

網路安全的理論與實務

楊中皇 著

第十三章 Snort

<http://crypto.nknu.edu.tw/textbook/>

金 禾 圖 書

伴 您 學 習 成 長 的 每 一 天



# 第十三章 Snort

- **Snort**簡介
- **Snort**的安裝方法
- **Snort**的使用



# Snort發展歷史

- Snort ( <http://www.snort.org/> ) 為Marty Roesch在1998年所發展出來的輕量級入侵偵測系統 ( Intrusion Detection System, IDS ) ，是遵循GPL授權規範的開放原始碼軟體
- Snort的運作模式有三個類型
  - 嗅探器模式 ( Sniffer mode )
  - 封包記錄器模式 ( Packet Logger mode )
  - 網路入侵偵測系統模式 ( Network Intrusion Detection System ( NIDS ) mode )



# Snort發展歷史(續)

- 一般 IDS 的主要設計都是利用規則集 ( Ruleset ) ，針對可能入侵的行為作偵測；在 Snort 的官方網站中有最新的規則集提供下載使用
- Snort 設計一套頗富彈性的規則語言 ( Rules Language ) ，因此使用者亦可以定義規則集，甚至將自行定義的規則集回報給 Snort 官方網站建議更新使用
- Snort 的系統架構是採模組化設計，系統管理者在安裝好基本的 Snort 套件之後，可以再安裝外掛套件增加功能，例如加強入侵偵測與防護的能力、擷取與維護現行的規則集...等



- Snort支援的作業系統如下：
  - Linux
  - Windows
  - FreeBSD
  - NetBSD
  - OpenBSD
  - Sun Solaris
  - HP-UX
  - IBM AIX
  - SGI IRIX
  - MacOS X
  - MkLinux



# Snort安裝-Linux

- 以Fedora Core 4（FC4）作為測試的作業系統
- 由於安裝Snort需要的套件不只一個，此外也會介紹外掛套件的安裝
- 一般最常用的組合是Snort + ACID（Analysis Console for Intrusion Databases），且使用ACID還要事先安裝MySQL、Apache及PHP，另外還有配合使用的ADOdb及JpGraph模組等
- 建議讀者以root權限依照下列的順序來安裝，安裝之前請確認SELinux的功能是關閉狀態，否則將無法順利執行



# Tarball套件安裝

- **libpcap**：FC4預設安裝libpcap的RPM版本為0.8.3版，以Tarball套件升級安裝0.9.1版的指令順序如下：
  - tar xvfz libpcap-0.9.1.tar.gz
  - cd libpcap-0.9.1
  - ./configure
  - make
  - make install



- **PCRE**：安裝Perl正規表示式函式庫，安裝6.1版指令如下：
  - tar xvfz pcre-6.1.tar.gz
  - cd pcre-6.1
  - ./configure
  - make
  - make install





# 安裝與設定MySQL

- **MySQL**：安裝MySQL版本為4.1.12，首先建立使用者及群組：
  - `/usr/sbin/groupadd mysql`
  - `/usr/sbin/useradd -g mysql mysql`
- 將mysql-4.1.12.tar.gz移到/usr/local目錄並解壓縮：
  - `mv mysql-4.1.12.tar.gz /usr/local`
  - `cd /usr/local`
  - `tar xvfz mysql-4.1.12.tar.gz`
  - `cd mysql-4.1.12`



# 安裝與設定MySQL(續)

- 編譯及安裝MySQL：
  - `./configure -prefix=/usr/local/mysql --with-charset=big5`
  - `make`
  - `make install`
- 初始化mysql資料庫：
  - `scripts/mysql_install_db`
- 設定相關目錄的擁有者：
  - `chown -R root /usr/local/mysql`
  - `chown -R mysql /usr/local/mysql/var`
  - `chown -R mysql /usr/local/mysql`



# 安裝與設定MySQL(續)

- 將設定檔複製到/etc目錄：
  - `cp support-files/my-medium.cnf /etc/my.cnf`
- 編輯/etc/ld.so.conf檔：
  - `vi /etc/ld.so.conf`
- 新增以下兩行：
  - `/usr/local/mysql/lib/mysql`
  - `/usr/local/lib`
- 儲存後離開，並執行：
  - `/sbin/ldconfig -v`
- 以安全模式啟動MySQL測試：
  - `/usr/local/mysql/bin/mysqld_safe -user=mysql &`



# 安裝與設定MySQL(續)

- 檢視MySQL服務是否順利執行：
  - `ps -ef | grep mysql`
- 設定MySQL服務在Linux開機時啟動：
  - `cp support-files/mysql.server /etc/rc.d/init.d/mysql`
  - `cd /etc/rc.d/init.d`
  - `chmod 755 mysql`
  - `cd /etc/rc3.d`
  - `ln -s /etc/rc.d/init.d/mysql S85mysql`
  - `ln -s /etc/rc.d/init.d/mysql K85mysql`
  - `cd /etc/rc5.d`
  - `ln -s /etc/rc.d/init.d/mysql S85mysql`
  - `ln -s /etc/rc.d/init.d/mysql K85mysql`



- 安裝Apache2.0.54版及PHP4.4版，先將套件檔移到/usr/local目錄：
  - mv httpd-2.0.54.tar.gz /usr/local
  - mv php-4.4.0.tar.gz /usr/local
  - cd /usr/local



- Apache解壓縮與安裝：
  - `tar xvfz httpd-2.0.54.tar.gz`
  - `cd httpd-2.0.54`
  - `./configure -prefix=/usr/local/apache -enable-so`
  - `make`
  - `make install`
- PHP解壓縮與安裝：
  - `tar xvfz php-4.4.0.tar.gz`
  - `cd php-4.4.0`
  - `./configure`設定為同一行：  
`./configure --prefix=/usr/local/php --with-apxs2=/usr/local/apache/bin/apxs --with-config-file-path=/usr/local/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib-dir=/usr/local --with-gd`



- 進行安裝，安裝完畢將設定檔php.ini-dist複製到PHP的安裝目錄：
  - make
  - make install
  - cp php.ini-dist /usr/local/php/php.ini
- 修改httpd.conf檔以載入PHP模組：
  - vi /usr/local/apache/conf/httpd.conf
- 新增下列設定：
  - LoadModule php4\_module modules/libphp4.so
- 修改mime.types檔以支援PHP文件：
  - vi /usr/local/apache/conf/mime.types



- 新增下列設定：
  - application/x-httpd-php php
  - application/x-httpd-php-source php
- 設定Apache服務在Linux開機時啓動，在此之前務必先關閉SELinux的功能：
  - `cp /usr/local/apache/bin/apachectl /etc/rc.d/init.d/httpd`
  - `cd /etc/rc3.d`
  - `ln -s /etc/rc.d/init.d/httpd S85httpd`
  - `ln -s /etc/rc.d/init.d/httpd K85httpd`
  - `cd /etc/rc5.d`
  - `ln -s /etc/rc.d/init.d/httpd S85httpd`
  - `ln -s /etc/rc.d/init.d/httpd K85httpd`





# Snort套件安裝

- 安裝Snort2.3.3版，首先建立使用者及群組：
  - groupadd snort
  - useradd -g snort snort
- 進行解壓縮並安裝：
  - mkdir /etc/snort
  - mkdir /var/log/snort
  - mv xvfz snort-2.3.3.tar.gz /usr/local
  - cd /usr/local
  - tar xvfz snort-2.3.3.tar.gz
  - cd snort-2.3.3
  - ./configure --with-mysql=/usr/local/mysql
  - make
  - make install



# Snort套件安裝(續)

- 配置規則集：
  - `cd rules`
  - `cp * /etc/snort`
  - `cd ../etc`
  - `cp snort.conf /etc/snort`
  - `cp *.config /etc/snort`
- 將unicode.map檔複製到/etc/snort目錄：
  - `cp unicode.map /etc/snort`
- 修改snort.conf檔：
  - `vi /etc/snort/snort.conf`



# Snort套件安裝(續)

- 修改下列設定：
  - var HOME\_NET 192.168.1.0/24
  - var RULE\_PATH /etc/snort
  - output database: log, mysql, user=snort password=使用者  
自定密碼 dbname=snort host=localhost
- 設定Snort服務檔及開機啓動：
  - cd /etc/rc.d/init.d/
- 建立並編輯snort服務啓動檔：
  - vi snort
- 新增下行指令字串到snort檔，儲存後離開：
  - /usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g snort &



# Snort套件安裝(續)

- 設定snort為執行檔：
  - `chmod 755 snort`
- 設定Snort服務在開機時啟動：
  - `cd /etc/rc3.d`
  - `ln -s /etc/rc.d/init.d/snort S99snort`
  - `ln -s /etc/rc.d/init.d/snort K99snort`
  - `cd /etc/rc5.d`
  - `ln -s /etc/rc.d/init.d/snort S99snort`
  - `ln -s /etc/rc.d/init.d/snort K99snort`
- 設定資料庫，並新建snort資料庫及配置使用者權限。以資料庫的root帳號登入，預設密碼為空白：
  - `/usr/local/mysql/bin/mysql mysql -u root -p`



# Snort套件安裝(續)

- 登入後會出現mysql>，後續操作如下：  
mysql> SET PASSWORD FOR root@localhost=PASSWORD("更改root密碼");  
>Query OK, 0 rows affected (0.25 sec)  
mysql> create database snort;  
>Query OK, 1 row affected (0.01 sec)  
mysql> grant INSERT,SELECT on root.\* to snort@localhost;  
>Query OK, 0 rows affected (0.02 sec)  
mysql> SET PASSWORD FOR snort@localhost=PASSWORD("設定snort密碼");  
>Query OK, 0 rows affected (0.25 sec)  
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.\* to snort@localhost;  
>Query OK, 0 rows affected (0.02 sec)  
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.\* to snort;  
>Query OK, 0 rows affected (0.02 sec)  
mysql> exit  
Bye



# Snort套件安裝(續)

- 以snort帳號登入，並建立snort資料庫的資料表，下述指令為同一行：
  - `/usr/local/mysql/bin/mysql -u snort -p < /usr/local/snort-2.3.3/schemas/create_mysql snort`
- 檢視所有資料庫：
  - `mysql> show databases;`
- 選取snort資料庫：
  - `mysql> use snort;`  
Database changed
- 檢視snort資料庫中的所有資料表，確認snort資料庫建置完畢：
  - `mysql> show tables;`



- 首先將相關套件移到/usr/local/apache/htdocs目錄：
  - mv acid-0.9.6b23.tar.gz /usr/local/apache/htdocs
  - mv adodb464.tgz /usr/local/apache/htdocs
  - mv jpgraph-1.19.tar.gz /usr/local/apache/htdocs



- 增加ADOdb資料庫存取介面模組：
  - tar xvfz adodb464.tgz
  - rm -rf adodb464.tgz
- 增加JpGraph繪圖模組：
  - tar xvfz jpgraph-1.19.tar.gz
  - rm -rf jpgraph-1.19.tar.gz
  - cd jpgraph-1.19/
  - rpm -rf README
  - rpm -rf QPL.txt





- 增加ACID模組並修改acid\_conf.php設定檔，以存取資料庫及使用繪圖模組：
  - tar xvfz acid-0.9.6b23.tar.gz
  - rm -rf acid-0.9.6b23.tar.gz
  - cd acid
  - vi acid\_conf.php



