u>	2	8	1	2
<u>131.195.253.41</u>	1	4287	1	21
<u>131.195.6.44</u>	1	1	1	1

3.2.4.10 SUNRPC highport access:

64 alerts with this signature among the files:

Earliest such alert at **09:39:11.608534** on 09/02

Latest such alert at **21:24:53.037663** on 09/11

SUNRPC highport access! 5 sources 3 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>193.64.205.17</u>	57	57	1	1
<u>212.204.196.241</u>	3	3	1	1
<u>209.10.41.242</u>	2	2	1	1
<u>207.29.195.22</u>	1	1	1	1
<u>205.188.4.42</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
<u>131.195.211.2</u>	60	60	3	3
<u>131.195.6.15</u>	3	45	1	9
<u>131.195.210.2</u>	1	1	1	1

3.2.4.11 NMAP TCP ping:

138 alerts with this signature among the files:

Earliest such alert at **12:57:26.064901** on 08/11

Latest such alert at **22:36:20.070878** on 09/12

NMAP TCP ping! [10 sources](#) [42 destinations](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.180.134.156	78	206	31	51
205.128.11.157	35	35	3	3
209.218.228.201	6	6	1	1
151.196.73.119	5	9	1	1
207.151.147.201	5	11	1	1
202.187.24.3	4	4	3	3
192.55.91.36	2	2	2	2
213.8.52.189	1	1	1	1
63.226.208.41	1	3	1	1
2.2.2.2	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.1.8	35	39	2	5
131.195.208.226	6	13	1	2
131.195.253.112	5	17	1	3
131.195.60.8	5	195	1	43
131.195.208.2	4	4	1	1
131.195.208.41	4	8	1	1
131.195.208.5	4	6	1	1
131.195.208.65	4	6	1	1
131.195.208.237	4	8	1	1
131.195.60.14	4	4	3	3
131.195.1.10	4	7	1	3
131.195.208.25	4	8	1	1
131.195.208.205	2	2	1	1
131.195.208.206	2	3	1	2
131.195.208.117	2	4	1	1
131.195.208.77	2	2	1	1
131.195.208.201	2	6	1	1
131.195.208.73	2	2	1	1
131.195.208.241	2	8	1	1
131.195.208.225	2	8	1	1
131.195.208.153	2	6	1	1
131.195.208.138	2	2	1	1
131.195.1.9	2	5	1	3
131.195.208.157	2	2	1	1

<u>131.195.208.114</u>	2	8	1	2
<u>131.195.208.213</u>	2	6	1	1
<u>131.195.208.1</u>	2	4	1	1
<u>131.195.208.193</u>	2	6	1	1
<u>131.195.208.214</u>	2	4	1	1
<u>131.195.208.230</u>	2	4	1	1
<u>131.195.208.145</u>	2	2	1	1
<u>131.195.208.161</u>	2	6	1	2
<u>131.195.208.182</u>	2	2	1	1
<u>131.195.208.169</u>	2	6	1	1
<u>131.195.208.45</u>	2	4	1	1
<u>131.195.208.33</u>	2	6	1	1
<u>131.195.208.17</u>	2	4	1	1
<u>131.195.179.77</u>	1	1	1	1
<u>131.195.1.3</u>	1	3	1	2
<u>131.195.5.111</u>	1	7	1	3
<u>131.195.5.29</u>	1	502	1	6
<u>131.195.253.41</u>	1	4287	1	21

3.2.4.12 Null scan:

181 alerts with this signature among the files:
Earliest such alert at **20:18:48.417718** on 08/11
Latest such alert at **16:18:53.799118** on 09/14

Null scan! 63 sources 73 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
<u>24.180.134.156</u>	38	206	19	51
<u>24.23.198.174</u>	31	32	1	1
<u>130.149.41.70</u>	25	42	1	1
<u>216.161.190.169</u>	8	8	1	1
<u>24.180.196.93</u>	4	4	1	1
<u>128.153.151.115</u>	4	4	1	1
<u>207.230.248.254</u>	4	4	1	1
<u>207.151.147.201</u>	3	11	1	1
<u>150.216.127.179</u>	2	2	1	1
<u>24.113.80.28</u>	2	2	1	1
<u>194.94.18.43</u>	2	2	1	1
<u>151.196.73.119</u>	2	9	1	1
<u>128.138.14.148</u>	2	2	1	1
<u>213.6.43.74</u>	2	2	1	1
<u>24.164.181.31</u>	2	2	1	1
<u>24.6.140.249</u>	2	2	1	1
<u>24.92.174.232</u>	2	2	1	1
<u>153.19.25.156</u>	1	1	1	1
<u>200.52.201.4</u>	1	1	1	1

<u>213.56.48.243</u>	1	1	1	1
<u>129.59.24.21</u>	1	1	1	1
<u>63.144.227.21</u>	1	1	1	1
<u>24.115.96.111</u>	1	1	1	1
<u>132.199.220.223</u>	1	1	1	1
<u>128.194.51.187</u>	1	1	1	1
<u>24.200.201.223</u>	1	1	1	1
<u>62.2.64.86</u>	1	1	1	1
<u>216.63.200.250</u>	1	1	1	1
<u>24.160.189.151</u>	1	1	1	1
<u>141.40.205.133</u>	1	1	1	1
<u>200.145.151.163</u>	1	1	1	1
<u>24.92.188.4</u>	1	1	1	1
<u>194.237.99.150</u>	1	1	1	1
<u>139.91.171.50</u>	1	1	1	1
<u>216.123.60.71</u>	1	1	1	1
<u>130.239.142.167</u>	1	1	1	1
<u>24.72.23.136</u>	1	1	1	1
<u>24.91.58.197</u>	1	1	1	1
<u>131.155.192.220</u>	1	1	1	1
<u>212.33.70.83</u>	1	1	1	1
<u>62.10.136.40</u>	1	1	1	1
<u>24.22.125.94</u>	1	1	1	1
<u>24.8.241.127</u>	1	1	1	1
<u>24.72.8.78</u>	1	1	1	1
<u>128.61.105.106</u>	1	3	1	1
<u>137.82.136.39</u>	1	1	1	1
<u>24.232.79.188</u>	1	1	1	1
<u>24.13.104.131</u>	1	1	1	1
<u>193.251.71.243</u>	1	1	1	1
<u>24.28.33.193</u>	1	1	1	1
<u>63.226.208.41</u>	1	3	1	1
<u>130.49.220.26</u>	1	1	1	1
<u>24.29.7.199</u>	1	1	1	1
<u>130.239.11.230</u>	1	1	1	1
<u>211.111.108.136</u>	1	1	1	1
<u>195.132.204.48</u>	1	1	1	1
<u>24.19.101.91</u>	1	1	1	1
<u>128.226.152.34</u>	1	1	1	1
<u>24.112.241.246</u>	1	1	1	1
<u>24.201.116.208</u>	1	1	1	1
<u>129.93.214.47</u>	1	1	1	1
<u>195.150.132.211</u>	1	1	1	1
<u>128.61.59.79</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
<u>131.195.217.46</u>	56	86	2	9
<u>131.195.226.54</u>	8	12	1	4

