第十五單元

網路入侵偵測系統

1.實驗目的

建置網路入侵偵測系統，並針對封包做偵測，具有網路資料即時分析、報告以及日誌的能力。

2.實驗設備

- 安裝 Linux 系統之電腦
- Snort(http://www.snort.org)

3.背景資料

Snort 是一個封包偵測工具，它可以針對封包做偵測，具有網路資料即時分析、報告以及日誌的能力。可偵測到各種攻擊，例如：CGI 攻擊、緩衝區溢出、隱藏埠的掃描，並將警告的資訊寫到 syslog 或特定的文件檔，如果有人嘗試用 telnet 或是 ftp 進入你的機器時，可以將這些動作紀錄起來，或者是用其他的方式來通知系統管理者。

Snort 在使用上並不是很困難，只是它的規則檔包含了許多指令及選項，很容易讓系統管理者覺得太複雜。其實只要將 snort 安裝完成，其基本的設置都已經足夠讓系統管理者不必去修改，只要再變動一些基礎的環境變數即可。

4.實驗方法

安裝 pcre，請連至 http://www.pcre.org 下載最新的程式碼：

```
[root@net122 root]# tar zxvf pcre-4.1.tar.gz
[root@net122 root]# cd pcre-4.1
[root@net122 pcre-4.1]# ./configure; make ; make install
```

連上 Snort 的官方網站(http://www.snort.org)下載最新版本，目前最新的版本為 2.1.0 版，將之解壓縮後，進入該目錄：

```
[root@net122 linul]# tar zxvf snort-2.1.0.tar.gz
```

安裝前請確認是否有安裝 libpcap 的套件，指令如下：

```
[root@net122 root]# rpm -qa|grep libpcap
```

libpcap-0.7.2-7.1

完成之後，分別下./configure、make、make install 指令來安裝程式。

./configure 的各項參數如下：

`--enable-debug'
Enable debugging options (bugreports and developers only).
`--with-snmp'
Enable SNMP alerting code.
`--enable-smbalerts'
Enable the SMB alerting code, which is somewhat unsafe as it executes a popen() call from within the program (which runs at root privs). You've been warned, use it with caution!
`--enable-flexresp'
Enable the 'Flexible Response' code, that allows you to cancel hostile connections on IP-level when a rule matches. When you enable this feature, you also need the 'libnet'-library that can be found at http://www.packetfactory.net/libnet. See README.FLEXRESP for details. This function is still ALPHA, so use with caution.
`--with-mysql=DIR'
Support for mysql, turn this on if you want to use ACID with MySQL.
`--with-odbc=DIR'
Support for ODBC databases, turn this on if you want to use ACID with a non-listed DB.
`--with-postgresql=DIR'
Support for Postgresql databases, turn this on if you want to use ACID with PostgreSQL.
`--with-oracle=DIR'
Support for Oracle databases, turn this on if you want to use ACID with Oracle.
`--with-openssl=DIR'
Support for openssl (used by the XML output plugin).
`--with-libpq-includes=DIR'
Set the include directories for Postgres SQL database support to DIR.
`--with-libpcap-includes=DIR'
If the configuration script can't find the libpcap include files on its own, the path can be set manually with this switch.
`--with-libpcap-libraries=DIR'
If the configuration script can't find the libpcap library files on its own, the path can be set manually with this switch.
`--with-libxml2-includes=DIR'
Libxml2 include directory.

`--with-libxml2-libraries=DIR'
    Libxml2 library directory.
`--with-libntp-libraries=DIR'
    Libntp library directory.
`--with-libidmef-includes=DIR'
    Libidmef include directory.
`--with-libidmef-libraries=DIR'
    Libidmef library directory.

執行下列的指令：

```
[root@net122 snort-2.1.0]# ./configure
[root@net122 snort-2.1.0]# make
[root@net122 snort-2.1.0]# make install
```

修改/etc/snort/snort.conf。並將：

```
var HOME_NET any
```

修改為：

```
var HOME_NET 192.192.73.0/24
```

然後設定成為自己的網路所在位置。

再將：

```
var RULE_PATH ../
```

修改為：

```
var RULE_PATH /etc/snort/rules
```

然後設定成為剛才拷貝的檔案目錄或是自訂的。

接著在本機測試 snort 是否正常運作，指令如下：

```
[root@net122 snort]# /usr/local/bin/snort -v -l /var/log/snort
```

其中的選項「-v」是開啟 sniffer 模式，而「-l」則是打開 packet logger 模式，稍後會有更詳細的介紹。

接下來到/var/log/snort 目錄下，如果發現多出很多記錄檔，即表示 snort 已經安裝成功。

```
[root@net122 snort]#ls
……..
210.118.121.13  218.76.106.77   65.93.73.29     83.112.2.70
210.202.66.14   218.80.11.115   66.111.54.190   alert
210.49.49.17    218.80.191.35   66.186.79.166   ARP
210.58.155.31   218.80.30.224   66.187.233.4    PACKET_NONIP
210.68.141.78   218.84.221.248  66.234.206.10
```