- 確認並修改下列內容：

```
/* Path to the DB abstraction library */
$DBlib_path = "/usr/local/apache/htdocs/adodb";
/* The type of underlying alert database */
$DBtype = "mysql";
/* Alert DB connection parameters */
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "之前設定的snort使用者密碼";
/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "之前設定的snort使用者密碼";
/* Path to the graphing library */
$ChartLib_path = "/usr/local/apache/htdocs/jpgraph-1.19/src";
```



# RPM套件安裝

- 使用**Snort + ACID**的組合，能讓系統管理者透過網頁介面，便利檢視入侵偵測的資訊，進而有效管理網路安全
- 但要安裝的相關套件實在繁多，使用**Tarball**套件安裝方式比較費時
- 因此以**RPM**套件安裝是不錯的選擇；如果在安裝**FC4**時沒有選擇安裝**Apache**、**PHP**及**MySQL**相關軟體，可以在裝完**FC4**後再自行安裝，所需的套件建議如下一頁表列，安裝完畢後請關閉**SELinux**的功能



# Snort + ACID安裝需先行安裝的RPM套件

金禾資訊

伴 您 學 習 成 長 的 每 一 天

套件檔名	簡介
crypto-utils-2.2-5.i386.rpm	SSL憑證與金鑰管理公用程式
httpd-2.0.54-10.i386.rpm	Apache網頁伺服器主要程式
httpd-devel-2.0.54-10.i386.rpm	Apache網頁伺服器開發工具
distcache-1.4.5-7.i386.rpm	分散式SSL session快取程式
distcache-devel-1.4.5-7.i386.rpm	分散式SSL session快取開發工具
mod_auth_mysql-2.6.1-4.i386.rpm	結合MySQL作Apache網頁伺服器基本認證
mod_perl-2.0.0-0.rc5.3.i386.rpm	Apache網頁伺服器用的嵌入式Perl直譯器
mod_perl-devel-2.0.0-0.rc5.3.i386.rpm	使用mod_perl建立XS模組所需的檔案
mod_ssl-2.0.54-10.i386.rpm	Apache網頁伺服器用的SSL/TLS安全連線模組
php-5.0.4-10.i386.rpm	PHP嵌入式網頁描述語言
php-mysql-5.0.4-10.i386.rpm	PHP應用程式存取MySQL資料庫用的模組
webalizer-2.01_10-28.i386.rpm	網頁伺服器日誌檔分析程式
MyODBC-2.50.39-24.i386.rpm	MySQL用的ODBC驅動程式
mysql-4.1.11-2.i386.rpm	MySQL客戶端程式及共享函數庫
mysql-devel-4.1.11-2.i386.rpm	MySQL應用程式的開發工具
mysql-server-4.1.11-2.i386.rpm	MySQL伺服器及相關檔案
Perl-DBD-MySQL-2.9007-1.i386.rpm	Perl用的MySQL資料庫存取介面



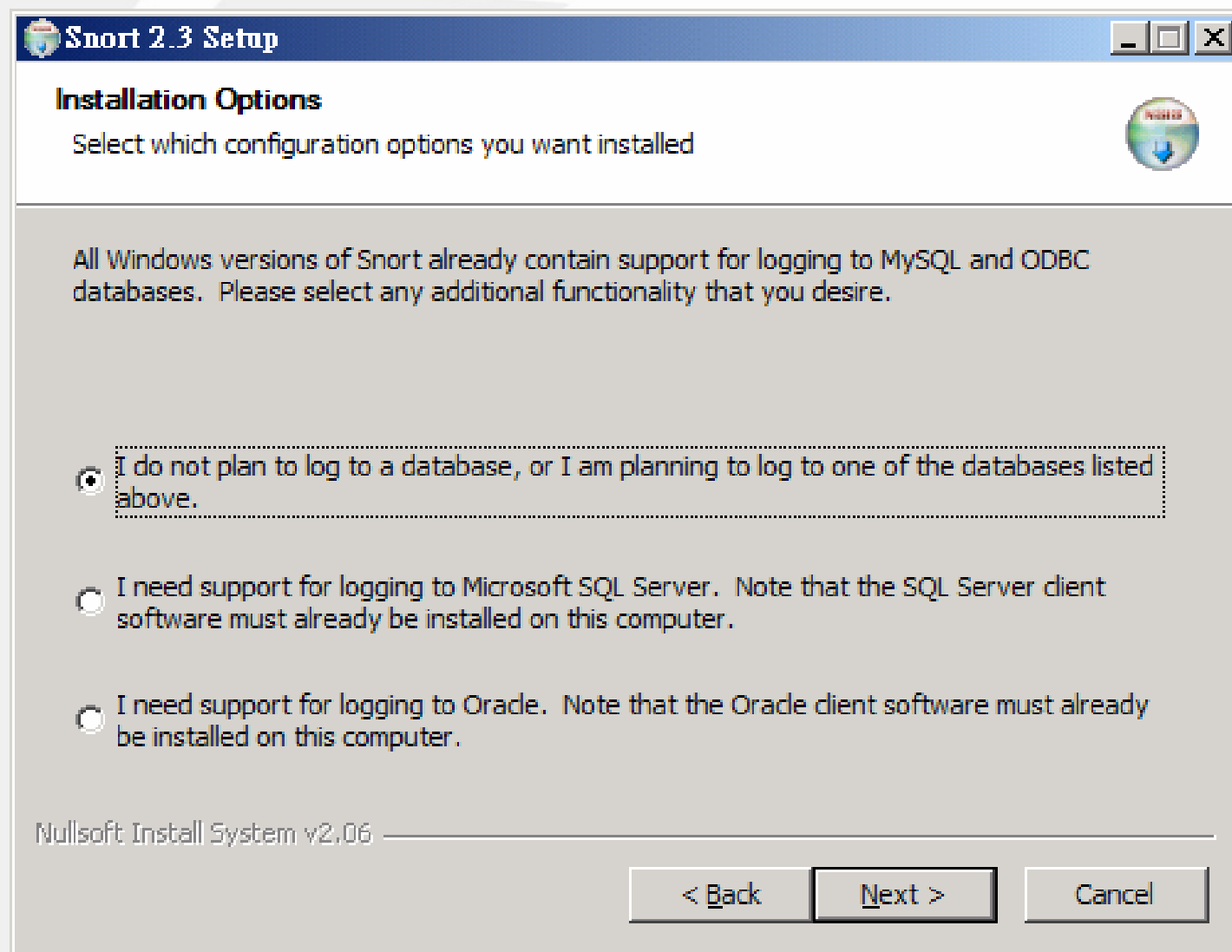
# Snort RPM套件安裝

- 若要安裝Snort的主要程式，則可使用Snort官方網站上專為Fedora Core Linux所提供的RPM版本，其安裝的指令及套件如下：
  - rpm -ivh snort-2.3.3-0.fdr.1.i386.rpm
  - rpm -ivh snort-mysql-2.3.3-0.fdr.1.i386.rpm
- 如安裝完畢後，則會有snortd檔案裝在/etc/rc.d/init.d目錄下，設定讓snortd在開機時（重新開機才會生效）啟動指令如下：
  - chkconfig --add snortd
  - chkconfig snortd on



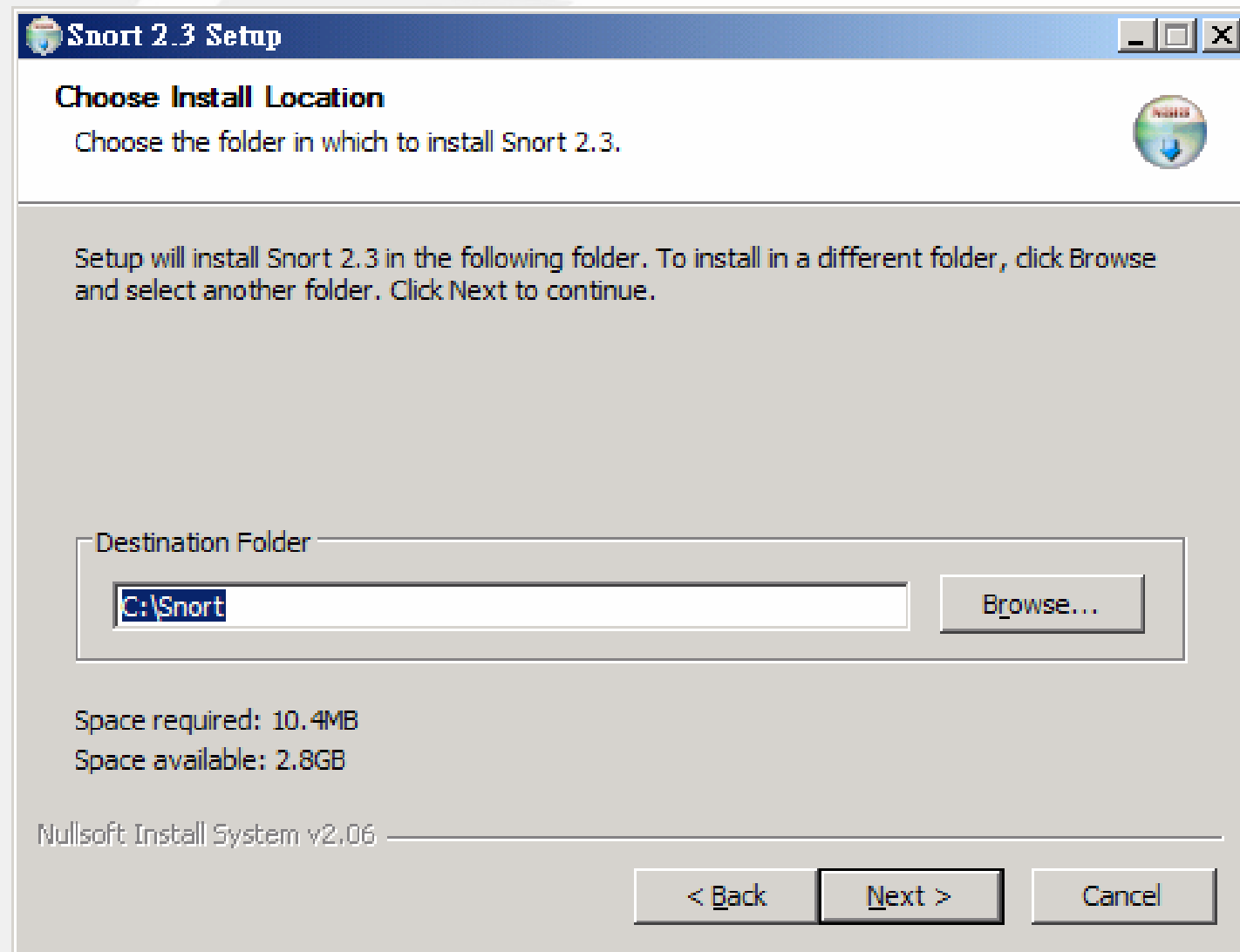
# Snort安裝-Windows

- **Snort + ACID**的組合安裝方式，在**Windows**系統上可以結合**Microsoft**的**IIS**網頁伺服器及**SQL Server**資料庫
- 本書介紹還是以**Windows XP**安裝使用開發原始碼的自由軟體為主，故仍比照**Linux**節所介紹的軟體來安裝
- 由於在**Windows**系統上安裝軟體十分容易，因此在安裝畫面就不逐一詳列講解，僅列出較重要的設定畫面供讀者參考
- 安裝版本檔案為**Snort\_233\_Build14\_Installer.exe**