<u>131.195.217.250</u>	4	4	1	1
<u>131.195.208.18</u>	4	4	1	1
<u>131.195.205.50</u>	4	4	1	1
<u>131.195.208.114</u>	4	8	2	2
<u>131.195.60.8</u>	3	195	1	43
<u>131.195.253.112</u>	3	17	2	3
<u>131.195.206.66</u>	3	3	2	2
<u>131.195.208.193</u>	2	6	1	1
<u>131.195.208.241</u>	2	8	1	1
<u>131.195.208.21</u>	2	6	1	1
<u>131.195.208.25</u>	2	8	1	1
<u>131.195.217.26</u>	2	3	1	2
<u>131.195.208.65</u>	2	6	1	1
<u>131.195.203.110</u>	2	5	1	3
<u>131.195.208.41</u>	2	8	1	1
<u>131.195.208.161</u>	2	6	1	2
<u>131.195.208.169</u>	2	6	1	1
<u>131.195.208.49</u>	2	4	1	1
<u>131.195.217.130</u>	2	2	1	1
<u>131.195.224.34</u>	2	4	2	3
<u>131.195.208.217</u>	2	4	1	1
<u>131.195.208.37</u>	2	4	1	1
<u>131.195.208.146</u>	2	4	1	2
<u>131.195.179.52</u>	2	2	1	1
<u>131.195.208.201</u>	2	6	1	1
<u>131.195.130.190</u>	2	5	1	3
<u>131.195.220.42</u>	2	3	1	2
<u>131.195.213.58</u>	2	2	2	2
<u>131.195.223.38</u>	2	2	2	2
<u>131.195.208.13</u>	2	2	1	1
<u>131.195.206.114</u>	2	2	2	2
<u>131.195.208.57</u>	2	4	1	1
<u>131.195.208.225</u>	2	8	1	1
<u>131.195.208.153</u>	2	6	1	1
<u>131.195.208.226</u>	2	13	1	2
<u>131.195.222.198</u>	1	34	1	8
<u>131.195.146.68</u>	1	1	1	1
<u>131.195.218.94</u>	1	1	1	1
<u>131.195.205.26</u>	1	4	1	3
<u>131.195.222.46</u>	1	2	1	2
<u>131.195.5.7</u>	1	5	1	2
<u>131.195.70.217</u>	1	1	1	1
<u>131.195.253.41</u>	1	4287	1	21
<u>131.195.223.186</u>	1	1	1	1
<u>131.195.220.206</u>	1	1	1	1
<u>131.195.221.114</u>	1	1	1	1
<u>131.195.202.158</u>	1	2	1	2
<u>131.195.181.173</u>	1	1	1	1
<u>131.195.201.58</u>	1	1	1	1
<u>131.195.224.134</u>	1	1	1	1

<u>131.195.162.183</u>	1	1	1	1
<u>131.195.217.222</u>	1	2	1	2
<u>131.195.209.210</u>	1	2	1	2
<u>131.195.218.202</u>	1	5	1	2
<u>131.195.202.134</u>	1	1	1	1
<u>131.195.97.150</u>	1	5	1	3
<u>131.195.204.126</u>	1	1	1	1
<u>131.195.211.234</u>	1	1	1	1
<u>131.195.106.164</u>	1	1	1	1
<u>131.195.220.154</u>	1	1	1	1
<u>131.195.208.190</u>	1	3	1	2
<u>131.195.212.134</u>	1	1	1	1
<u>131.195.201.198</u>	1	1	1	1
<u>131.195.218.10</u>	1	1	1	1
<u>131.195.223.58</u>	1	1	1	1
<u>131.195.217.34</u>	1	3	1	2
<u>131.195.203.106</u>	1	1	1	1
<u>131.195.221.230</u>	1	1	1	1
<u>131.195.210.114</u>	1	3	1	2
<u>131.195.226.6</u>	1	1	1	1
<u>131.195.223.42</u>	1	4	1	3

3.2.4.13 SMB Name Wildcard (scan for smb services; MS or Samba):

338 alerts with this signature among the files:
 Earliest such alert at **16:13:19.788046** on 08/11
 Latest such alert at **19:29:55.728337** on 09/13

SMB Name Wildcard 17 sources 15 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>131.195.101.160</u>	280	280	1	1
<u>166.72.86.217</u>	19	19	2	2
<u>131.118.254.222</u>	6	6	1	1
<u>207.79.66.3</u>	6	6	1	1
<u>168.143.29.9</u>	6	6	1	1
<u>129.37.161.200</u>	4	4	1	1
<u>162.33.184.239</u>	3	3	1	1
<u>206.171.108.1</u>	2	2	1	1
<u>62.136.168.18</u>	2	2	1	1
<u>4.17.88.66</u>	2	2	1	1
<u>209.150.98.231</u>	2	2	1	1
<u>64.7.58.194</u>	1	1	1	1
<u>129.37.160.81</u>	1	1	1	1
<u>205.229.90.194</u>	1	1	1	1
<u>24.28.62.226</u>	1	1	1	1
<u>168.167.8.12</u>	1	1	1	1

216.164.133.254	1	1	1	1
-----------------	---	---	---	---

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.101.192	280	1202	1	17
131.195.100.165	12	37	1	2
131.195.6.7	8	2577	2	13
131.195.100.230	7	535	1	14
131.195.60.17	6	14	1	8
131.195.253.53	6	11	1	4
131.195.100.130	5	10	2	6
131.195.70.121	3	3	2	2
131.195.60.11	3	363	1	47
131.195.6.15	2	45	1	9
131.195.130.91	2	2	1	1
131.195.20.10	1	3	1	2
131.195.181.37	1	1	1	1
131.195.253.24	1	2	1	2
131.195.60.8	1	195	1	43

3.2.4.14 SNMP public access:

922 alerts with this signature among the files:

Earliest such alert at **19:59:52.855020** on 08/15

Latest such alert at **19:35:04.125023** on 09/13

SNMP public access 16 sources 1 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
131.195.98.172	226	226	1	1
131.195.98.109	208	208	1	1
131.195.97.217	194	194	1	1
131.195.97.154	53	53	1	1
131.195.98.114	52	52	1	1
131.195.98.171	33	33	1	1
131.195.98.191	31	31	1	1
131.195.98.181	26	26	1	1
131.195.97.244	23	23	1	1
131.195.98.159	21	21	1	1
131.195.98.201	19	19	1	1
131.195.98.148	16	16	1	1
131.195.97.246	6	6	1	1
131.195.97.206	5	5	1	1
131.195.98.177	5	5	1	1
131.195.98.190	4	4	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
131.195.101.192	922	1202	16	17