210.75.28.5　　218.89.138.22　　66.38.8.84

接下來開啟 snort 的 NIDS 模式，指令如下：

```
[root@net122 snort]# /usr/local/bin/snort -c /etc/snort/snort.conf -D
```

其中的選項「-c」是使用指定的檔來做為 snort 的設置檔，在此使用 /etc/snort/snort.conf。而「-D」的選項則是將 snort 設定為 daemon 的方式啟動，啟動後會看到在/var/log/snort/alert 檔案中有許多『事件』，然後可以針對系統的警告來判斷網路狀態為何，這個檔案會視網路狀態的多寡來決定檔案新增的大小，像筆者存在的網路是學校網路，事件很多，打開 NIDS 模式十分鐘，檔案就變成 50k 左右，所以在使用時務必要注意『預設』的記錄模式會產生多少的記錄，千萬不要讓硬碟塞爆。

/var/log/snort/alert 的指令如下：

```
[root@net122 snort]# less alert
```

而其內容如下：

```
[**] [119:13:1] (http_inspect) NON-RFC HTTP DELIMITER [**]
02/18-15:47:31.389221 192.192.73.121:1374 -> 66.35.229.185:80
TCP TTL:128 TOS:0x0 ID:14579 IpLen:20 DgmLen:736 DF
***AP*** Seq: 0xE345D9D    Ack: 0x8DDCB4EA    Win: 0x4320    TcpLen: 20

[**] [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING [**]
02/18-15:47:35.861355 192.192.73.121:1372 -> 66.102.9.99:80
TCP TTL:128 TOS:0x0 ID:14608 IpLen:20 DgmLen:635 DF
***AP*** Seq: 0xE2E6680    Ack: 0x8D953196    Win: 0x4320    TcpLen: 20

[**] [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING [**]
02/18-15:47:35.862964 192.192.73.121:1372 -> 66.102.9.99:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:1110
***AP*** Seq: 0x8D953196    Ack: 0xE2E68D3    Win: 0x16D0    TcpLen: 20
```

雖然 snort 已經在進行記錄所有事件的動作，但由於檔案太太，而且全都是文字介面，看起來有點吃力，所以 snort 也附有其他的 pluggin（外掛）程式，以用來分析及觀察所有事件的記錄。接下來即以一個較簡單的工具－guardian 來說明。

Guardian 可以將 snort 所產生的 alert 檔簡化，長期的記錄下來可以簡化掉不少的記錄檔。首先先到 snort 的官方網站

（http://www.snort.org/dl/contrib/other_tools/guardian/）下載 guardian 的程式，找到最新版本後，解壓縮進入該目錄。

由於 Guardian 是一支用 perl 寫成的程式，所以要修改 guardian.conf 檔，將 Interface eth0 修改為機器上的實際設定。然後將 HostGatewayByte 1 修改為機器上的 IP Address，例如：

```
HostGatewayByte 192.192.73.122
```

將 AlertFile　/var/adm/secure 修改為/var/log/snort/alert，該檔案就是 snort 預設的的警告記錄檔。

接著建立/etc/guardian.ignore，這個檔案是將所有忽略的機器位置列出來，例如 DNS 或是 gateway 等。

將 guardian.conf 拷貝至/etc 中，指令如下：

```
[root@net122 guardian-1.6]# mv guardian.conf /etc
```

再來執行下列指令：

```
cp guardian.pl /usr/local/bin
cd script/
mv iptables_block.sh guardian_block.sh
mv iptables_unblock.sh guardiam_unblock.sh
cp guardian_block.sh /usr/local/bin
cp guardian_unblock.sh /usr/local/bin
```

最後再啟動 guardian：

```
/usr/local/bin/guardian.pl –c /etc/guardian.conf
```

另外，還可以使用如 snortsnarf 的圖形分析工具來觀察 snort 的 alert。

首先先到 snort 的官方網站

（http://www.snort.org/dl/contrib/data_analysis/snortsnarf/）下載 snortsnarf 的程式，然後解壓縮：

```
[root@net122 linul]# tar zxvf SnortSnarf-021111.1.tar.gz
[root@net122 linul]# cd SnortSnarf-021111.1
```

建立 snortsnarf 所需要的 cgi 目錄及網頁輸出目錄：

```
[root@net122 SnortSnarf-021111.1]# mkdir /var/www/cgi-bin/snort
```

```
[root@net122 SnortSnarf-021111.1]# mkdir /var/www/html/snort
```

將陽春的 snort 程式複製到 cgi-bin 中，下列分別是將 SnortSnarf 目錄中的 cgi 程式、include/目錄下的所有東西、以及 snortsnarf.pl 這隻程式複製到正確位置：

```
[root@net122 SnortSnarf-021111.1]# cp cgi/* /var/www/cgi-bin/snort/
[root@net122 SnortSnarf-021111.1]# cp -R include/ /var/www/cgi-bin/snort/
[root@net122 SnortSnarf-021111.1]# cp snortsnarf.pl /var/www/cgi-bin/snort/
```