# 將Snort的安裝目錄設定為C:\Snort

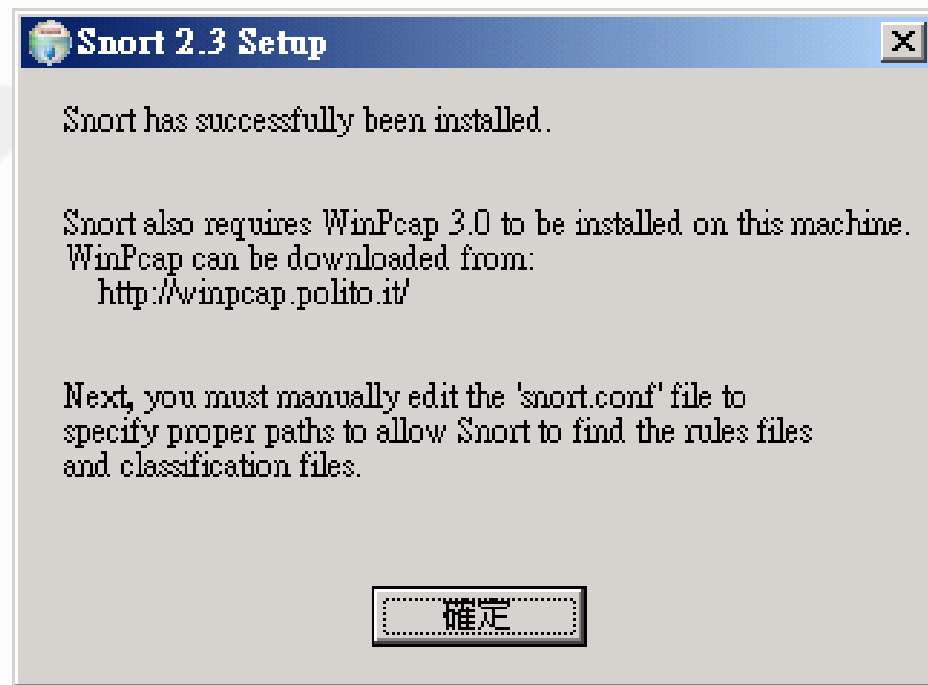






# Snort安裝完畢

- 安裝完之後，開啓C:\Snort\etc的snort.conf尋找並修改下列設定的屬性如下：
- var HOME\_NET 192.168.1.0/24
- var RULE\_PATH C:/Snort/rules
- output database: log, mysql,  
user=snort password=使用者自  
定密碼dbname=snort  
host=localhost
- include  
C:\Snort\etc\classification.config



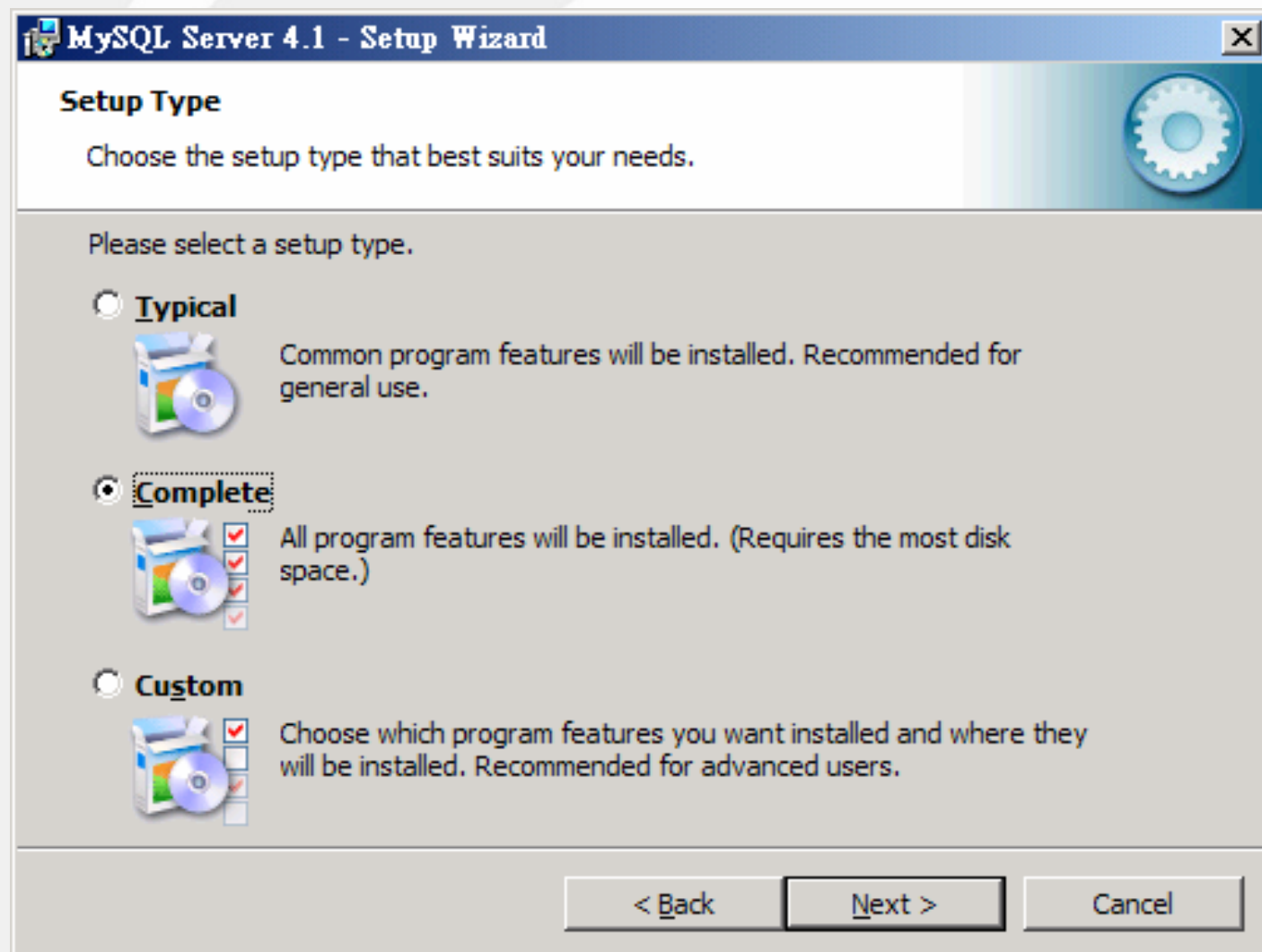


# WinPcap安裝

- 若系統為Snort2.3版，則需安裝WinPcap 3.0版
- 如果已經裝其他版本，請先移除後重新安裝
- 在裝完WinPcap 3.0版後務必先重新開機，否則系統不會生效



# MySQL安裝





MySQL.com Sign Up - Setup Wizard

**MySQL.com Sign-Up**

Login or create a new MySQL.com account.

Please log in or select the option to create a new account.

☐ **Create a new free MySQL.com account**

If you do not yet have a MySQL.com account, select this option and complete the following three steps.

☐ **Login to MySQL.com**

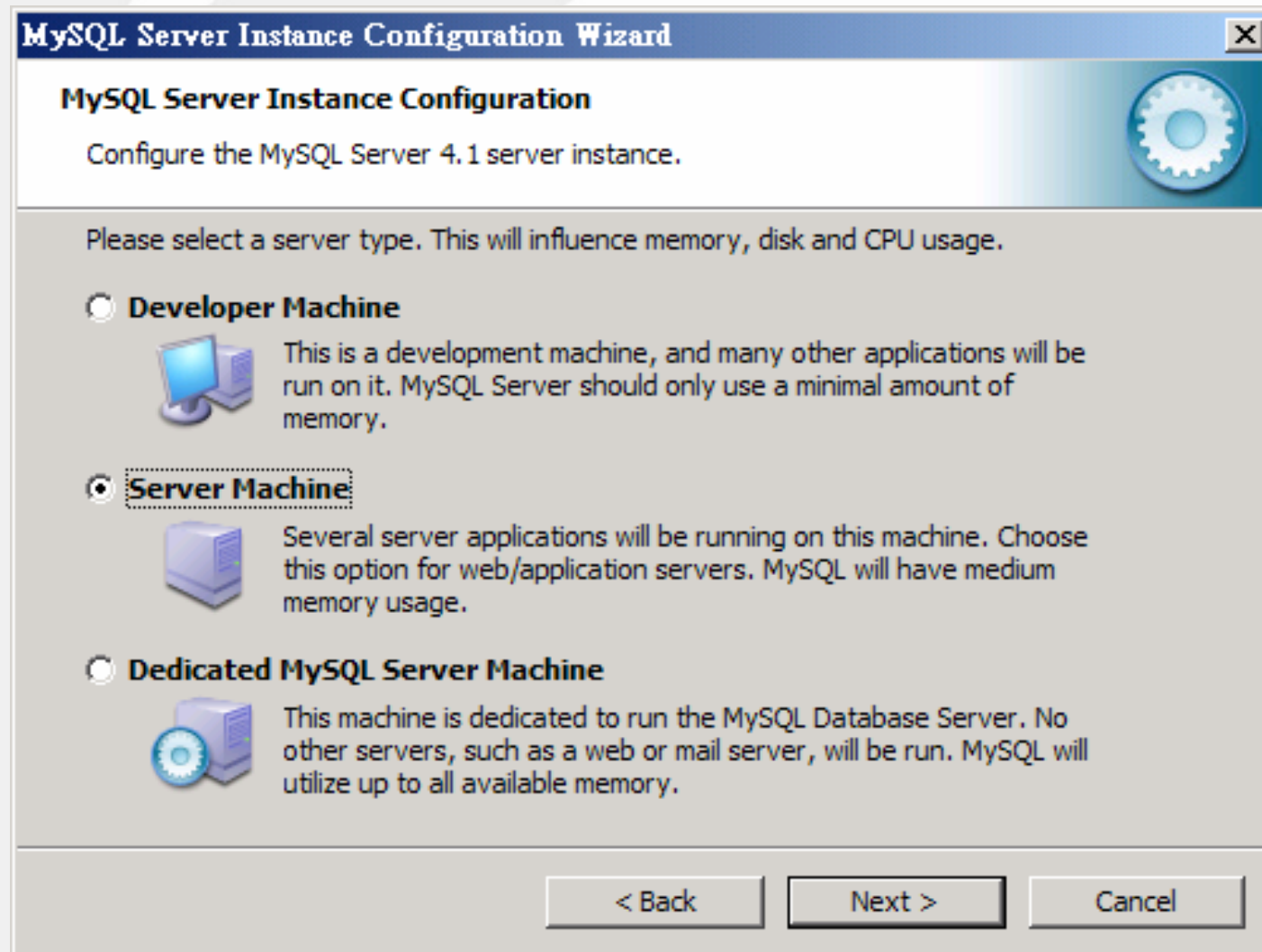
Select this option if you already have a MySQL.com account. Please specify your login information below.

Email address:

Password:

☒ **Skip Sign-Up**

Next > Cancel





# 設定同時可接受的連線數


**MySQL Server Instance Configuration Wizard**

**MySQL Server Instance Configuration**


Configure the MySQL Server 4.1 server instance.

Please set the approximate number of concurrent connections to the server.


☐ **Decision Support (DSS)/OLAP**

 Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed.

☐ **Online Transaction Processing (OLTP)**

 Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers.

☒ **Manual Setting**

 Please enter the approximate number of concurrent connections.

Concurrent connections:

< Back    Next >    Cancel




**MySQL Server Instance Configuration Wizard**

**MySQL Server Instance Configuration**


Configure the MySQL Server 4.1 server instance.

Please select the default character set.


☐ **Standard Character Set**

 Makes Latin1 the default charset. This character set is suited for English and other West European languages.

☐ **Best Support For Multilingualism**

 Make UTF8 the default character set. This is the recommended character set for storing text in many different languages.

