**Using ACID and SnortSnarf with Snort:**

***Analysis Console for Intrusion Databases (ACID)*** is a tool used to analyze and present Snort data using a web interface. It is written in PHP. It works with Snort and databases like MySQL.

**What is ACID?:** ACID consists of many Pretty Home Page (PHP) scripts and configuration files that work together to collect and analyze information from a database and present it through a web interface. A user will use a web browser to interact with ACID. You have to have a web server, database server, PHP and some other tools installed on your system to make it work.

**ACID offers many features:**

1. Searching can be done on a large number of criteria like source and destination addresses, time, ports and so on.

2. Packet viewing is used to view different parts of packet. You can view different header parts as well as the payload.

3. Alerts can be managed by creating alert classes, exporting and deleting and sending them to an e-mail address.

4. Graphical representation includes charts based upon time, protocol, IP addresses, port numbers and classifications.

5. Snapshots can be taken of the alerts database. As an example, you can view alerts for the last 24 hours, unique alerts, frequent alerts and so on.

6. You can go to different who is databases on the Internet to find out who owns a particular IP address that is attacking your network. You can then contact the responsible person to stop it. The who is database contains information about owners of domain names and IP addresses.

**Installation and Configuration:** The following step-by-step process makes it easy to put everything in place.

• Install and test Snort

• Install and test MySQL

• Install Apache

• Download ACID from http://www.cert.org/kb/acid/ and uncompress it in /var/www/html directory. This process creates a directory named acid under /var/www/html directory

• Get and Install PHP. You can download it from <http://www.php.net>

• Get and install GD library from <http://www.boutell.com/gd/>.

• Download PHPLOT from http://www.phplot.com and uncompress it in /var/ www/html directory. This is used to create graphics in the web pages.

• Download ADODB from http://php.weblogs.com/adodb and install it in /var/ www/html directory. ADODB is an object oriented library written in PHP and is used to connect to the database.

**Now download and install the software as mentioned below:**

• Download ACID file acid-0.9.6b21.tar.gz from http://www.cert.org/ kb/acid/ and put it in /opt directory.

• Download ADODB file adodb221.tgz from http://php.weblogs.com/adodb and put it in /opt directory.

• Download PHPLOT file phplot-4.4.6.tar.gz from http:// www.phplot.com and put it in /opt directory.

• Move to /var/www/html directory.

• Use the command “tar zxvf /opt/acid-0.9.6b21.tar.gz.” This will create a directory /var/www/html/acid and put all ACID files under it.

• Use the cd command to go to /var/www/html/acid directory.

• Use the command “tar zxvf /opt/adodb221.tgz” to extract ADODB files. The command will create a directory /var/www/html/acid/adodb and put all ADODB files under this directory.

• Use the command “tar zxvf /opt/phplot-4.4.6.tar.gz” to extract PHPLOT files. This will create a directory /var/www/html/acid/ phplot-4.4.6 and put all PHPLOT files under this directory.

• Create another database snort\_archive using “create database snort\_archive;” command after starting mysql client using the procedure described in Chapter 5. You have already created a database with the name “snort” and a user with the name “rr” as discussed in Chapter 5. The new snort\_archive database is used by ACID to archive old data. The new database is not required by Snort to log data. If you don’t want to archive old data using ACID, you can skip this step and the next step as well.

• Grant permissions to user rr to manage snort\_archive database using the command “grant CREATE, INSERT, DELETE, UPDATE, SELECT on snort\_archive.\* to rr@localhost;”.

• Create tables in this database using the command “mysql -u rr -p snort\_archive.

• Set display\_errors variable in /etc/php.ini to Off.

The following lines in acid\_conf.php file set up the main Snort database information where Snort logs its data:

$alert\_dbname = "snort";

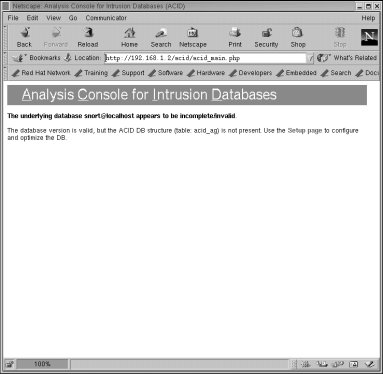
$alert\_host = "localhost";