另外，由於 021111.1 這個版本並不是很完整，所以筆者下載了 020316.1 的版本，解壓縮後，將 Time-modules/lib/Time 這個目錄複製到/var/www/cgi-bin/snort 的目錄下：

```
[root@net122 SnortSnarf-020316.1]# cp -R Time-modules/lib/Time
/var/www/cgi-bin/snort
```

最後再修改 snortsnarf.pl 檔案，之前找的 alert 檔案，其原始設定是：

```
$def_source= $root."var".$dirsep."log".$dirsep."snort.alert";
```

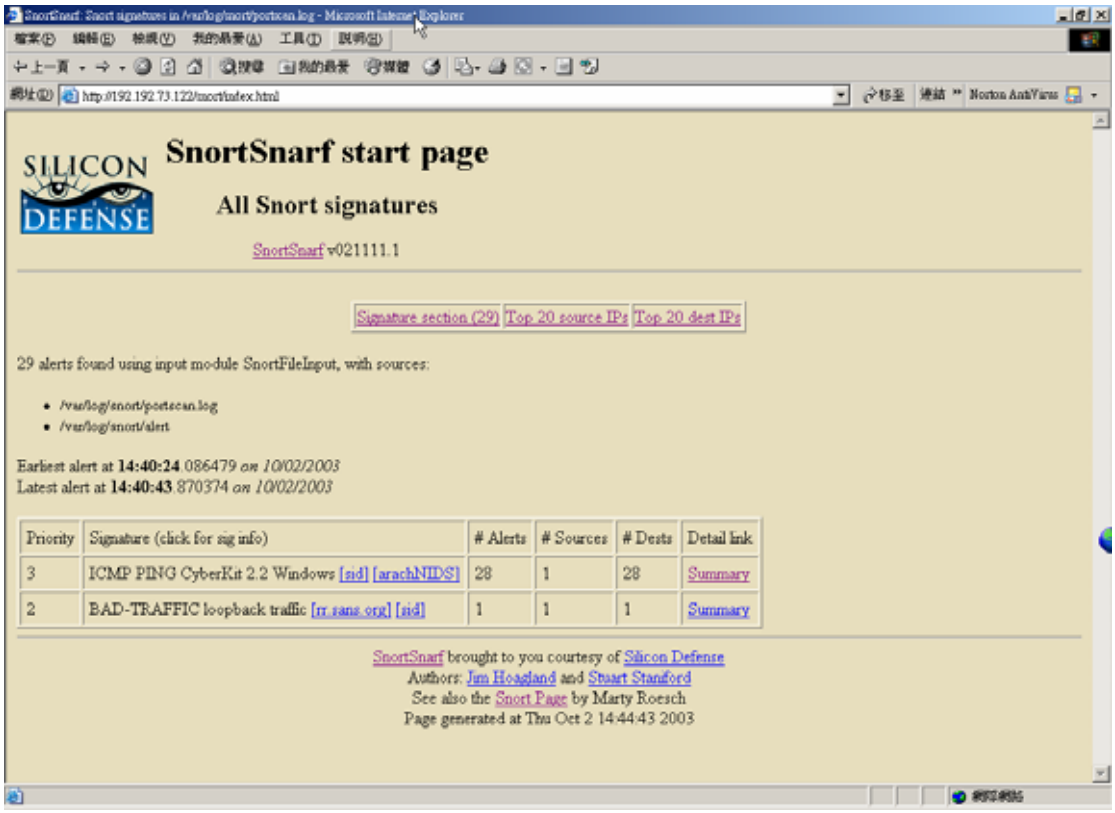
修改之後如下圖所示。

```
$def_source= $root."var".$dirsep."log/snort".$dirsep."alert";
```

最後再執行程式的語法，-d 是指定產生網頁的目錄，-d 是指定規則的目錄及產生的記錄檔的路徑，完整指令如下：

```
[root@net122 snort]# ./snortsnarf.pl -d /var/www/html/snort -color='yes' -rulesdir
/etc/snort/rules /var/log/snort/portscan.log /var/log/snort/alert
```

產生的畫面如下面三張圖所示。



SnortSnarf: Snort signatures in /var/log/snort/portscan.log - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網址(D) http://192.192.73.122/snort/index.html