☒ **Manual Selected Default Character Set / Collation**

 Please specify the character set to use.

Character Set:

< Back   Next >   Cancel



# [Include Bin Directory in Windows PATH]

金禾資訊

伴

您

學

習

成

長

的

每

一

天


**MySQL Server Instance Configuration Wizard**

**MySQL Server Instance Configuration**

Configure the MySQL Server 4.1 server instance.

Please set the Windows options.

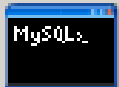
☒ **Install As Windows Service**

 This is the recommended way to run the MySQL server on Windows.

Service Name:

☐ Launch the MySQL Server automatically

☒ **Include Bin Directory in Windows PATH**

 Check this option to include the directory containing the server / client executables in the Windows PATH variable so they can be called from the command line.

< Back    Next >    Cancel






**MySQL Server Instance Configuration Wizard**


**MySQL Server Instance Configuration**

Configure the MySQL Server 4.1 server instance.

Please set the security options.


☒ **Modify Security Settings**

 New root password:  Enter the root password.

 Confirm:  Retype the password.

☐ Enable root access from remote machines

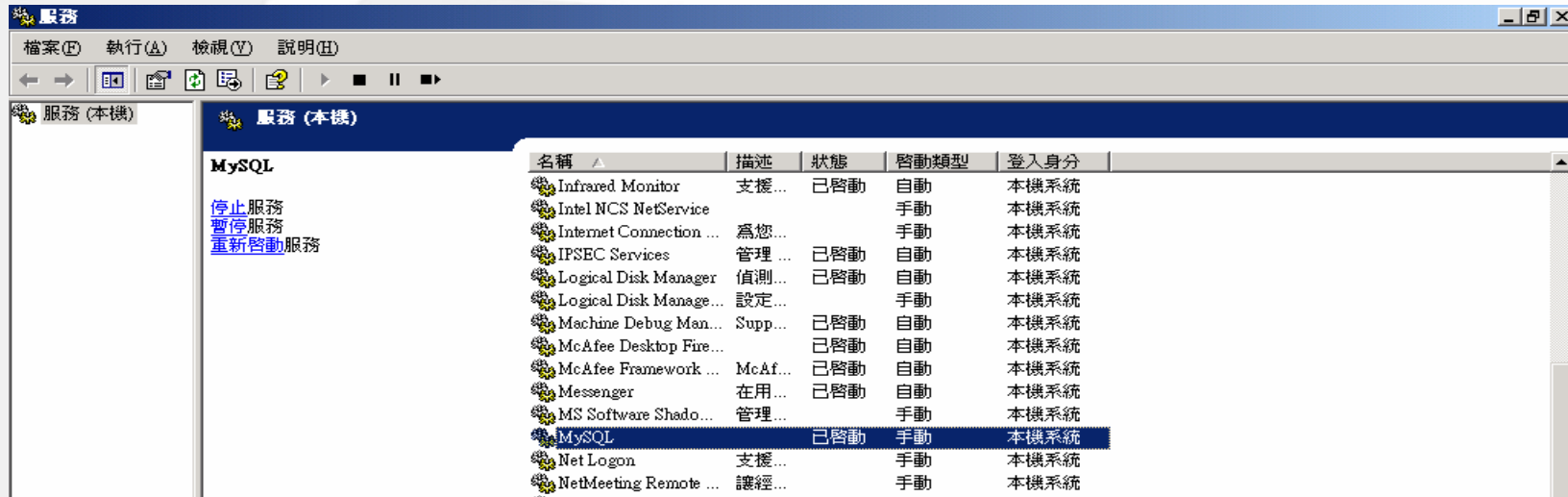
☐ **Create An Anonymous Account**

 This option will create an anonymous account on this server. Please note that this can lead to an insecure system.

< Back   Next >   Cancel



# 選取MySQL服務



- MySQL安裝完畢後，請開啓Windows XP的「服務」設定，將MySQL啓動，並設定爲自動啓動，以便在下次重新開機時就啓動MySQL服務



# 設定MySQL爲自動啓動

MySQL 內容 (本機電腦) ? X

一般 登入 修復 依存性

服務名稱: MySQL

顯示名稱(N): MySQL

描述(D):

執行檔所在路徑(H):  
"C:\Program Files\MySQL\MySQL Server 4.1\bin\mysqld-nt" --defaults-file:

啓動類型(E): 自動

服務狀態: 已啓動

啓動(S) 停止(T) 暫停(P) 繼續(R)

您可以在這裡指定啓動服務時所要套用的參數。

啓動參數(M):

確定 取消 套用(A)



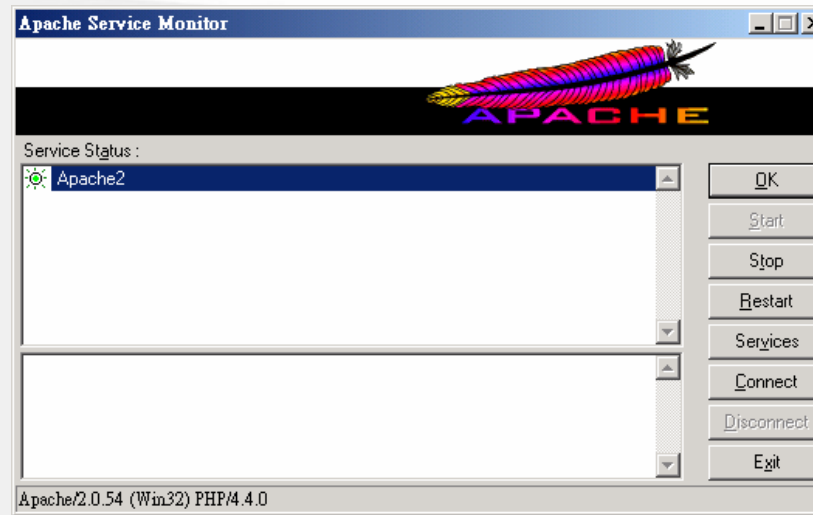
# 設定MySQL

- 安裝完成後，一樣必須設定資料庫，並新建snort資料庫及配置使用者權限；開啓MS-DOS命令視窗執行mysql以資料庫的root帳號登入，其預設密碼爲空白：
- `mysql -u root -p`  
登入後會出現mysql>，後續操作如下：  
`mysql> SET PASSWORD FOR root@localhost=PASSWORD("更改root密碼");`  
`mysql> create database snort;`  
`mysql> grant INSERT,SELECT on root.* to snort@localhost;`  
`mysql> SET PASSWORD FOR snort@localhost=PASSWORD("設定snort密碼");`  
`mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;`  
`mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;`  
`mysql> exit`
- 再以snort帳號登入，並建立snort資料庫的資料表：  
`mysql -u snort -p < C:\Snort\schemas\create_mysql snor`



# Apache+PHP

- **Apache**（建議安裝2.0.54版）：Apache網頁伺服器的安裝十分容易，不需特別變更設定，因此就不列出畫面，安裝完畢後應會立即啟動服務，並且自動於Windows XP的「服務」中設定自動於開機時啟動
- **PHP**（4.4.0版）：將PHP安裝在C:\Snort\php，安裝完畢時，須在php的目錄進行下列動作：
  - 將php4ts.dll複製到C:\WINDOWS\system32下
  - 將php.ini-dist複製到C:\WINDOWS下，並變更檔名為php.ini，開啓php.ini檔尋找並修改下列設定的屬性如下：
    - max\_execution\_time = 60
    - extension\_dir = "C:\Snort\php\extensions"
    - session.save\_path = "C:\Snort\php\sessiondata"
  - 在C:\Snort\php底下新增資料夾，命名為sessiondata，這是為ACID而設的。



- 在安裝完PHP後，切換到Apache預設的安裝目錄C:\Program Files\Apache Group\Apache2\conf開啓httpd.conf，並增加下列兩行設定：
  - LoadModule php4\_module "C:\Snort\php\sapi\php4apache2.dll"
  - AddType application/x-httpd-php .php
- 設定完畢之後，可以開啓Apache Service Monitor檢視服務狀態，如上圖



- 只需使用Tarball套件安裝時所用到的acid-0.9.6b23.tar.gz檔案即可，將該壓縮檔中所有檔案解壓縮至 C:\Program Files\Apache Group\Apache2\htdocs\acid，並開啓 acid\_conf.php 檔尋找並修改下列設定的屬性如下：
- ```
/* Path to the DB abstraction library */
$DBlib_path = "C:\Snort\php\adodb";
/* The type of underlying alert database */
$DBtype = "mysql";
/* Alert DB connection parameters */
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "之前設定的snort使用者密碼";
/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "之前設定的snort使用者密碼";
/* Path to the graphing library */
$ChartLib_path = "C:\Snort\php\jpgraph-1.19\src";
```





- 分別將adodb464.zip及jpgraph-1.19.tar.gz的檔案解壓縮到
  - C:\Snort\php\adodb
  - C:\Snort\php\jpgraph-1.19
- 接著開啓C:\Snort\php\jpgraph-1.19\src下的jpgraph.php檔，並增加一行設定如下：  
// For internal use only  
DEFINE("\_JPG\_DEBUG",false);  
DEFINE("\_FORCE\_IMGTOFILE",false);  
DEFINE("\_FORCE\_IMGDIR","/tmp/jpgimg/");  
**DEFINE("CACHE\_DIR", "/tmp/jpgraph\_cache");** //只要增加此行





# 安裝結果測試

- 無論是在Linux或是Windows系統上安裝，對於安裝後的測試，一律使用ACID來檢視
- 首先必須先確認系統的Apache、MySQL及Snort是處於啓動狀態
- 前面介紹在Linux安裝Snort時，已說明如何設定讓Snort在Linux開機時即啓動
- 在Windows底下，則可以開啓MS-DOS命令視窗輸入如下指令執行啓動Snort