3.2.4.15 Attempted Sun RPC High port access:

1990 alerts with this signature among the files:

Earliest such alert at **04:17:41.894013** on 08/15

Latest such alert at **19:14:42.174099** on 09/12

Attempted Sun RPC high port access [8 sources](#) [11 destinations](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
205.188.179.33	1054	1054	1	1
205.188.153.98	410	410	3	3
205.188.153.115	252	252	2	2
205.188.153.109	222	222	1	1
205.188.153.112	40	40	1	1
205.188.153.114	8	8	2	2
141.213.191.50	3	3	1	1
128.211.224.100	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
131.195.217.42	1054	1054	1	1
131.195.218.218	240	240	1	1
131.195.219.26	222	222	1	1
131.195.222.66	184	185	1	2
131.195.217.82	174	178	1	2
131.195.220.58	52	52	1	1
131.195.105.2	45	45	2	2
131.195.53.15	12	14	1	2
131.195.98.160	3	3	1	1
131.195.206.38	3	3	1	1
131.195.98.111	1	32	1	5

3.2.4.16 Watchlist 000220 IL-ISDNNET-990517:

5276 alerts with this signature among the files:

Earliest such alert at **11:35:46.194548** on 08/11

Latest such alert at **22:43:47.936898** on 09/14

Watchlist 000220 IL-ISDNNET-990517 [19 sources](#) [21 destinations](#)

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>212.179.58.174</u>	1615	1615	1	1
<u>212.179.66.2</u>	1144	1144	2	2
<u>212.179.29.150</u>	542	542	1	1
<u>212.179.127.45</u>	460	460	1	1
<u>212.179.27.111</u>	345	345	1	1
<u>212.179.58.2</u>	271	271	1	1
<u>212.179.61.244</u>	254	254	1	1
<u>212.179.61.252</u>	168	168	1	1
<u>212.179.61.5</u>	145	145	2	2
<u>212.179.47.30</u>	139	139	1	1
<u>212.179.61.247</u>	71	71	1	1
<u>212.179.7.36</u>	46	46	3	3
<u>212.179.32.2</u>	30	30	2	2
<u>212.179.58.4</u>	20	20	2	2
<u>212.179.67.195</u>	11	11	1	1
<u>212.179.27.6</u>	8	8	1	1
<u>212.179.62.74</u>	3	3	1	1
<u>212.179.44.62</u>	3	3	1	1
<u>212.179.58.204</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
<u>131.195.157.200</u>	1615	1615	1	1
<u>131.195.221.94</u>	612	612	1	1
<u>131.195.53.28</u>	542	542	1	1
<u>131.195.181.87</u>	532	532	1	1
<u>131.195.5.29</u>	493	502	3	6
<u>131.195.202.58</u>	460	460	1	1
<u>131.195.206.154</u>	345	345	1	1
<u>131.195.98.168</u>	271	281	1	7
<u>131.195.204.150</u>	144	146	1	3
<u>131.195.223.62</u>	139	139	1	1
<u>131.195.253.43</u>	28	5419	1	20
<u>131.195.253.41</u>	27	4287	2	21
<u>131.195.98.164</u>	27	35	1	3
<u>131.195.253.42</u>	11	4416	2	23
<u>131.195.208.178</u>	11	11	1	1
<u>131.195.253.105</u>	8	8	1	1
<u>131.195.15.41</u>	3	3	1	1
<u>131.195.224.78</u>	3	3	1	1
<u>131.195.10.77</u>	3	3	1	1
<u>131.195.205.254</u>	1	3	1	3
<u>131.195.220.42</u>	1	3	1	2

3.2.4.17 SynFin scan:

5457 alerts with this signature among the files:

Earliest such alert at **09:39:01.814788** on 08/17

Latest such alert at **07:06:48.842343** on 09/11

SYN-FIN scan! 6 sources 3005 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
<u>210.61.144.125</u>	4784	4784	2392	2392
<u>213.25.136.60</u>	663	663	663	663
<u>130.149.41.70</u>	4	42	1	1
<u>18.116.0.75</u>	3	14	3	3
<u>210.101.101.110</u>	2	3	1	1
<u>24.201.209.192</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
<u>131.195.217.46</u>	4	86	1	9
<u>131.195.2.45</u>	3	3	2	2
<u>131.195.18.90</u>	3	3	2	2
<u>131.195.2.37</u>	3	3	2	2
<u>131.195.5.184</u>	3	3	2	2
<u>131.195.25.248</u>	3	5	2	3
<u>131.195.18.115</u>	3	3	2	2
<u>131.195.68.206</u>	3	3	2	2
<u>131.195.1.32</u>	3	3	2	2
<u>131.195.6.186</u>	3	5	2	3
<u>131.195.7.57</u>	3	7	2	3
<u>131.195.25.25</u>	3	3	2	2
<u>131.195.25.23</u>	3	5	2	3
<u>131.195.75.230</u>	3	3	2	2
<u>131.195.21.55</u>	3	3	2	2
<u>131.195.15.5</u>	3	5	2	3
<u>131.195.5.15</u>	3	7	2	3
<u>131.195.6.252</u>	3	3	2	2
<u>131.195.7.7</u>	3	3	2	2
<u>131.195.85.227</u>	3	3	2	2
<u>131.195.85.163</u>	3	3	2	2
<u>131.195.75.16</u>	3	3	2	2
<u>131.195.2.235</u>	3	5	2	3
<u>131.195.70.55</u>	3	3	2	2
<u>131.195.12.94</u>	3	3	2	2
<u>131.195.9.27</u>	3	3	2	2
<u>131.195.6.111</u>	3	3	2	2
<u>131.195.85.229</u>	3	3	2	2
<u>131.195.68.138</u>	3	3	2	2

<u>131.195.13.60</u>	3	5	2	3
<u>131.195.6.155</u>	3	3	2	2
<u>131.195.6.15</u>	3	45	2	9
<u>131.195.26.201</u>	3	3	2	2
<u>131.195.17.103</u>	3	3	2	2
<u>131.195.69.111</u>	3	3	2	2
<u>131.195.4.130</u>	3	3	2	2
<u>131.195.1.106</u>	3	3	2	2
<u>131.195.4.11</u>	3	5	2	3
<u>131.195.15.233</u>	3	5	2	3
<u>131.195.11.18</u>	3	3	2	2
<u>131.195.17.63</u>	3	3	2	2
<u>131.195.9.81</u>	3	3	2	2
<u>131.195.53.64</u>	3	5	2	3
<u>131.195.2.163</u>	3	5	2	3
<u>131.195.7.75</u>	3	5	2	3
<u>131.195.11.3</u>	3	5	2	3
<u>131.195.18.20</u>	3	3	2	2
<u>131.195.10.57</u>	3	3	2	2
<u>131.195.4.224</u>	3	3	2	2
<u>131.195.71.171</u>	3	3	2	2
<u>131.195.7.147</u>	3	3	2	2
<u>131.195.9.113</u>	3	5	2	3
<u>131.195.1.239</u>	3	3	2	2
<u>131.195.12.103</u>	3	3	2	2
<u>131.195.68.74</u>	3	3	2	2
<u>131.195.2.218</u>	3	3	2	2
<u>131.195.20.66</u>	3	5	2	3