SnortSnarf start page

All Snort signatures

SnortSnarf v021111.1

Signature section (29) | Top 20 source IPs | Top 20 dest IPs

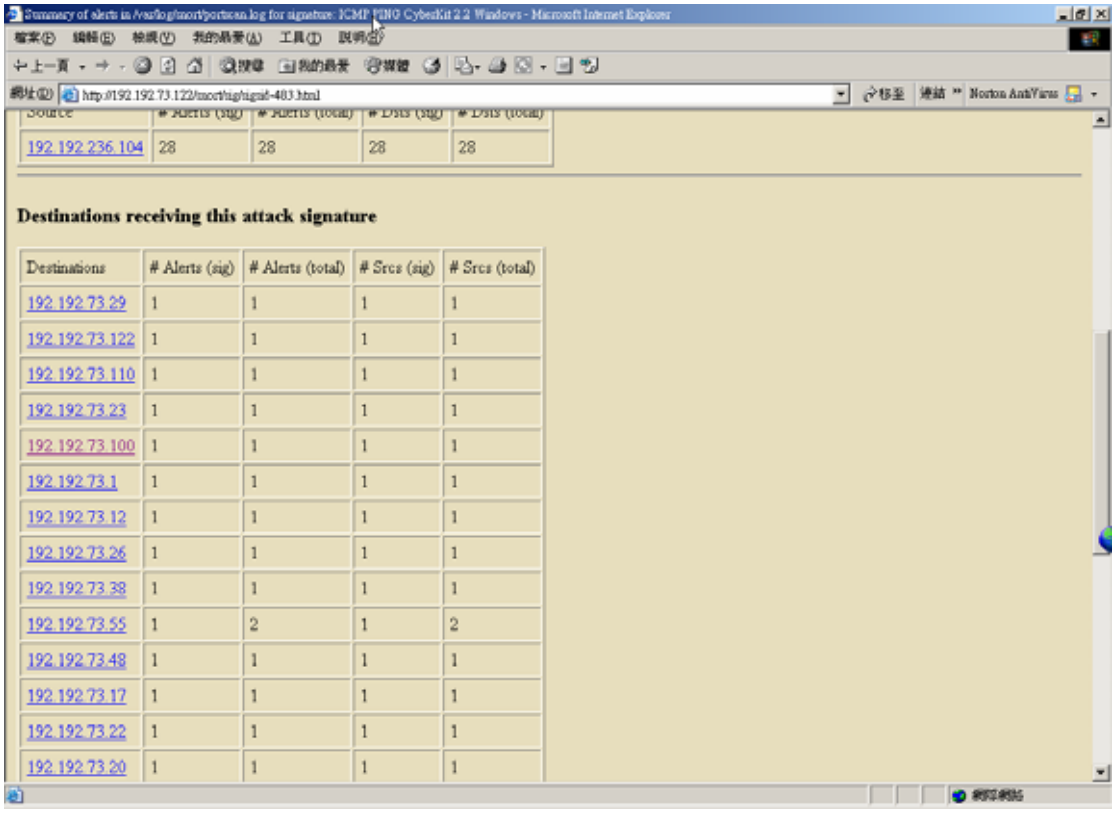
29 alerts found using input module SnortFileInput, with sources:

- /var/log/snort/portscan.log
- /var/log/snort/alert

Earliest alert at **14:40:24** 086479 *on 10/02/2003*
Latest alert at **14:40:43** 870374 *on 10/02/2003*

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
3	ICMP PING CyberKit 2.2 Windows [sid] [arachNIDS]	28	1	28	Summary
2	BAD-TRAFFIC loopback traffic [rr.sans.org] [sid]	1	1	1	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 Thu Oct 2 14:44:43 2003



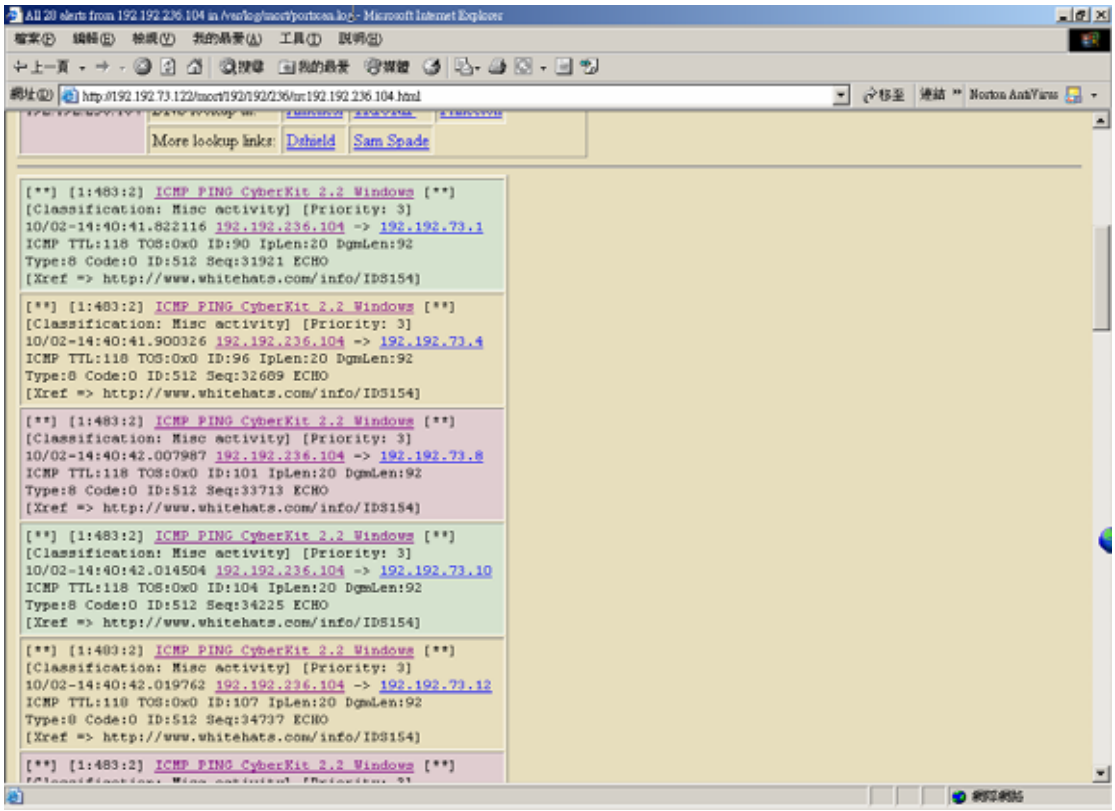
Summary of alerts in /var/log/snort/portscan.log for signature: ICMP PING CyberKit 2.2 Windows - Microsoft Internet Explorer