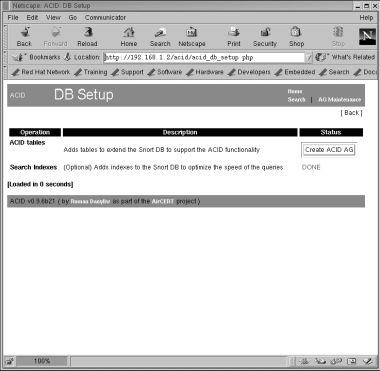
$alert\_port = "";

$alert\_user = "rr";

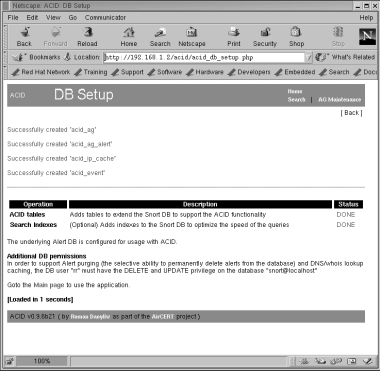
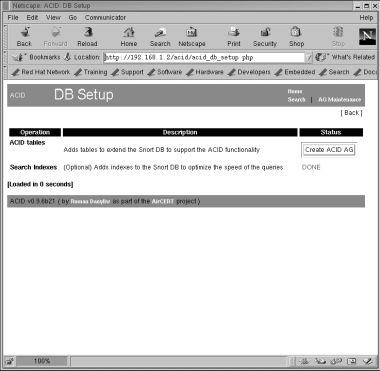
$alert\_password = "rr78x";

**Using ACID:**

**Invoking ACID for the first time **



**Creating ACID tables to existing database**

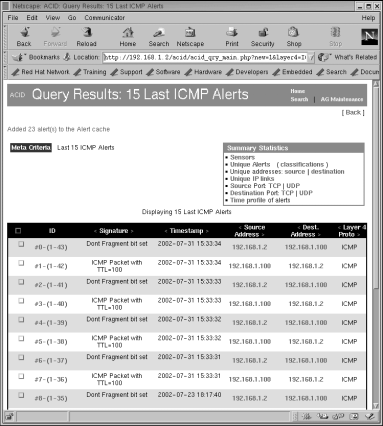
**Creating ACID tables to existing database **

**The result of creating additional tables in the Snort database to support ACID**

#### ACID Main Page:

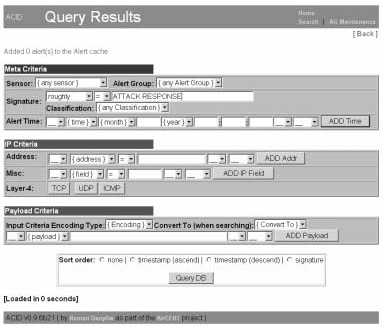
#### 

#### Listing Protocol Data

**ICMP protocol data**

#### Alert Details

#### Searching



**Searching for all alerts that contain “ATTACK RESPONSE” string in the signature**

## **SnortSnarf:**

SnortSnarf is another tool to display Snort data using a web interface. It is available from its web site at [http://www.silicondefense.com/software/snortsnarf/index.htm.](http://www.silicondefense.com/software/snortsnarf/index.htm) Basically it is a Perl script and you can run it after downloading without going through any compilation process. It can parse Snort log files as well as extract data from MySQL database. The following command parses /var/log/snort/alert file and places the newly generated HTML files in the /var/www/html/snortsnarf directory where they can be viewed later using a web browser.

**snortsnarf.pl /var/log/snort/alert -d /var/www/html/snortsnarf**

The following command extracts data from MySQL database running on the localhost. It uses a user name rr and password rr78x to login to the database.

**snortsnarf.pl rr:rr78x@snort@localhost -d /var/www/html/snortsnarf**

To get data from a database, you have to define the following parameters on the command line:

* Database user name
* Password
* Database name
* Host where database server is running
* Port number for the database server. By default the port number is 3306 and this parameter is optional.

The general format of defining these parameters is:

**user:passwd@dbname@host:port**

**Architecture models of IDs and IPs.**

[**https://flylib.com/books/en/2.352.1/ids\_and\_ips\_architecture.html**](https://flylib.com/books/en/2.352.1/ids_and_ips_architecture.html)