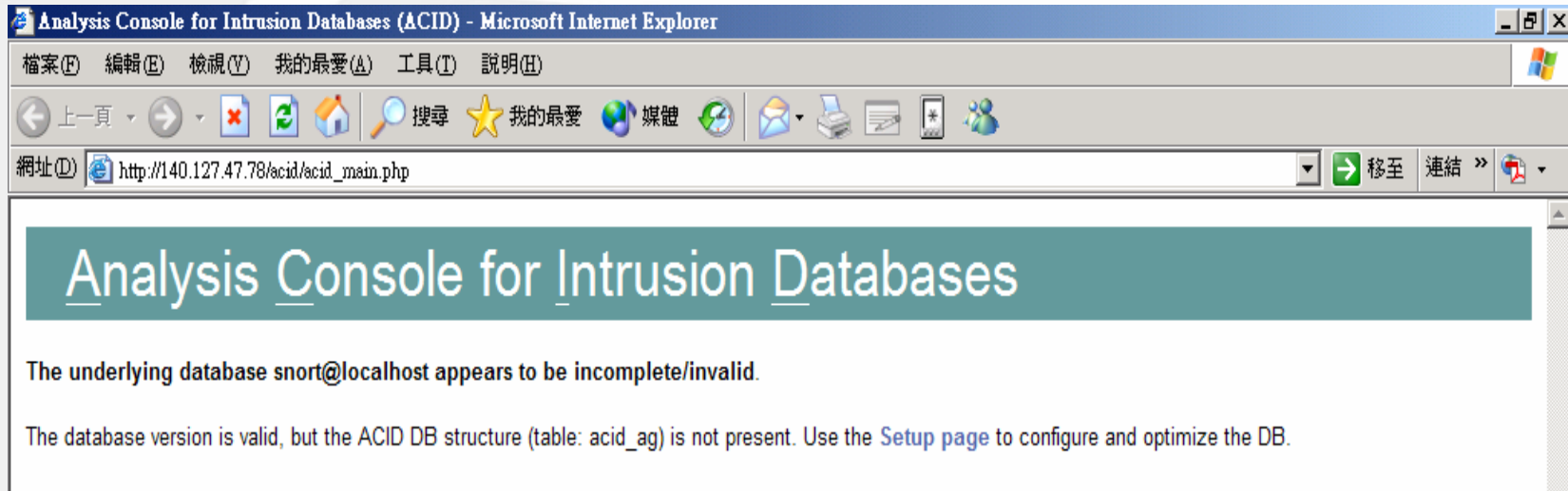
```
C:\WINDOWS\System32\cmd.exe - C:\Snort\bin\snort -c C:\Snort\etc\snort.conf -l C:\Snort\log -il
60
! gen-id=1      sig-id=2275      type=Threshold tracking=dst count=5  seconds=
60
! gen-id=1      sig-id=3152      type=Threshold tracking=src count=5  seconds=
2
! gen-id=1      sig-id=2924      type=Threshold tracking=dst count=10 seconds=
60
! gen-id=1      sig-id=2496      type=Both      tracking=dst count=20 seconds=
60
! gen-id=1      sig-id=3273      type=Threshold tracking=src count=5  seconds=
2
+-----[suppression]-----+
! none
+-----+
Rule application order: ->activation->dynamic->alert->pass->log
Log directory = C:\Snort\log

--- Initialization Complete ---

'''      -*> Snort! <*-
o"  >~    Version 2.3.3-ODBC-MySQL-FlexRESP-WIN32 (Build 14)
'''      By Martin Roesch & The Snort Team: http://www.snort.org/team.html
        (C) Copyright 1998-2004 Sourcefire Inc., et al.
```



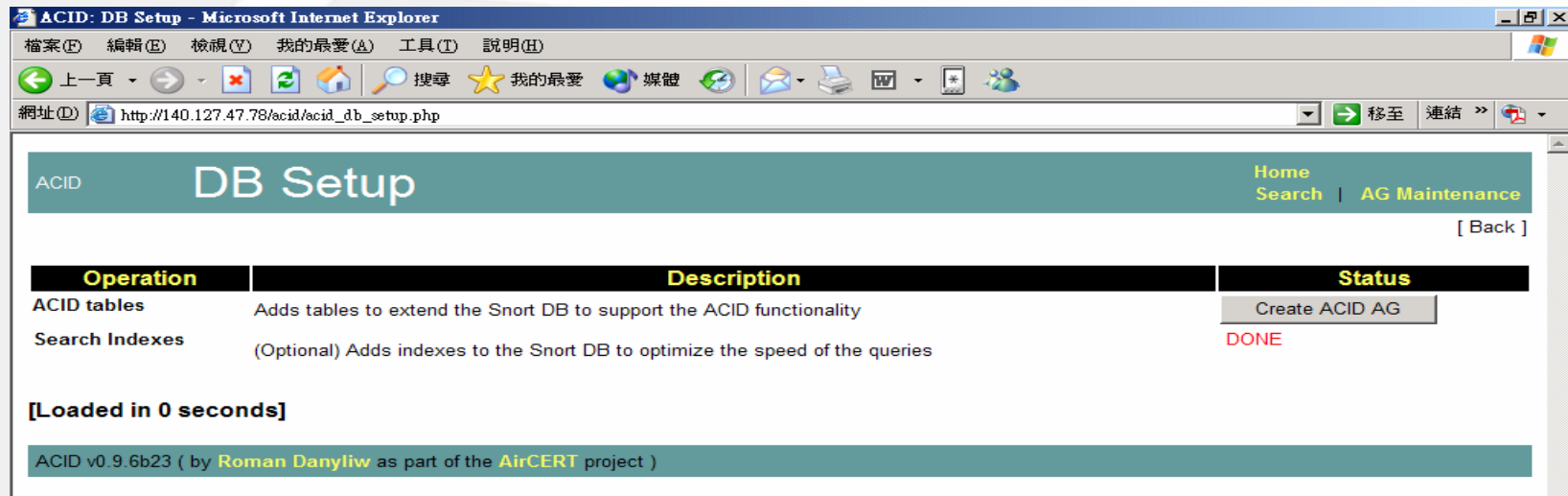
# ACID初始網頁



- 確定所需要的服務都啟動之後，開啓瀏覽器（如Microsoft Internet Explorer），在網址列中輸入：『http://安裝Snort的主機位址/acid/acid\_main.php』，應該會看到上圖



# ACID的資料庫設定網頁

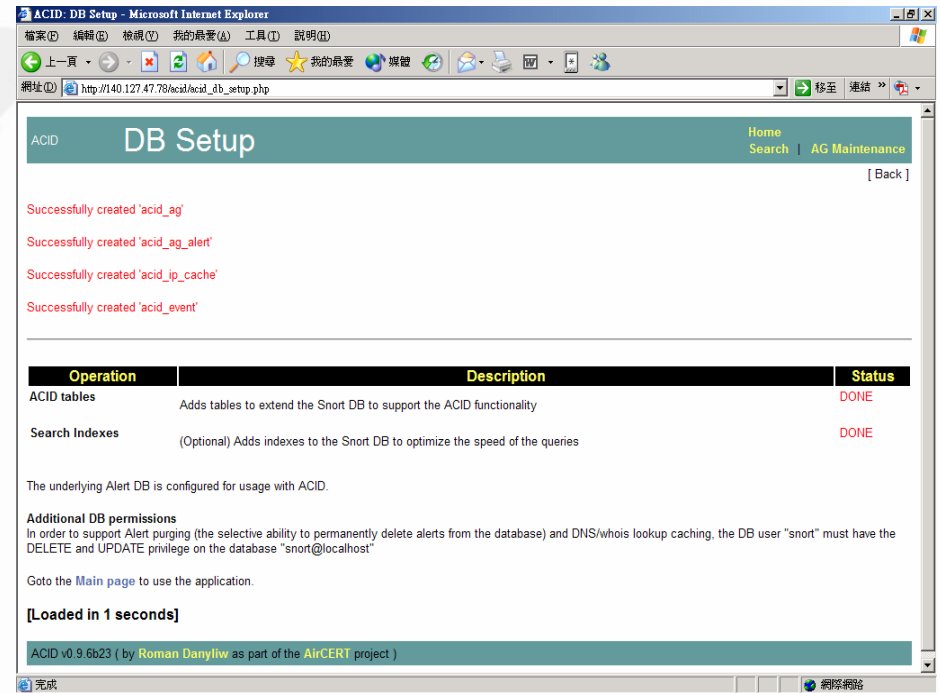


- 因為執行ACID所需要用到的資料表尚未建立，因此請點選“Setup page”超連結執行，如上圖



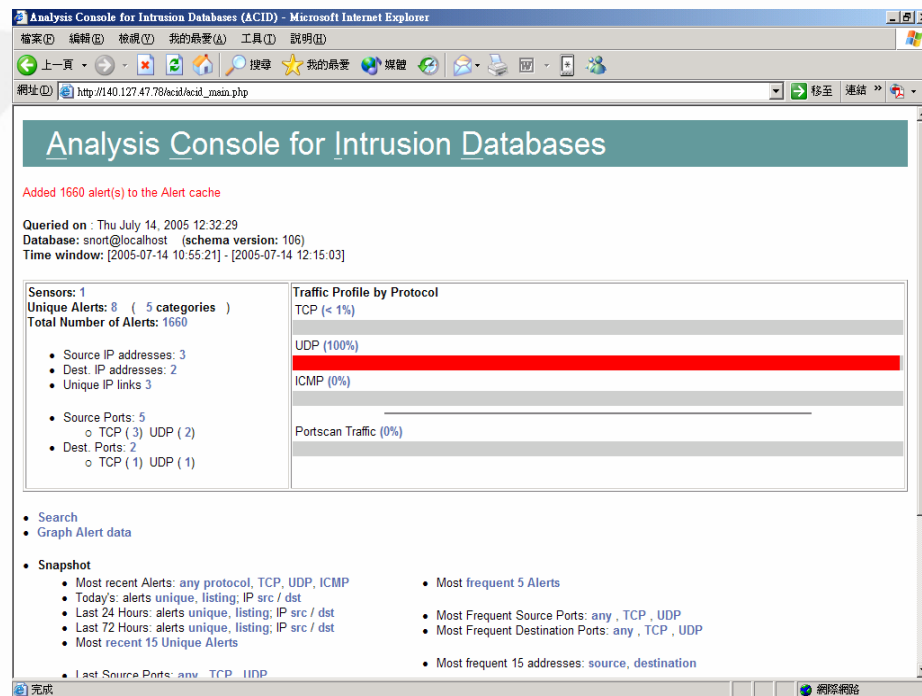
# 成功建立ACID資料表

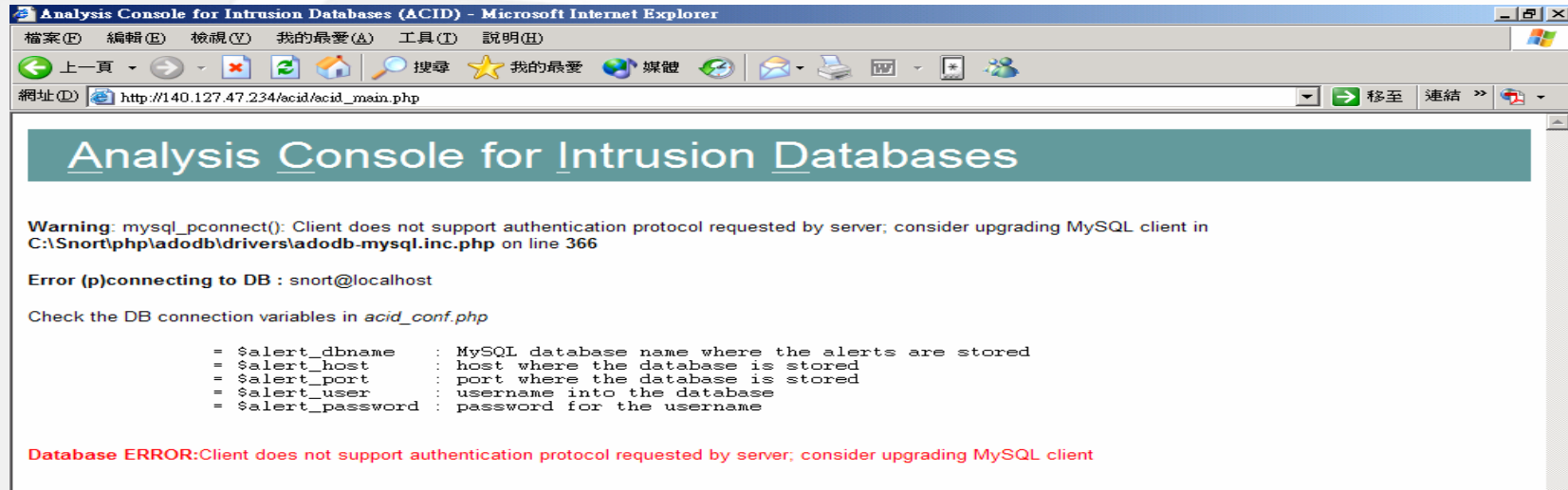
- 請點選 [Create ACID AG] 按鈕執行
- 在snort資料庫中建立ACID的資料表，執行成功的話，應如右圖