網址(D) http://192.192.73.122/snort/sig/sig4-403.html

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
192.192.236.104	28	28	28	28

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
192.192.73.29	1	1	1	1
192.192.73.122	1	1	1	1
192.192.73.110	1	1	1	1
192.192.73.23	1	1	1	1
192.192.73.100	1	1	1	1
192.192.73.1	1	1	1	1
192.192.73.12	1	1	1	1
192.192.73.26	1	1	1	1
192.192.73.38	1	1	1	1
192.192.73.55	1	2	1	2
192.192.73.48	1	1	1	1
192.192.73.17	1	1	1	1
192.192.73.22	1	1	1	1
192.192.73.20	1	1	1	1

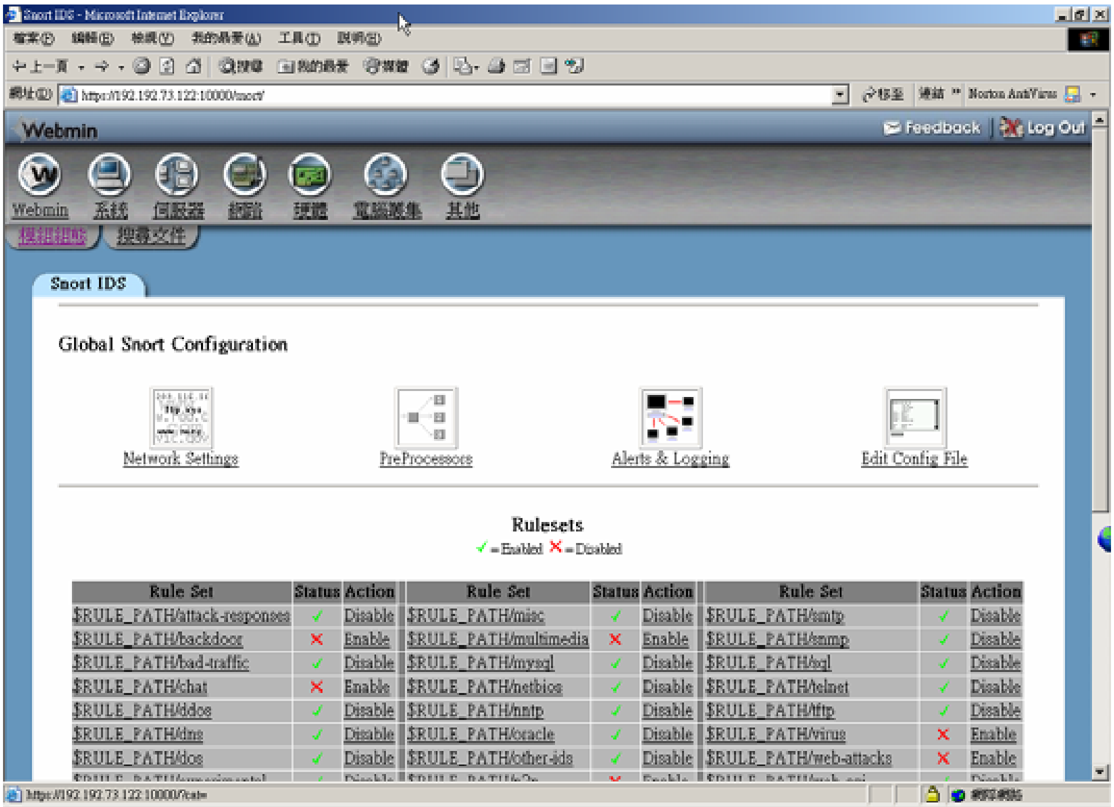


在 Webmin 上的 snort 模組

在 snort 的官方網站（http://www.snort.org/dl/contrib/front_ends/webmin_plugin/）上也存有 Webmin 的 snort 模組。將 snort-1.0.wbm 上傳後，使用 Webmin 的模組安裝程式來安裝，然後到 Webmin 組態的 Webmin 模組將 snort-1.0.wbm 的路徑定義好，然後再按下安裝即可。