..... <<< TRUNCATED >>>

3.2.4.18 WinGate 1080 Attempt:

6193 alerts with this signature among the files:

Earliest such alert at **00:46:56.976538** on 08/11

Latest such alert at **23:21:39.338983** on 09/14

WinGate 1080 Attempt 347 sources 2156 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>168.187.26.157</u>	4290	4290	1755	1755
<u>168.120.16.250</u>	136	136	23	23
<u>208.240.218.220</u>	111	111	64	64
<u>208.47.92.164</u>	64	64	23	23
<u>204.117.70.5</u>	61	61	11	11
<u>216.179.0.37</u>	61	61	25	25
<u>207.126.106.118</u>	61	61	22	22

<u>207.114.4.46</u>	59	59	50	50
<u>208.194.161.50</u>	45	45	30	30
<u>24.180.134.156</u>	44	206	22	51
<u>151.17.144.213</u>	44	44	1	1
<u>64.86.5.250</u>	35	35	18	18
<u>194.75.152.237</u>	31	31	25	25
<u>207.175.201.164</u>	25	25	5	5
<u>151.17.144.96</u>	24	24	1	1
<u>207.175.201.141</u>	23	23	4	4
<u>212.72.75.236</u>	22	22	17	17
<u>166.62.4.48</u>	22	22	6	6
<u>194.87.13.86</u>	21	21	10	10
<u>204.137.237.1</u>	21	21	9	9
<u>209.10.77.201</u>	20	20	6	6
<u>209.10.218.250</u>	18	18	3	3
<u>151.17.144.216</u>	18	18	1	1
<u>216.67.82.151</u>	18	18	4	4
<u>24.113.168.58</u>	17	17	11	11
<u>207.175.201.165</u>	17	17	2	2
<u>62.158.0.201</u>	17	17	4	4
<u>64.86.6.250</u>	16	16	11	11
<u>216.176.130.250</u>	14	14	13	13
<u>168.120.16.155</u>	13	13	3	3
<u>216.67.50.108</u>	13	13	2	2
<u>207.175.201.168</u>	13	13	2	2
<u>62.158.0.215</u>	12	12	2	2
<u>216.67.50.180</u>	11	11	2	2
<u>195.139.15.242</u>	11	11	10	10
<u>209.246.213.5</u>	10	10	2	2
<u>207.175.201.144</u>	10	10	4	4
<u>212.25.67.88</u>	10	10	7	7
<u>207.175.201.171</u>	9	9	1	1
<u>63.168.242.5</u>	9	9	2	2
<u>207.175.201.128</u>	9	9	3	3
<u>199.182.91.232</u>	9	9	1	1
<u>207.25.80.133</u>	8	8	2	2
<u>216.67.50.77</u>	7	7	2	2
<u>194.84.208.118</u>	7	7	7	7
<u>62.156.39.124</u>	7	7	3	3
<u>129.242.219.27</u>	7	7	5	5
<u>194.204.236.62</u>	7	7	1	1
<u>192.216.128.28</u>	7	7	5	5
<u>206.50.68.20</u>	7	7	6	6
<u>64.252.66.8</u>	7	7	4	4
<u>63.103.51.242</u>	7	7	1	1
<u>24.115.76.63</u>	6	6	4	4
<u>207.175.201.174</u>	6	6	2	2
<u>168.120.12.113</u>	6	6	1	1
<u>216.67.50.247</u>	6	6	1	1
<u>200.48.9.37</u>	5	5	1	1

<u>161.58.8.77</u>	5	5	3	3
<u>24.129.69.120</u>	5	5	1	1
<u>151.17.144.109</u>	5	5	1	1
<u>166.62.216.254</u>	5	5	2	2
<u>209.92.13.74</u>	5	5	1	1
<u>207.175.201.192</u>	5	5	1	1
<u>207.175.201.215</u>	5	5	3	3
<u>63.238.214.65</u>	5	5	3	3
<u>216.152.64.213</u>	5	5	2	2
<u>172.138.254.180</u>	5	5	1	1
<u>213.167.201.68</u>	5	5	4	4
<u>24.114.91.40</u>	5	5	4	4
<u>62.156.39.136</u>	5	5	2	2
<u>199.120.223.4</u>	5	5	4	4
<u>24.113.213.145</u>	4	4	1	1
<u>209.214.169.1</u>	4	4	1	1
<u>203.130.2.59</u>	4	4	1	1
<u>216.67.82.19</u>	4	4	1	1
<u>198.88.16.33</u>	4	4	4	4
<u>24.218.207.146</u>	4	4	4	4
<u>62.158.0.171</u>	4	4	2	2
<u>200.48.131.246</u>	4	4	1	1
<u>208.186.209.60</u>	4	4	2	2
<u>193.226.122.85</u>	4	4	1	1
<u>207.175.201.139</u>	4	4	2	2
<u>216.206.201.130</u>	4	4	2	2
<u>203.155.129.184</u>	4	4	1	1
<u>207.175.201.241</u>	4	4	1	1
<u>216.35.217.51</u>	4	4	2	2
<u>4.4.24.171</u>	4	4	1	1
<u>209.133.28.137</u>	4	4	1	1
<u>212.55.140.11</u>	4	4	1	1
<u>207.175.201.207</u>	4	4	2	2
<u>24.5.243.38</u>	4	4	1	1
<u>216.152.64.151</u>	4	4	3	3
<u>211.109.190.131</u>	4	4	1	1
<u>207.175.201.156</u>	4	4	2	2
<u>4.48.207.52</u>	4	4	3	3
<u>206.48.149.28</u>	4	4	1	1
<u>24.112.167.171</u>	4	4	2	2
<u>62.158.106.112</u>	4	4	1	1
<u>192.16.122.4</u>	4	4	3	3
<u>216.15.153.106</u>	4	4	4	4
<u>216.252.144.239</u>	4	4	1	1
<u>4.4.24.166</u>	4	4	1	1
<u>207.7.26.15</u>	4	4	2	2
<u>207.127.235.56</u>	3	3	1	1
<u>166.62.205.97</u>	3	3	1	1
<u>202.5.132.54</u>	3	3	1	1
<u>212.29.92.167</u>	3	3	1	1