- ACID資料表建立完成後，再於網址列輸入：`http://安裝 Snort 的主機位址/acid/acid_main.php`，就能看到如右圖的主畫面





- 如果Snort是安裝在Windows系統，執行時很有可能會出現如上圖的錯誤畫面，這是因為MySQL4.0版以上的版本中更新密碼驗證機制之緣故。本書介紹Windows安裝的PHP4.4版內建的Client Library為3.23版，而必須安裝PHP5才有支援MySQL4.0版以上的Client Library，但由於ACID需使用JpGraph繪圖模組程式目前僅支援到PHP4，因此在使用PHP4時，要解決連線MySQL4.0以上版本的問題，所以可開啓MS-DOS命令視窗執行mysql，指令如下：
  - mysql -u root -p
- 登入後會出現mysql>，後續操作如下：
  - mysql> UPDATE mysql.user SET Password = **OLD\_PASSWORD**("使用者自定密碼")  
-> WHERE Host = "localhost" AND User = "snort";
  - mysql> FLUSH PRIVILEGES;
  - mysql> exit





- ACID套件是專為Snort設計的網頁操作介面
- 在Snort官方網站提供許多有關安裝Snort的文件，都會介紹如何安裝ACID
- 專門介紹Snort的書籍，也必定會談及ACID的應用
- ACID提供友善的網頁介面，使得系統管理者在檢索與管理入侵偵測資訊時更能得心應手
- 在介紹完Snort + ACID安裝之後，首先就藉由ACID來瞭解Snort的使用





Added 0 alert(s) to the Alert cache

Queried on : Sun July 17, 2005 10:52:20

Database: snort@localhost (schema version: 106)

Time window: [2005-07-14 10:55:21] - [2005-07-17 10:39:38]

Sensors: 1

Unique Alerts: 20 ( 7 categories )

Total Number of Alerts: 5000

- Source IP addresses: 321
- Dest. IP addresses: 16
- Unique IP links 342
- Source Ports: 657
  - TCP ( 635) UDP ( 23)
- Dest. Ports: 4
  - TCP ( 2) UDP ( 2)

Traffic Profile by Protocol

TCP (14%)

UDP (85%)

ICMP (1%)

Portscan Traffic (0%)

- ACID的主網頁畫面請參考上圖，是將ACID主網頁拆成二個部分作說明
- 使用者在實際操作使用ACID時，在網頁畫面上是淡藍色字體均是超連結，點選之後會顯示其相關資訊



# ACID主網頁-第一部分(說明)

- **Added 0 alert(s) to the Alert cache**：最新加入的警訊數量。
- **Queried on**：最新查詢的日期時間。
- **Database**：資料庫資訊，以「資料庫帳號@資料庫伺服器位址」表示。
- **Time windows**：ACID安裝之後使用迄今的起迄日期時間。
- **Sensors**（感應器的數量）：感應器指的就是Snort執行入侵偵測的網路連線裝置，如網路卡。
- **Unique Alerts: (categories)**：不重複的警訊及警訊種類數量。
- **Total Number of Alerts**：警訊的總數。
- **Source IP addresses**：封包的來源主機IP位址總數。
- **Dest. IP addresses**：封包的目的地主機IP位址總數。
- **Unique IP links**：不重複IP位址的連結數。
- **Source Ports**：封包來源主機IP位址的埠號數，可區分TCP及UDP檢視。
- **Dest. Ports**：封包目的地主機IP位址的埠號數，可區分TCP及UDP檢視。
- **Traffic Profile by Protocol**：將偵測到的封包區分協定統計，針對埠掃描的警訊另外計算，並依所佔比例繪製成長條圖顯示。



- [Search](#)
- [Graph Alert data](#)
- **Snapshot**
  - Most recent Alerts: [any protocol](#), [TCP](#), [UDP](#), [ICMP](#)
  - Today's: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
  - Last 24 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
  - Last 72 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
  - Most [recent 15 Unique Alerts](#)
  - Last Source Ports: [any](#) , [TCP](#) , [UDP](#)
  - Last Destination Ports: [any](#) , [TCP](#) , [UDP](#)
- [Graph alert detection time](#)
- [Alert Group \(AG\) maintenance](#)
- [Application cache and status](#)
- Most [frequent 5 Alerts](#)
- Most Frequent Source Ports: [any](#) , [TCP](#) , [UDP](#)
- Most Frequent Destination Ports: [any](#) , [TCP](#) , [UDP](#)
- Most frequent 15 addresses: [source](#), [destination](#)



# ACID主網頁-第二部分(說明)

- **Search**：使用複合條件查詢警訊資料。
- **Graph Alert data**：設定以統計圖方式呈現警訊記錄情況。
- **Most recent Alerts: any protocol, TCP, UDP, ICMP**（最新的警訊）：可全部檢視，或依封包協定類別區分TCP、UDP、ICMP檢視。
- **Today's: alerts unique, listing; IP src / dst**（今天的警訊）：可檢視不重複的警訊，或總覽警訊；亦可依來源/目的主機IP位址區分檢視。
- **Last 24 Hours: alerts unique, listing; IP src / dst**（最近24小時的警訊）：可檢視不重複的警訊，或總覽警訊；亦可依來源/目的主機IP位址區分檢視。
- **Last 72 Hours: alerts unique, listing; IP src / dst**（最近72小時的警訊）：可檢視不重複的警訊，或總覽警訊；亦可依來源/目的主機IP位址區分檢視。
- **Most recent 15 Unique Alerts**（最新15種不重複的警訊）
- **Last Source Ports: any, TCP, UDP**：最新警訊的來源位址埠號，可全部檢視，或依封包協定類別區分TCP、UDP檢視。



- Last Destination Ports: **any** , **TCP** , **UDP** : 最新警訊的目的位址埠號，可全部檢視，或依封包協定類別區分TCP、UDP檢視。
- Most frequent 5 Alerts (最頻繁的5種警訊)
- Most Frequent Source Ports: **any** , **TCP** , **UDP** : 最頻繁警訊的來源位址埠號，可全部檢視，或依封包協定類別區分TCP、UDP檢視。
- Most Frequent Destination Ports: **any** , **TCP** , **UDP** : 最頻繁警訊的目的位址埠號，可全部檢視，或依封包協定類別區分TCP、UDP檢視。
- Most frequent 15 addresses: **source**, **destination** (15個最頻繁警訊的位址) : 區分來源或目的位址檢視。
- Graph alert **detection time** : 設定起迄日期時間以統計圖方式呈現警訊偵測時間的記錄情況。
- Alert Group (AG) **maintenance** : 警訊群組的維護與管理。
- Application **cache and status** : 應用程式的資料快取管理與系統狀態檢視。



- 請注意**ACID**在安裝好之後，由於警訊查詢網頁的時間年份條件預設值是從**1999**年到**2004**年，且又不允許使用者在網頁上面直接輸入要查詢的年份，
- 故必須予以修改原始程式，而要修改的檔案為**acid\_state\_citems.inc**
- 以文字編輯器（如**vi**）開啓後找到如下頁上圖的程式片段，改成如下頁下圖所示，自安裝時年份起算逐一修改。此外，用以設定年份值的**<OPTION VALUE>HTML**的標籤亦可以自行視需要增減





## acid\_state\_citems.inc 修改前

## acid\_state\_citems.inc 修改後



# 警訊查詢網頁

- 系統管理者可設定查詢警訊的條件（如右圖）
- 其設定條件的方式相當有彈性，在畫面上的[ADD ...]按鈕都可讓使用者自行增設條件
- 如[ADD Time]增設查詢不同的起迄日期時間，或[ADD IP Field]增設查詢其他的封包欄位資訊...等

The screenshot shows the 'ACID: Query Results' web interface in a Microsoft Internet Explorer browser. The page title is 'ACID: Query Results' and the URL is 'http://140.127.47.78/acid/acid\_qry\_main.php?new=1'. The interface includes a navigation bar with 'Home', 'Search', and 'AG Maintenance' links. Below the navigation bar, there is a status message: 'Added 0 alert(s) to the Alert cache'. The main content area is divided into several sections for defining search criteria:

- Meta Criteria:** Includes fields for 'Sensor' (dropdown), 'Alert Group' (dropdown), 'Signature' (text input), 'Classification' (dropdown), 'Priority' (dropdown), and 'Alert Time' (date and time pickers). There is an 'ADD Time' button.
- IP Criteria:** Includes fields for 'Address' (text input), 'Misc' (text input), and 'Layer-4' (dropdown with options TCP, UDP, ICMP). There are 'ADD Addr' and 'ADD IP Field' buttons.
- Payload Criteria:** Includes fields for 'Input Criteria Encoding Type' (dropdown), 'Convert To (when searching)' (dropdown), and 'payload' (text input). There is an 'ADD Payload' button.

At the bottom of the form, there is a 'Sort order' section with radio buttons for 'none', 'timestamp (ascend)', 'timestamp (descend)', and 'signature'. A 'Query DB' button is located at the bottom right of the form.





## 警訊查詢結果網頁

ACID: Query Results - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://140.127.47.78/acid/acid\_qry\_main.php 移至 連結 »

## ACID Query Results

Home Search | AG Maintenance [ Back ]

Added 0 alert(s) to the Alert cache

Queried DB on : Sun July 17, 2005 12:19:33

|                         |                                             |
|-------------------------|---------------------------------------------|
| <b>Meta Criteria</b>    | Sensor = [1] 140.127.47.78:eth0 ...clear... |
| <b>IP Criteria</b>      | any                                         |
| <b>Layer 4 Criteria</b> | none                                        |
| <b>Payload Criteria</b> | any                                         |

**Summary Statistics**

- Sensors
- Unique Alerts ( classifications )
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-50 of 5000 total

| <input type="checkbox"/> | ID       | < Signature >                                                               | < Timestamp >       | < Source Address >  | < Dest. Address >    | < Layer 4 Proto > |
|--------------------------|----------|-----------------------------------------------------------------------------|---------------------|---------------------|----------------------|-------------------|
| <input type="checkbox"/> | #0-(1-1) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #1-(1-2) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #2-(1-3) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #3-(1-4) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #4-(1-5) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #5-(1-6) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #6-(1-7) | url[cve][icat][cve][icat][bugtraq][snort] MISC UPnP malformed advertisement | 2005-07-14 10:55:21 | 140.127.47.226:1900 | 239.255.255.250:1900 | UDP               |