進入『模組組態』，將 Command to start Snort （optional）的內容改為如下，即可啟動 snort：

```
/usr/local/bin/snort    -vde -D -c /etc/snort/snort.conf
```



指令及語法介紹

在開始介紹 Snort 的用法之前，先介紹 Snort 的動作原理及使用模式。Snort 在使用上有三種模式：sniffer 模式（一種收集封包數據的工具）、packet logger 模式（將所有的封包記錄成檔案）以及 network intrusion detection system 模式（NIDS 網路入侵偵測系統）。嚴格來說，snort 不只是一個網路入侵偵測的軟體，它同時還具有網管工具的功能，可以依照管理者不同的需求來轉換不同的模式。

Sniffer 模式

如果只要在螢幕上顯示出 TCP/IP 的封包標頭時，可以使用下列的指令：

[root@net122 root]# /usr/local/bin/snort -v

```
10/02-09:53:28.860517 192.192.73.122:22 -> 61.62.103.105:1091
TCP TTL:64 TOS:0x10 ID:27420 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xEF0CAF2A  Ack: 0x7FDF42EC  Win: 0x1D50  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

以上的指令只能顯示 IP 和 TCP/UDP/ICMP 的封包標頭而已，如果要顯示應用層的資料時，可以在選項的部份再加上一個 d 的選項，指令如下：

[root@net122 root]# /usr/local/bin/snort -vd

```
10/02-09:56:52.611775 192.192.73.100:4662 -> 218.162.171.44:62035
TCP TTL:128 TOS:0x0 ID:49187 IpLen:20 DgmLen:466 DF
***AP*** Seq: 0x2F275718  Ack: 0x38E607E0  Win: 0x1DE8  TcpLen: 20
9E 23 D6 10 C6 9E 09 43 01 70 37 DC AD 1A 8A 6F  .#.....C.p7....o
04 C3 04 42 BD EA C1 6B 1E 9E 5A 35 31 7E 7B AE  ...B...k..Z51~{.
BD 35 FC 35 7D EC 82 0C 0C 73 A5 B2 D9 41 F1 B0  .5.5}....s...A..
C7 C0 CC 76 25 2F E8 86 72 21 10 78 F1 EC 13 46  ...v%/..r!.x...F
7A 27 FA 30 06 38 0C F1 E9 7E CE 83 8D 06 9B 45  z'.0.8...~.....E
3F CF B2 59 98 23 8C 69 32 B2 05 56 50 8E 4D 39  ?..Y.#.i2..VP.M9
43 8D A3 56 10 6D 63 53 DB 6C 52 2E B6 35 5D F6  C..V.mcS.lR..5].
A5 23 72 FA 15 36 03 64 14 02 2F 6F 8B 58 56 10  .#r..6.d../o.XV.
57 78 28 46 75 6C E5 17 27 58 2E 9A 57 A0 F9 6A  Wx(Ful..'X..W..j
04 84 00 54 00 53 2D 50 A0 85 99 D2 51 81 D2 F8  ...T.S-P....Q...
92 5F 06 52 5A AE 8F E1 A7 F6 19 8E F3 9D C6 47  ._.RZ..........G
46 04 F6 F4 CE DA 4F F4 E6 7A 25 FD 66 68 38 82  F.....O..z%.fh8.
06 A5 2F B8 B3 6B ED 38 86 5A 10 68 B8 A2 10 41  ../..k.8.Z.h...A
CB 31 1E 18 B6 CB C2 A2 9C 8D 20 B1 09 4B 42 EB  .1.........KB.
A9 6A AA 24 DC DE 37 CD 2C 4A 69 FB D3 B0 AD 4E  .j.$..7.,Ji....N
1E 00 DF 51 22 50 92 27 F7 C2 FF 74 30 55 C0 D9  ...Q"P.'...t0U..
90 B5 87 4E 20 BA D0 CC 60 51 D1 A8 5C 7B 07 F8  ...N ...`Q..\{..
D1 31 CB 7B D2 B5 B2 7F 40 90 0D 7C 9B D5 BD DD  .1.{....@..|....
71 CD DF 2B 7C 96 48 1A FB E5 57 CF 0D 53 F7 D5  q..+|.H...W..S..
8E F7 7B 82 57 81 E2 AC 02 2C D4 19 02 31 B5 70  ..{.W.....,..1.p
4F FA 83 65 B3 B6 BD A0 75 56 7C 7F 0B AD 79 E3  O..e....uV|...y.
E9 F3 FA 7C 37 FA 94 40 8F 93 A1 16 10 10 20 D5  ...|7..@....... .
AD 0C A2 94 49 FA 37 63 70 CC B5 F7 52 08 F9 EE  ....I.7cp...R...
B3 E6 70 BB 58 8F 65 4B 7D BA B7 BF 02 34 B9 FA  ..p.X.eK}....4..
AB 09 14 70 7E 16 52 AD 8B F5 97 80 31 E8 09 1A  ...p~.R.....1...
C2 CD 0A F2 C5 13 BC 51 F5 A5 CC BD C1 E4 B7 66  .......Q.......f
8F 5F DF DC 77 3D 9D C8 85 E3                    ._..w=....
```

如果要抓取鏈結層的資訊，可以使用 e 的選項，指令如下：

/usr/local/bin/snort -ve

或是使用/usr/local/bin/snort –vde，也可以將全部資訊都抓下來。