<u>166.90.40.24</u>	3	3	1	1
<u>4.4.24.207</u>	3	3	1	1
<u>144.132.54.170</u>	3	3	1	1
<u>212.72.72.66</u>	3	3	3	3
<u>193.95.97.60</u>	3	3	1	1
<u>209.1.233.136</u>	3	3	2	2
<u>207.175.201.221</u>	3	3	2	2
<u>207.175.201.224</u>	3	3	1	1
<u>209.58.12.152</u>	3	3	1	1
<u>216.67.50.182</u>	3	3	1	1
<u>213.153.147.128</u>	3	3	1	1
<u>216.152.64.129</u>	3	3	2	2
<u>199.182.91.111</u>	3	3	1	1
<u>213.8.211.125</u>	3	3	1	1
<u>216.238.1.44</u>	3	3	1	1
<u>193.166.0.134</u>	3	3	2	2
<u>210.9.30.247</u>	3	3	1	1
<u>216.67.82.246</u>	3	3	1	1
<u>216.152.64.130</u>	3	3	2	2
<u>212.181.158.169</u>	3	3	1	1
<u>64.39.31.153</u>	3	3	3	3
<u>4.4.24.243</u>	3	3	1	1
<u>216.152.64.137</u>	3	3	2	2
<u>203.135.53.108</u>	3	3	2	2
<u>168.120.13.177</u>	3	3	1	1
<u>207.175.201.242</u>	3	3	2	2
<u>131.151.185.69</u>	3	3	1	1
<u>216.67.50.74</u>	3	3	1	1
<u>166.62.216.107</u>	3	3	1	1
<u>202.172.112.90</u>	3	3	1	1
<u>205.150.96.2</u>	3	3	2	2
<u>154.5.3.177</u>	3	3	1	1
<u>62.253.45.50</u>	3	3	1	1
<u>212.72.6.227</u>	3	3	1	1
<u>209.214.90.71</u>	3	3	1	1
<u>161.53.3.232</u>	3	3	1	1
<u>210.228.161.36</u>	3	3	1	1

..... <<< TRUNCATED >>>

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
<u>131.195.60.11</u>	177	363	45	47
<u>131.195.60.8</u>	139	195	41	43
<u>131.195.100.2</u>	91	91	4	4
<u>131.195.60.16</u>	39	39	8	8

<u>131.195.222.198</u>	33	34	7	8
<u>131.195.98.111</u>	31	32	4	5
<u>131.195.98.124</u>	23	23	9	9
<u>131.195.97.192</u>	22	22	5	5
<u>131.195.98.185</u>	21	23	6	7
<u>131.195.98.162</u>	20	20	5	5
<u>131.195.98.130</u>	19	19	5	5
<u>131.195.97.237</u>	18	18	2	2
<u>131.195.98.193</u>	18	18	5	5
<u>131.195.97.119</u>	18	18	4	4
<u>131.195.98.106</u>	17	19	6	7
<u>131.195.97.215</u>	17	17	3	3
<u>131.195.53.48</u>	17	17	6	6
<u>131.195.97.169</u>	16	18	6	7
<u>131.195.98.157</u>	16	16	3	3
<u>131.195.97.187</u>	15	15	3	3
<u>131.195.97.115</u>	15	15	4	4
<u>131.195.201.50</u>	14	14	7	7
<u>131.195.97.226</u>	13	13	6	6
<u>131.195.98.170</u>	13	15	2	3
<u>131.195.203.218</u>	13	13	4	4
<u>131.195.60.38</u>	13	13	8	8
<u>131.195.217.46</u>	12	86	7	9
<u>131.195.98.131</u>	12	12	6	6
<u>131.195.98.197</u>	12	12	6	6
<u>131.195.98.137</u>	12	12	4	4
<u>131.195.202.118</u>	12	12	1	1
<u>131.195.152.45</u>	11	13	4	5
<u>131.195.98.127</u>	11	11	3	3
<u>131.195.98.108</u>	11	11	3	3
<u>131.195.98.129</u>	11	11	5	5
<u>131.195.98.199</u>	10	10	6	6
<u>131.195.97.182</u>	10	10	5	5
<u>131.195.97.156</u>	10	10	5	5
<u>131.195.185.20</u>	10	10	4	4

..... <<< TRUNCATED >>>

3.2.4.19 Watchlist 000222 NET-NCFC (The Computer Network Center Chinese Academy of Sciences):

19478 alerts with this signature among the files:

Earliest such alert at **00:33:44.374672** on 08/11

Latest such alert at **17:34:54.171711** on 09/14

Watchlist 000222 NET-NCFC 45 sources 19 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
<u>159.226.63.190</u>	10920	10920	3	3
<u>159.226.45.108</u>	2346	2346	2	2
<u>159.226.114.129</u>	1746	1746	1	1
<u>159.226.45.3</u>	1558	1558	8	8
<u>159.226.63.200</u>	1556	1556	4	4
<u>159.226.5.77</u>	258	258	4	4
<u>159.226.41.166</u>	183	183	1	1
<u>159.226.5.222</u>	161	161	3	3
<u>159.226.21.3</u>	144	144	4	4
<u>159.226.115.1</u>	87	87	4	4
<u>159.226.64.152</u>	77	77	4	4
<u>159.226.23.155</u>	61	61	3	3
<u>159.226.5.94</u>	55	55	3	3
<u>159.226.228.1</u>	52	52	5	5
<u>159.226.66.130</u>	28	28	2	2
<u>159.226.124.58</u>	27	27	1	1
<u>159.226.5.152</u>	25	25	1	1
<u>159.226.159.1</u>	24	24	3	3
<u>159.226.158.188</u>	21	21	3	3
<u>159.226.39.1</u>	16	16	3	3
<u>159.226.22.30</u>	13	13	2	2
<u>159.226.5.65</u>	13	13	3	3
<u>159.226.5.188</u>	12	12	2	2
<u>159.226.64.61</u>	10	10	1	1
<u>159.226.159.146</u>	10	10	1	1
<u>159.226.8.6</u>	9	9	1	1
<u>159.226.22.44</u>	7	7	1	1
<u>159.226.64.138</u>	7	7	3	3
<u>159.226.156.1</u>	6	6	1	1
<u>159.226.118.1</u>	6	6	1	1
<u>159.226.116.129</u>	6	6	2	2
<u>159.226.114.1</u>	5	5	1	1
<u>159.226.47.196</u>	5	5	1	1
<u>159.226.47.14</u>	5	5	1	1
<u>159.226.5.225</u>	4	4	1	1
<u>159.226.128.1</u>	3	3	1	1
<u>159.226.45.195</u>	3	3	1	1
<u>159.226.91.20</u>	2	2	1	1
<u>159.226.128.8</u>	1	1	1	1
<u>159.226.99.1</u>	1	1	1	1
<u>159.226.120.19</u>	1	1	1	1
<u>159.226.120.14</u>	1	1	1	1
<u>159.226.41.188</u>	1	1	1	1
<u>159.226.92.10</u>	1	1	1	1
<u>159.226.68.65</u>	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
131.195.253.43	5387	5419	18	20
131.195.253.42	4404	4416	20	23
131.195.253.41	4256	4287	17	21
131.195.6.7	2565	2577	8	13
131.195.162.199	1746	1746	1	1
131.195.100.230	526	535	12	14
131.195.163.32	260	262	1	2
131.195.60.11	183	363	1	47
131.195.60.8	45	195	1	43
131.195.70.33	40	40	3	3
131.195.100.165	25	37	1	2
131.195.110.150	11	11	1	1
131.195.253.112	7	17	1	3
131.195.1.2	7	7	2	2
131.195.145.18	5	5	1	1
131.195.253.52	5	5	2	2
131.195.6.34	3	8	1	4
131.195.253.53	2	11	2	4
131.195.1.14	1	3	1	2