國際網路



# 警訊統計圖

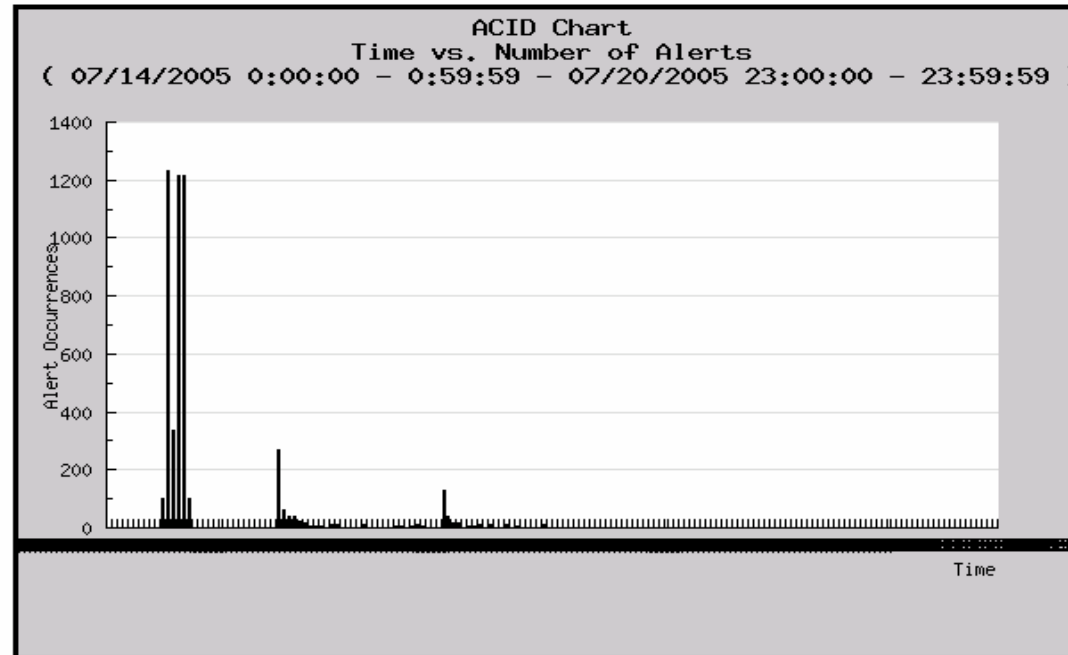
- 從主網頁點選可以檢視警訊統計圖的功能網頁有兩個：
- **Graph Alert data**：可以指定所要呈現的統計圖大小、類型、座標邊界，並設定警訊群組及資料的起迄日期時間...等條件。
- **Graph alert detection time**：只能設定起迄日期時間呈現警訊偵測時間的記錄情況，而且不能設定統計圖的大小、類型、警訊群組...等其他條件。



| Chart Title: <input type="text" value="ACID Chart"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|--------|--------|----------------------------------------------------------------|---------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------|--|-------------------------------------------------|--|-----------------------------------------------------------------------|--|
| Chart Type: <input type="text" value="Time (hour) vs. Number of Alerts"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Chart Period: <input type="text" value="no period"/>       |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Size: (width x height) <input type="text" value="600"/> x <input type="text" value="400"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Plot Margins: (left x right x top x bottom) <input type="text" value="50"/> x <input type="text" value="50"/> x <input type="text" value="70"/> x <input type="text" value="80"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Plot type: <input checked="" type="radio"/> bar <input type="radio"/> line <input type="radio"/> pie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Chart Begin: <input type="text" value="0"/> <input type="text" value="10"/> <input type="text" value="July"/> <input type="text" value="2005"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Chart End: <input type="text" value="0"/> <input type="text" value="20"/> <input type="text" value="July"/> <input type="text" value="2005"/> <input type="button" value="Graph Alerts"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| <table border="1"><thead><tr><th>X Axis</th><th>Y Axis</th></tr></thead><tbody><tr><td>Data Source: <input type="text" value="{ data source (AG) }"/></td><td><input type="checkbox"/> Y-axis logarithmic</td></tr><tr><td>Minimum Threshold Value ( &gt;= ): <input type="text" value="0"/></td><td><input checked="" type="checkbox"/> Show Y-axis grid-lines</td></tr><tr><td><input type="checkbox"/> Rotate Axis Labels (90 degrees)</td><td></td></tr><tr><td><input type="checkbox"/> Show X-axis grid-lines</td><td></td></tr><tr><td>Display X-axis label every <input type="text" value="1"/> data points</td><td></td></tr></tbody></table> |                                                            | X Axis | Y Axis | Data Source: <input type="text" value="{ data source (AG) }"/> | <input type="checkbox"/> Y-axis logarithmic | Minimum Threshold Value ( >= ): <input type="text" value="0"/> | <input checked="" type="checkbox"/> Show Y-axis grid-lines | <input type="checkbox"/> Rotate Axis Labels (90 degrees) |  | <input type="checkbox"/> Show X-axis grid-lines |  | Display X-axis label every <input type="text" value="1"/> data points |  |
| X Axis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Y Axis                                                     |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Data Source: <input type="text" value="{ data source (AG) }"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <input type="checkbox"/> Y-axis logarithmic                |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Minimum Threshold Value ( >= ): <input type="text" value="0"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <input checked="" type="checkbox"/> Show Y-axis grid-lines |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| <input type="checkbox"/> Rotate Axis Labels (90 degrees)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| <input type="checkbox"/> Show X-axis grid-lines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |
| Display X-axis label every <input type="text" value="1"/> data points                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                            |        |        |                                                                |                                             |                                                                |                                                            |                                                          |  |                                                 |  |                                                                       |  |



No AG was specified. Using all alerts.





# Graph alert detection time統計圖的測試結果

金禾資訊

伴

您

學

習

成

長

的

每

一

天

Queried DB on : Sun July 17, 2005 12:58:58

|                  |      |
|------------------|------|
| Meta Criteria    | any  |
| IP Criteria      | any  |
| Layer 4 Criteria | none |
| Payload Criteria | any  |

Added 0 alert(s) to the Alert cache

## Time Criteria

Profile by : ☐ Hour ☒ Day ☐ Month

between    --

| Time       | # of Alerts | Alerts      |
|------------|-------------|-------------|
| 07/15/2005 | 489         | <div></div> |
| 07/16/2005 | 276         | <div></div> |
| 07/17/2005 | 42          | <div></div> |



# 警訊群組管理

- 警訊群組主要是讓系統管理者對於**Snort**所發出的警訊做有效的管理
- 如何管理，其實端看系統管理者本身的喜好或需求，也可以依封包類型、警訊類型或起迄的日期時間等來設定群組以分開管理
- 通常警訊群組的管理會配合查詢網頁來將警訊分類歸納



ACID Alert Group (AG) Maintenance [Home](#) [Search](#) | [AG Maintenance](#) [\[ Back \]](#)

[list all](#) | [create](#) | [view](#) | [edit](#) | [delete](#) | [clear](#)

---

Create group

|             |                                                  |
|-------------|--------------------------------------------------|
| ID #        | not assigned yet                                 |
| Name        | <input type="text" value="AG_netscan"/>          |
| Description | <input type="text" value="network-scan alerts"/> |

- 首先建立一個群組名為AG\_netscan，準備用來儲存偵測網路掃描攻擊的警訊，如上圖
- 再來執行查詢所有的網路掃描警訊，開啓查詢網頁，將 **[Signature:]** 資訊的 **[Classification:]** 欄位條件設為 "network-scan"，其餘條件不用更改



## network-scan 類型警訊查詢結果

ACID
Query Results
Home  
Search | AG Maintenance
[ Back ]

Added 2 alert(s) to the Alert cache

Queried DB on : Sun July 17, 2005 15:55:00

**Meta Criteria**  
**IP Criteria**  
**Layer 4 Criteria**  
**Payload Criteria**

Signature Classification = network-scan ...clear...  
any  
none  
any

**Summary Statistics**

- Sensors
- Unique Alerts ( classifications )
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-50 of 75 total

| <input type="checkbox"/> | ID          | < Signature >                              | < Timestamp >       | < Source Address >  | < Dest. Address >    | < Layer 4 Proto > |
|--------------------------|-------------|--------------------------------------------|---------------------|---------------------|----------------------|-------------------|
| <input type="checkbox"/> | #0-(1-250)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:25 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #1-(1-251)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:28 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #2-(1-252)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:31 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #3-(1-1662) | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:39 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #4-(1-1663) | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:42 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #5-(1-1664) | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:45 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #6-(1-1665) | [snort] SCAN UPnP service discover attempt | 2005-07-14 13:00:29 | 140.127.47.226:1523 | 239.255.255.250:1900 | UDP               |



|                                     |              |                                            |                     |                     |                      |     |
|-------------------------------------|--------------|--------------------------------------------|---------------------|---------------------|----------------------|-----|
| <input checked="" type="checkbox"/> | #45-(1.4727) | [snort] SCAN UPnP service discover attempt | 2005-07-16 10:50:33 | 140.127.47.205:1033 | 239.255.255.250:1900 | UDP |
| <input checked="" type="checkbox"/> | #46-(1.4728) | [snort] SCAN UPnP service discover attempt | 2005-07-16 10:50:36 | 140.127.47.205:1033 | 239.255.255.250:1900 | UDP |
| <input checked="" type="checkbox"/> | #47-(1.4729) | [snort] SCAN UPnP service discover attempt | 2005-07-16 10:53:49 | 140.127.47.205:1034 | 239.255.255.250:1900 | UDP |
| <input checked="" type="checkbox"/> | #48-(1.4730) | [snort] SCAN UPnP service discover attempt | 2005-07-16 10:53:52 | 140.127.47.205:1034 | 239.255.255.250:1900 | UDP |
| <input checked="" type="checkbox"/> | #49-(1.4731) | [snort] SCAN UPnP service discover attempt | 2005-07-16 10:53:55 | 140.127.47.205:1034 | 239.255.255.250:1900 | UDP |

Query Results  
[0] 1

Action

Add to AG (by Name)

- 選取想要加入群組的警訊，再移至網頁最下方，於[Action]設定的第一個欄位設為Add by AG (by Name)
- 在第二個欄位則設定警訊群組的名稱，如AG\_netscan，最後按下[Selected]按鈕執行，如上圖



## View group

|             |                     |
|-------------|---------------------|
| ID #        | 3                   |
| Name        | AG_netscan          |
| Description | network-scan alerts |

Displaying alerts 1-50 of 50 total

| <input type="checkbox"/> | ID           | < Signature >                              | < Timestamp >       | < Source Address >  | < Dest. Address >    | < Layer 4 Proto > |
|--------------------------|--------------|--------------------------------------------|---------------------|---------------------|----------------------|-------------------|
| <input type="checkbox"/> | #0-(1-250)   | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:25 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #1-(1-251)   | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:28 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #2-(1-252)   | [snort] SCAN UPnP service discover attempt | 2005-07-14 11:05:31 | 140.127.47.226:1033 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #3-(1-1662)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:39 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #4-(1-1663)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:42 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #5-(1-1664)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 12:40:45 | 140.127.47.205:3014 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #6-(1-1665)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 13:00:29 | 140.127.47.226:1523 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #7-(1-1666)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 13:00:29 | 140.127.47.226:1527 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #8-(1-1717)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 13:00:32 | 140.127.47.226:1527 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #9-(1-1758)  | [snort] SCAN UPnP service discover attempt | 2005-07-14 13:00:35 | 140.127.47.226:1527 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #10-(1-2979) | [snort] SCAN UPnP service discover attempt | 2005-07-14 14:03:18 | 140.127.47.205:3006 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #11-(1-2980) | [snort] SCAN UPnP service discover attempt | 2005-07-14 14:03:21 | 140.127.47.205:3006 | 239.255.255.250:1900 | UDP               |
| <input type="checkbox"/> | #12-(1-2981) | [snort] SCAN UPnP service discover attempt | 2005-07-14 14:03:24 | 140.127.47.205:3006 | 239.255.255.250:1900 | UDP               |

- 最後來檢視一下AG\_netscan警訊群組，如上圖，總共已加入**50**筆警訊資料，若系統管理者如果能利用警訊群組善加分類管理，才能真正發揮ACID的優點



# 關於ACID

- 以上簡要說明ACID的使用方式，仍還有許多尚未介紹的警訊管理功能網頁，且ACID的功能豐富、操作簡單，讀者可自行測試其他的網頁功能
- ACID最重要的功能還是警訊查詢及群組管理，因此[Search]與[AG Maintenance]這兩個功能網頁的連結均固定在網頁的右上方，以便於系統管理者隨時做好警訊管理
- 若是長期使用的話，會損耗系統本身的效能，尤其是入侵動作過於頻繁的話，由於會不斷執行資料庫讀寫的動作，勢必將大幅增加系統負擔
- 如果想要擁有網頁介面管理的便利性，同時亦欲稍微減輕系統的負擔，可以考慮改用BASE（Basic Analysis and Security Engine）套件，而BASE是ACID的精簡版