```
10/02-10:00:50.208426 0:E0:18:B2:92:15 -> 0:D0:D3:2D:8D:4B type:0x800 len:0x1AD
192.192.73.100:4662 -> 218.162.194.47:3804 TCP TTL:128 TOS:0x0 ID:36435 IpLen:20 DgmLen:415 DF
***AP*** Seq: 0x6BC8D155  Ack: 0xC1E2C1E0  Win: 0x21AE  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

在使用 snort 的選項時，可以將它拆開來用，例如：/usr/local/bin/snort –vde 與 /usr/local/bin/snort –v –d -e
是相同的。

Packet logger 模式

Sniffer 雖然可以在螢幕上顯示所有的封包訊息，但卻無法記錄成檔案來分析資訊，所以 snort 也提供了另一個模式來供管理者使用，如果要將所有與預設的區網內的主機有通訊的封包抓取下來，可以使用下列的指令：

[root@net122 root]# /usr/local/bin/snort -vde -l /var/log/snort

```
[root@net122 snort]# ls
12.103.239.80     192.192.73.1     192.192.73.45    210.50.248.126   218.166.150.19  24.84.232.246   61.59.106.130  ARP
140.119.225.243   192.192.73.10    192.192.73.47    210.85.144.125   218.167.36.113  61.218.0.98     61.62.103.105  PACKET_NONIP
140.119.74.21     192.192.73.100   192.192.73.59    211.21.63.155    218.20.123.73   61.223.132.27   61.64.109.12
163.28.4.1        192.192.73.122   203.168.242.9    211.75.4.190     218.84.50.83    61.230.140.74   61.64.109.128
192.192.232.248   192.192.73.17    203.204.93.167   218.160.49.144   219.68.42.161   61.230.75.156   61.70.135.250
192.192.236.146   192.192.73.2     203.64.127.48    218.163.170.142  219.68.67.103   61.231.26.3     61.70.173.127
192.192.72.232    192.192.73.22    210.19.86.131    218.164.242.39   219.91.87.206   61.56.137.163   66.120.56.173
```

下完指令後，可以在/var/log/snort 目錄下看到許多以 IP 分類的目錄，其中記載了 snort 所記錄的資訊，內容就和之前 sniffer 模式完全相同。

```
[root@net122 61.62.103.105]# pwd
/var/log/snort/61.62.103.105
[root@net122 61.62.103.105]# ls
TCP:1114-22
```

接著查看 61.62.103.105 目錄中 TCP:1114-22 檔案的資訊，會發現其實是相同的，如下圖所示。

```
10/02-10:28:38.462239 0:D0:D3:2D:8D:4B -> 0:2:44:13:46:E4 type:0x800 len:0x4A
61.62.103.105:1114 -> 192.192.73.122:22 TCP TTL:115 TOS:0x0 ID:20005 IpLen:20 DgmLen:60 DF
***AP*** Seq: 0xA68B3D10  Ack: 0x931D43B6  Win: 0x7FFF  TcpLen: 20
00 00 00 0A B7 1A 44 D0 FB 16 11 1C 11 B0 F4 E4  ......D.........
49 75 D1 BD                                      Iu..
```

假設為了伺服器的效能，要使用二進制的 tcpdump 格式來進行記錄的話，可以使用選項 b 來進行記錄，因為如此一來只會記錄成一個 tcpdump 檔案，而要查看這個檔案時候，只要用選項 r 即可。

■ 記錄

[root@net122 snort]# /usr/local/bin/snort -vde -l -h 61.62.103.105 /var/log/snort

■ 閱讀

[root@net122 snort]# /usr/local/bin/snort -r ./snort.log.1065106946

入侵偵測模式

入侵偵測模式也是記錄的一種，只不過它所記錄的規則是由/etc/snort/rules 所制定的事件規則及資訊兩者，與先前封包記錄的方式不大一樣，它除了會將事件記錄在 alert 檔外，還會將出現在 alert 中的 IP 傳送的資料分類在各個目錄中，換句話說，入侵偵測模式會將網路上出現不正常的封包記錄到 alert 中，然後將這些發出不正常記錄的封包的 IP 傳輸記錄也記錄下來，因此，它的記錄檔並不會將所有的封包都記錄下來，只是將錯誤的或是具有攻擊性的封包及事件記錄下來。