3.2.4.20 Summary of the possible exploit from the Snort Scan Report:

250175 alerts found among the files: (Scan with less than 8 alerts are not displayed)

Earliest alert at **00:18:09** on 8/15

Latest alert at **22:37:46** on 9/14

Signature	# Alerts	# Sources	# Destinations
TCP 21S*R*A* scan	8	4	3
TCP **SF*P** scan	8	4	4
TCP 2**F*P** scan	8	4	4
TCP 2***P** scan	8	5	4
TCP ****P*U scan	8	5	5
TCP 2**FRP** scan	8	4	3
TCP 2**F*PAU scan	8	4	4
TCP **S*R*** scan	8	4	4
TCP *1*FRP*U scan	8	2	1
TCP 21SFRP*U scan	8	3	3
TCP **SF**A* scan	9	4	4
TCP ***F***U scan	9	4	4
TCP 21SF**** scan	9	5	5
TCP *1***** scan	9	5	5
TCP **S****U scan	9	4	4
TCP ***FRPAU scan	10	2	2
TCP *1***P*U scan	10	3	2

TCP ***FRPA* scan	10	7	8
TCP **S*R*A* scan	10	7	7
TCP 2***RP*U scan	10	8	7
TCP 21S*R*AU scan	10	4	3
TCP *1F**A* scan	11	4	4
TCP *1S*RNAU scan	11	6	6
TCP 2*S*R*A* scan	12	5	5
TCP **SFR*A* scan	12	4	4
TCP 2***R*** scan	12	3	3
TCP 21SFR**U scan	12	6	5
TCP *1**RNAU scan	12	5	4
TCP *1SFRP** scan	13	7	7
TCP **S**PA* scan	13	7	7
TCP *1S*R**U scan	14	5	4
TCP 21S***A* scan	15	2	2
TCP ***FRP*U scan	17	5	4
TCP ****R**U scan	18	5	5
TCP *1**R*** scan	19	8	9
TCP *1***PAU scan	20	5	5
TCP 21SFRPAU scan	21	8	8
TCP 2*S***** scan	35	7	20
TCP ***FR*A* scan	36	11	17
TCP ***F**** scan	40	19	21
TCP **SF*P*U scan	41	7	28
TCP 21S***** scan	44	12	23
TCP 21SF**A* scan	44	4	4
TCP ***F*P*U scan	47	5	32
TCP ***** scan	164	63	73
TCP **SF**** scan	3065	6	3005
UDP scan	58282	52	520
TCP **S***** scan	187304	75	29242

3.2.4.21 UDP Scan Report:

As we just saw in above, we had 58282 udp port scan. It was a little bit hard to find a way to show and represent all the UDP port scan because it reach so many different UDP port. I found that it was more significant to show where it come from and destination addresses of those attack. Here is a resume:

Sources of the attackers(most udp port used): (hostname.domainname)	# Alerts	Most Destination addresses attacked (most udp port used)
210.125.174.11	27125	131.195.97.199(*)
63.248.55.245 (7777) (3ff837f5.dsl.flashcom.net)	17566	131.195.201.150,131.195.203.210,131.195.204.126, 131.195.204.166,131.195.206.222, 131.195.207.50, 131.195.208.238, 131.195.208.58, 131.195.213.10, 131.195.213.78, 131.195.203.210, 131.195.211.146

131.195.1.13	2563	131.195.6.33(7008), 131.195.60.12(7002), 131.195.6.33(7002), 131.195.100.121(7001), 131.195.152.12(7001), 131.195.152.214(7001), 131.195.152.169(7001), 131.195.152.52(7001), 131.195.152.65(7001),
131.195.1.3(53-123)	2564	131.195.*(123,137,53,1029,1283,2563-2567,6821-6822, 31786-31867, 45462-55925,.....)
131.195.1.4(53,123)	2311	131.195.*(123,137, 53,1029,1283,2563-2567,6821-6822, 31786-31867, 45462-55925,.....)
131.195.1.5(53,123)	2158	131.195.*(123,137, 53,1029,1283,2563-2567,6821-6822, 31786-31867, 45462-55925,.....)
209.123.198.156(7777)	1781	131.195.204.126(2286,2295,2297,2306,2314,2317,2322,23 28,2367,2370,...2432), 131.195.213.10(1063-1071), 131.195.204.126(2000)
216.99.200.242(56815) (securedesign.net)	486	131.195.98.188
159.226.185.4	383	131.195.97.199(*)
136.160.7.2(53) (umbi.umd.edu)	212	131.195.1.3-4-5(53), 131.195.115.115(1112-4476), 131.195.110.100(53), 131.195.110.131(53)
24.3.39.44(7001) (cc295102-b.owml1.md.home.com)	147	131.195.6.12-33-42-43-45-48(7000-7003), 131.195.70.142(7000)
128.183.104.105 (neptune.gsfc.nasa.gov)	74	131.195.144.50(3506-3565)
210.61.144.125(1024)	27	131.195.1.3-4-5(53),131.195.110.100(53)
206.186.79.9 (ns.arex.com)	16	131.195.1.4-5(53),131.195.71.15(53), 131.195.109.41(53), 131.195.130.134, 131.195.140.198(53), 131.195.204.218, 131.195.100.165(53), 131.195.106.128, 131.195.109.41(53), 131.195.130.134(53), 131.195.144.25(53), 131.195.181.88(53), 131.195.218.122(53)
216.68.89.4 (ns1.squared.fuse.net)	3	131.195.1.3-4-5(53)
207.151.147.201(2956) (pool.207.151.147.201.cinenet.net)	2	131.195.1.3-4(53)

3.2.4.22 Summary of the possible alert from the raw Snort log file (SOOS*.txt):

After looking into the files, we found that is was only TCP packet. Here is the summary for suspected attack:

7506 alerts found among the files:

Earliest alert at **00:27:14.374672** on 08/28

Latest alert at **22:37:37.338983** on 09/14

Type of attack (by TCP port number)	# Alerts	# Sources	# Destinations
FTP 21 SynFin Scanned or attacked	5818	210.61.144	131.195.*.*
NNTP Port 119 scanned or attacked	139	131.195.217.218	207.172.3.46
TCP port 5190 (AOL) Scanned or attacked	15	131.195.222.110	24.18.91.196
TCP port 9704 (rpc.statd)	1037	213.25.136.60	131.195.*.*
TCP port 6699 (real audio server)	93	*	*
TCP port 2272 (weird TCP flags *1SFR*AU)	32	24.113.80.28	131.195.207.34

Telnet TCP port 23 (weird TCP flags **SF*P*U)	20	24.180.134.156	131.195.208.*
TCP port 2439 (possibly SybaseDBS)	13	24.113.80.28	131.195.207.34
TCP port 6688 (possibly Napster)	13	*	*
TCP port 22 (SSH)	6	151.196.73.119	131.195.253.112
TCP port 20 (ftp-data)	7	24.6.140.249	131.195.130.190

Assignment 4 – “Analysis Process :

This assignment is to describe the process used in analyzing the data in assignment 3. As you must read, I did a lot during the assignment 3 because I made an effort to explain the steps in all sub section and detail of the detects.

How I did it

Here is a list of each of the steps I used to analyze the scenario of the assignment 3.

1. Collect all the material and the data required for the assignment:

- Get the description of the practical assignment
- Download the Snort data from <http://www.sans.org/NS2000/snort/index.htm>
- Get all the standard sets of Snort rule from <http://www.snort.org/>
- TCP/IP protocol reference from the SANS course
- Port lists (Well known ports, registered ports, trojan ports)
- Sample of practical exams from GIAC certified analysts
- Needed of hand-on of Unix and Windows workstations.

2. Indeeep detail analysis of the Snort data:

At first, I found the amount of data overwhelming. So, I start to look for a tool to help me. I already use Snort with a tool called snort2html (http://www.geocities.com/swan_daniel/snort2html.txt). It is very useful and good to see in a per day basis attack and alert made by Snort. But, for screening all that data, I needed something else. So, I download and installed snortsnarf (<http://www.silicondefense.com/snortsnarf/>). That tool was perfect to extract and summarized almost all the data files from SnortA*.txt and SnortS*.txt. Here is a picture of SnortSnarf:

Netscape: SnortSnarf: Snort signatures in SnortA-GIAC-trace-Monterey2K.log et al

File Edit View Go Communicator Help



SnortSnarf start page

All Snort signatures

[SnortSnarf](#) v111500.1

40225 alerts found among the files:

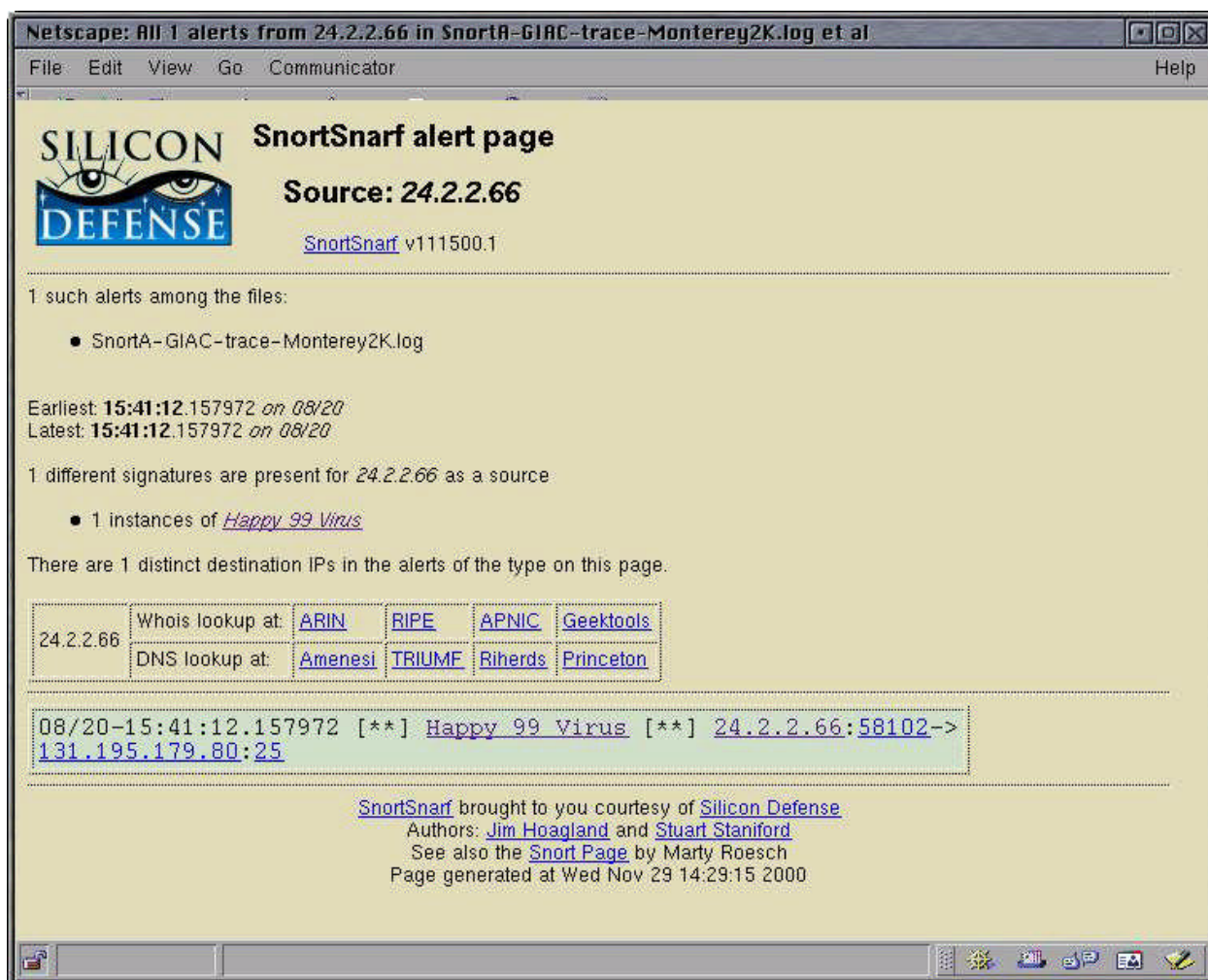
- SnortA-GIAC-trace-Monterey2K.log

Earliest alert at **00:33:44.374672** on 08/11
 Latest alert at **23:21:39.338963** on 09/14