# Snort指令

- Snort有三種運作模式，分別是：
  - 嗅探器模式
  - 封包記錄器模式
  - 網路入侵偵測系統（**NIDS**）模式
- 對於系統管理者而言，雖然使用**ACID**的網頁介面來檢視並管理入侵偵測的資訊較為方便，然而瞭解相關指令仍有其必要性，下面就區分**Snort**三個運作模式講解基本指令的操作



# 嗅探器模式的指令

- 啓用嗅探器模式，**Snort**會讀取在網路上傳送的封包資訊，並連續顯示在終端機畫面上，若只須列出**TCP/IP**封包標頭資訊，則輸入下列指令即可：
  - **snort -v**
- **-v**選項只會顯示**IP**、**TCP**、**UDP**及**ICMP**等封包的標頭資訊，若要檢視應用層傳輸的資料內容，請加入**-d**選項；檢視資料連結層的資訊則加入**-e**選項，如下列指令：
  - **snort -d -e -v**
- 上述指令也可僅用一個**"-"**符號同時設定，如下：
  - **snort -dev**
- 使用嗅探器模式時由於封包資訊會不斷地顯示在終端機畫面，如果要中斷執行的話，只要按下**Ctrl+C**即可。





# 封包記錄器模式的指令

- 啓用封包記錄器模式，會將**Snort**讀取到的網路封包儲存在硬碟中，通常需要利用選項**-l**來指定一個**log**目錄（名稱自訂）儲存，指令如下：
  - **snort -dev -l ./log**
- **log**目錄必須事先建立好，否則**Snort**就會顯示錯誤訊息而無法儲存
- 執行封包儲存時，**Snort**會將所接收到的封包依其外部的**IP**位址（即封包接收端的目的主機位址）分類，並在指定的**log**目錄底下，以外部**IP**位址作為名稱再建立子目錄，並儲存目的主機位址相同的封包資訊



# log目錄依封包外部IP位址建立子目錄並儲存

金禾資訊

伴

您

學

習

成

長

的

每

一

天

```
[root@icebug ~]# ls log/
140.127.47.213  140.127.47.66    218.172.58.111  59.113.74.128  ARP
140.127.47.253  140.127.47.78    220.160.117.210  61.185.14.197  PACKET_NONIP
140.127.47.6    210.76.112.198   255.255.255.255  62.121.67.182
140.127.47.65   218.162.199.185  38.113.196.52    62.174.211.92
[root@icebug ~]#
```

- Snort有時會使用遠端主機IP位址作為目錄名稱，而有時又以本地網路的主機IP位址為目錄命名。若加上-h選項的指令，便可令Snort僅記錄本地網路之封包資訊
  - snort -dev -l ./log -h 192.168.1.0/24
- 上述指令意思是將進入192.168.1這個C級網路所有的TCP/IP、資料連結層、應用層的封包資訊儲存到log目錄下；-h選項後面指定的位址須是CIDR（Classless Inter-Domain Routing）位址



```
[root@icebug ~]# ls log/  
snort.log.1121501111  
[root@icebug ~]#
```

- 以上的封包記錄指令，都是將封包資訊儲存成**ASCII**編碼檔，如果要儲存成相容於**tcpdump**或**Ethereal**可以讀取的**tcpdump**二進位格式檔，可以指定**-b**選項，其操作指令如下：
  - snort -l ./log -b
- 使用**-b**選項的話，所有封包及封包中全部的內容都會儲存在一個**tcpdump**二進位檔案中，不需要另外再設定**-d**、**-e**或**-v**選項，如上圖所示，而執行上述指令測試封包記錄儲存的日誌檔名稱爲**snort.log.1121501111**





```
Breakdown by protocol:
  TCP: 104          (14.900%)
  UDP: 266          (38.109%)
  ICMP: 29          (4.155%)
  ARP: 92           (13.181%)
  EAPOL: 0          (0.000%)
  IPv6: 11          (1.576%)
  IPX: 0            (0.000%)
  OTHER: 196        (28.080%)
  DISCARD: 0        (0.000%)
```

```
=====
Action Stats:
```

```
ALERTS: 0
LOGGED: 0
PASSED: 0
```

```
=====
Snort exiting
```

```
[root@icebug log]#
```

- 要檢視該日誌檔的資訊則使用-r選項，將其內容顯示在終端機畫面，指令如下：**snort -r** 日誌檔名稱（如 **snort.log.1121501111**）
- 指定顯示不同層協定的封包，可以選擇加上-d、-e或-v選項：**snort -dv -r** 日誌檔名稱測試的顯示結果如上圖



```
Breakdown by protocol:
  TCP: 104          (100.000%)
  UDP: 0            (0.000%)
  ICMP: 0           (0.000%)
  ARP: 0            (0.000%)
  EAPOL: 0          (0.000%)
  IPv6: 0           (0.000%)
  IPX: 0            (0.000%)
  OTHER: 0          (0.000%)
  DISCARD: 0        (0.000%)
=====
Action Stats:
ALERTS: 0
LOGGED: 0
PASSED: 0
=====
Snort exiting
[root@icebug log]#
```

- 要指定顯示的封包種類，如TCP封包，指令：『snort -dv -r』日誌檔名稱 **tcp**，測試檔案的顯示結果共記錄104個TCP封包，如上圖



# 將讀取資料存成ASCII編碼的純文字檔

- 由於在終端機螢幕顯示從tcpdump格式檔讀出的內容，不方便日後再作檢視或查詢，所以能利用下列指令將讀取資料存成ASCII編碼的純文字檔：
  - snort -r 日誌檔名稱 > snort.log.asc
- Snort在任何運作模式都可以操作存取tcpdump二進位格式的日誌檔，但因為此種格式的檔案記錄相當詳細，所以對系統的負擔較重，若非Snort主機是位於高速網路的環境或系統管理者認為有其必要詳實記錄以便日後分析之用，否則建議要慎重考慮使用**-b**選項來記錄封包資訊



# NIDS模式的指令

- 作為網路入侵偵測系統是**Snort**最重要的用途，要設定**Snort**執行入侵偵測的功能，必須要以**-c**選項來指定設定檔，其預設的檔案是**snort.conf**
- **snort.conf**檔會包含有關入侵偵測的各項設定，系統管理者只需依自己的需求加以調整



## NIDS模式的指令(續)

- 指定規則集的所在路徑也必須於**snort.conf**中修改，使用者可以定義多個不同的設定檔，只要在操作時指定要用的設定檔即可，其指令如下：
  - **snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf**
- 如果要使用**Snort**長期記錄入侵偵測資訊，應省略一些選項避免記錄到不太需要的資訊，同時也可減輕**Snort**主機負擔，並加快**Snort**的處理速度，通常需要記錄供作日後分析使用的就是應用層封包而已，因此一般設定啟動**Snort**的入侵偵測服務時，可以省略**-ev**兩個選項，只需輸入下列指令即可：
  - **snort -d -l ./log -h 192.168.1.0/24 -c snort.conf**



# NIDS的報警機制

- Snort執行NIDS時，有6種報警機制可以設定，其中有4種是使用-A選項配合參數使用，說明如下：
- -A fast（快速報警模式）：報警資訊的格式較單純，僅包含一個時間戳、警告訊息、封包的來源/目的主機位址及埠號等
- -A full（完整報警模式）：為預設選項，未做任何報警機制設定時，即自動選用此參數
- -A unsock（將報警資訊傳遞給另一個 Unix Socket）：該Socket需要執行一支程式進行傾聽，以便能夠即時報警
- -A none（關閉報警機制）





# NIDS的報警機制(續)

- 另外2種報警機制便是將報警資訊傳送到syslog或透過Samba的smbclient傳輸至Windows系統的WinPopup程式報警
- -s（傳送報警資訊到syslog）：Linux系統預設的接收檔案為/var/log/secure，其他的Unix-like系統可能記錄在/var/log/messages
- -M（經由smbclient將報警資訊傳送到Windows系統）：要使用這個功能，必須要以Tarball套件來安裝Snort，且在執行./configure編譯步驟時，附加--enable-smbalerts選項，否則無法執行此選項



- Snort在Linux開機時即時自動啓動，在該Snort啓動檔中，加入一行指令如下：  
– `/usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g snort &`
- `-i`選項是指定Snort執行嗅探封包功能時，所使用的網路連線裝置（如網路卡）
- `-g`選項的g代表群組（Group），在Snort以root權限初始化完畢後，便將後續作業的執行權限卸交給指定的群組使用者，如snort
- 以上就是在安裝Snort前，要先新增一個snort群組及snort使用者帳號，並將snort使用者指定給snort群組的原因





- 前置處理器（Preprocessor）是從Snort 1.5版以後開始引進的機制
- 使得Snort容易增加其他功能，無論是使用者或是程式開發人員都可以利用此機制將模組化的套件與Snort主程式結合，以擴展Snort運行之系統
- 前置處理器的動作是在網路封包解碼之後，入侵偵測引擎啟動之前



# 配置前置處理器

- 要配置前置處理器就是利用**preprocessor**關鍵字在**snort.conf**檔中作設定，其指令格式如下：
  - `preprocessor <name_of_processor>: <configuration_options>`
- 通常配置前置處理器的作用有三：
  - （一）重組封包
  - （二）處理協定解碼
  - （三）偵測不規則或不正常的攻擊動作



# preprocessor的配置範例及作用

- **preprocessor frag2**
  - 提供IP碎片重組及偵測碎片攻擊，使用的記憶體為預設值4MB，碎片時間逾時值預設為30秒。
- **preprocessor stream4: detect\_scans**
  - 若偵測到隱蔽掃描，將會發出警告。
- **preprocessor http\_decode: 80 -unicode -cginull**
  - 制止發出因CGI Null攻擊及IIS Unicode攻擊所產生的警報。
- **preprocessor bo**
  - 偵測Back Orifice流量，Back Orifice是相當著名的特洛伊木馬後門程式
- 其實在Snort入侵偵測設定檔snort.conf中，就已經包含各個前置處理器的介紹、選項及使用說明



- ACID (Analysis Console for Intrusion Databases),  
<http://www.cert.org/kb/acid/>
- BASE (Basic Analysis and Security Engine),  
<http://secureideas.sourceforge.net/>
- Brian Caswell, Jay Beale, Toby Kohlenberg, *Snort 2.1 Intrusion Detection Second Edition*, SYNGRESS, 2004
- Bert Hayes, Charlie Scott, Paul Wolfe, *Snort For Dummies*, WILEY, 2004
- Christina Neal, “Snort Install on Win2000/XP with Acid, and MySQL”,  
<http://www.sans.org/rr/whitepapers/detection/362.php>
- Patrick Harper, “Snort, Apache, SSL, PHP, MySQL, and BASE Install on Fedora Core 3”,  
[http://www.ntsug.org/docs/snort\\_base\\_fc3.pdf](http://www.ntsug.org/docs/snort_base_fc3.pdf)
- Roman Danyliw, “ACID: Installation and Configuration”,  
[http://www.andrew.cmu.edu/user/rdanyliw/snort/acid\\_config.html](http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_config.html)
- SnortUsers Manual 2.3.3,  
[http://www.snort.org/docs/snort\\_htmanuals/htmanual\\_233/](http://www.snort.org/docs/snort_htmanuals/htmanual_233/)