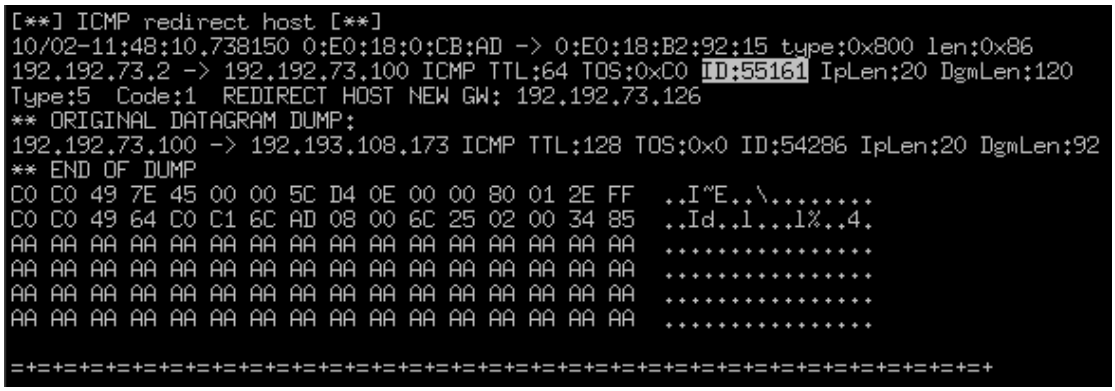
舉例來說，如果要抓取 alert 事件中的所有封包資訊，請使用下列指令：

[root@net122 snort]# /usr/local/bin/snort -vde -c /etc/snort/snort.conf

在/var/log/snort/alert 中找尋一個 ICMP 事件的 ID：55161，如下圖所示。

```
[**] [1:472:1] ICMP redirect host [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/02-11:48:10.738150 0:E0:18:0:CB:AD -> 0:E0:18:B2:92:15 type:0x800 len:0x86
192.192.73.2 -> 192.192.73.100 ICMP TTL:64 TOS:0xC0 ID:55161 IpLen:20 DgmLen:120
Type:5  Code:1  REDIRECT HOST NEW GW: 192.192.73.126
** ORIGINAL DATAGRAM DUMP:
192.192.73.100 -> 192.193.108.173 ICMP TTL:128 TOS:0x0 ID:54286 IpLen:20 DgmLen:92
** END OF DUMP
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0265][Xref => http://www.whitehats.com/info/IDS135]
```

然後在目錄/var/log/snort/192.192.73.2/的 ICMP_REDIRECT 檔中找到下面的 ID，並檢視它的封包訊息，如下圖所示。

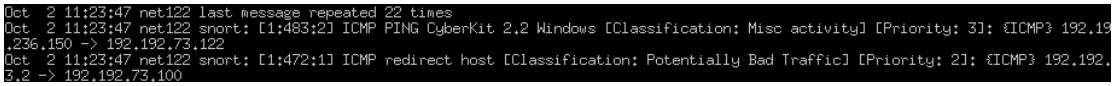


如果是針對惡意的攻擊事件來分析封包內容，可以容易的得知來源及攻擊的模式。

另外，如果要把 alert 記錄到 syslog 中，只要用選項 s 即可，指令如下：

[root@net122 snort]# /usr/local/bin/snort -c /etc/snort/snort.conf -s

接著到/var/log/messages 目錄下，即可看到訊息，如下圖所示。



假設有架設 samba 伺服器，即可利用 samba 將 alert 的訊息用 WinPopup 的方式丟到 windows 的機器，而且在下./configure 指令時就要用-enable-smbalerts 的參數，然後在指令裡面使用 M 的選項。不過，建議不需要這樣做，因為如果訊息一多，管理者可能會瘋掉，指令如下：

[root@net122 snort]# /usr/local/bin/snort -c /etc/snort/snort.conf –M 主機名稱

最後是 rule 的升級。由於 snort 版本經常在更新，所以為了保持最新的規則來防禦不正常的網路行為，必須要不定時升級規則檔，最新的 rule 下載位置為 http://www.snort.org/dl/rules/snortrules-current.tar.gz。下載之後，將這個目錄解壓縮至 rule 的目錄中即可使用，在此是使用 /etc/snort/rules 這個目錄。

[root@net122 snort]#tar zxvf snortrules-current.tar.gz /etc/snort/rules

如此一來即完成了 rules 的升級動作，或是也可以將以上的動作加到 cron 的行程中，固定每隔一段時間抓一次新的 rule。然後將 snort 以 daemon 的模式啟動，再把這行指令加到 rc.local 檔，以後在開機的時候就會自動啟動入侵偵測的模式。

入侵偵測模式的指令相當多，但一般的使用者只要使用預設的命令就足以滿足大部份的狀況，在此介紹的只是一些基本的指令模式，對大部份攻擊模式的偵測，snort 在 rules 的目錄中都已經定義了所有的偵測規則；另外一個較複雜的是 rules 的各項語法，如果有興趣進一步研究，可以到 snort 官方網站找尋資料。

5.問題與討論

1. 說明網路中的哪一個位置是安裝 snort 的最佳位置？
2. 說明規則要如何更新？
3. 說明 snort 的紀錄檔，並當發現有人入侵時會如何反應？
4. 說明 snort 如何安裝在 MS 系統上？
5. 如果發現有人入侵時，該如何即時通知管理者？