Signature (click for definition)	# Alerts	# Sources	# Destinations	Detail link
Happy 99 Virus	2	2	2	Summary
Possible wu-ftpd exploit - GIAC000623	2	1	2	Summary
site exec - Possible wu-ftpd exploit - GIAC000623	6	1	4	Summary
TCP SMTP Source Port traffic	8	2	2	Summary
Tiny Fragments - Possible Hostile Activity	12	5	8	Summary
External RPC call	40	6	3	Summary
Queso fingerprint	54	11	23	Summary
Probable NMAP fingerprint attempt	64	7	28	Summary
SUNRPC highport access!	64	5	3	Summary
NMAP TCP ping!	138	10	42	Summary
Null scan!	181	63	73	Summary
SMB Name Wildcard	338	17	15	Summary
SNMP public access	922	16	1	Summary
Attempted Sun RPC high port access	1990	8	11	Summary
Watchlist 000220 IL-ISDNNET-990517	5276	19	21	Summary
SYN-FIN scan!	5457	6	3005	Summary
WinGate 1080 Attempt	6193	347	2156	Summary
Watchlist 000222 NET-NCFC	19478	45	19	Summary

[SnortSnarf](#) brought to you courtesy of [Silicon Defense](#)
 Authors: [Jim Hoagland](#) and [Stuart Stanford](#)
 See also the [Snort Page](#) by Marty Roesch
 Page generated at Wed Nov 29 14:20:18 2000

100%



The command line is very easy with SnortSnarf. All you have to do is :

```
./snortsnarf.pl <options> <file1 file2 file3 ...>
```

And, here are the options:

- d directory:** *directory is the path to the directory the HTML pages will be generated in, overriding the default.*
- dns:** *This will cause the script to lookup the DNS name of each IP it writes a page for. On a large alert file, this will take a very long time and will hammer your DNS server.*
- ldir URL:** *URL is the URL of a base directory in which the log files usually found in /var/log/snort are living. With this option, snortsnarf will generate lots of links into those files based at that URL. Eg: with -ldir "http://host.name.here/logs" we get links like http://host.name.here/logs/10.0.0.1/UDP-137-137. Note that the logs themselves aren't parsed.*
- homenet network:** *network is the network IP address or CIDR network notation for your home network, as told to snort. CIDR takes that standard form of address/masksize (sizes 0-32 supported). In the other form, 1-3 zeros at the end of the address are assumed to be what varies within your network. If this argument is not provided, the home network is assumed to be 0.0.0.0 (no home). This is currently used only with the -ldir option.*
- color=<option>:** *option is 'yes' or 'no' or 'rotate'. The style of coloring is given by the option if any. 'rotate' is the only style currently available. This changes the background color between an alert/portscan report and the next one iff the next one has*

a different message signature) source host, or destination host. If 'yes' or this not given on the command line, the the default ('rotate' in this version) is used.

- split=<threshold>: To speed up display of pages containing lots of alerts, <threshold> is a maximum number of alerts to display on a page unless explicitly requested. Instead the alerts are broken into several pages. Default is 100. Can be set to 0 to never split the list alerts being displayed.
- onewindow: If this option is given, certain URs will not be targeted to other browser windows as is the default.
- db path: path is the full path to the annotation database (an XML file), from the point of view of the server hosting the CGI scripts that access it, or the empty string to not use an annotation database. The default is to not use it.
- cgidir URL: URL is the location of the cgi-bin directory that CGI scripts than go along with the program are stored. This make to relative to the pages that are generated (so that when a link appears on a page with URL as a prefix, it will be valid). "/cgi-bin" is the default.
- sisr configfile: Generate links with SnortSnarf Incident Storage and Reporting (SISR). The argument is the full path to the SISR configuration file to use. This file is not parsed by snortsnarf.pl.
- nmapurl URL: URL is the URL of a base URL directory in which the html output of running nmap2html on nmap output is living. With this option, snortsnarf will generate links to output for IP addresses. If the path to that directory is given with the -nmapdir option, then only those pages that actually exist (at the time snortsnarf is run) are linked to.
- nmapdir dir: dir is the directory on the file system in which output is stored. When the -nmapurl option is given, this is used to verify that a nmaplog.pl page actually exists before linking to it.
- rulesfile file: file is the base rule file (e.g., snort.lib) that snort was run with. If this option is given, the rules in that file (and included files) generating a signature are included in the page for that signatures alerts. Note that the processing of the rule files are pretty rough. E.g., variables are ignored.
- rulesdir dir: dir is a directry to use as the base path for rules files rather than the one given or the paths listed in include directives. (Useful if the files have been relocated.)
- refresh=<secs>: add a refresh tag to every HTML page generated, causing browsers to refresh the page ever <secs> seconds.

So, at that point, I had a good idea of the major Snort alert. But that was not done because we had also the files SnortSOOS*.txt. Those files were raw Snort output and snortsnarf does not treat pure raw output. And Snort could not re-read that So, I had to do some grep and regular expression into the text editor vi. Like for example, I wanted to put all the trace on a same line to export it in a spreadsheet after. To do that, I did “:g/^09/j3” for the month of September and “:g/^08/j3” for the month August.

After that I merged all the Snort Alert reports with the TCP/UDP scan and a resume of the raw Snort output.. Then I ran my version of snort_stat.pl on the big alert report file. This gave me 29 pages of sorted statistics. The output lists are:

The number of attack from same host to same destination using same method,
Percentage and number of attacks from a host to a destination
The percentage and number of attacks to one certain host
Percentage and number of attacks from one host to any with same method
The distribution of attack methods

The output of snort_stat.pl gave me a good indication of the suspicious activity on MY.NET.

I also extracted all the ?spp_portscan? messages from the alert reports because they contain more information than reported by snort_stat.pl. In particular, this line with the total values:

```
[**] spp_portscan: End of portscan from 208.160.10.19 (TOTAL HOSTS:8 TCP:6 UDP:2) [**]
```

The list of all the ?End of portscan? lines were imported in Microsoft Excel. It is then easy to apply filters, to sort, etc?

I merged all the Snort Scan reports into one big file also. I used many grep commands, or even Windows FIND when I am stuck on my Win98 machine at home, and simple shell scripts to extract information from this big scan report file, like:

How many times each MY.NET hosts is hit by a port scan
How many hits for each of the 65535 ports

3) High level analysis of the Snort data

I used the top part of the sorted statistics tables just described to establish:

What are the main attack methods used and that I should research and understand
What are the main sources of attacks
What are the most targeted hosts
What are the most scanned port numbers

I also researched the main IP addresses attacking with whois and nslookup queries.

I treated all the events from two aspects:

Snort alert event or scan event
Source is outside or inside MY.NET

4) Detailed analysis of specific Snort alerts