Snort 1.9.1, Apache 1.3.27, PHP 4.3.1, MySQL 3.23.56 and Acid 0.9.6b23 install on RedHat 8.0

Created by Patrick S. Harper, CISSP MCSE

Introduction:

This document originated when a friend of mine asked me to put together this procedure for him so that he could install Snort and Acid. It is pretty basic and for the beginner. I hope it does not insult the intelligence of anyone that has a good bit of Linux experience, but it is geared to a windows administrator with minimal Linux knowledge. This is not an ultra-secure end-all to Snort IDS deployment guide; this is a "How in the hell do I get this installed and working" guide. This document will walk you through installing a stand alone RedHat system; this is not for dual booting. I hope it is found to be useful by someone.
For editors I would suggest using pico, it is very easy to use. Type "pico <filename>" and it will open the file in the editor; all the commands are listed on the bottom. (Remember the ^ is for ctrl)

Acknowledgments:

I would like to thank all my friends and the people on the snort-users list that proofed this for me. And my fiancée Kris who did a test install with almost no Linux experience.

Comments or Corrections:

Please e-mail any comments or corrections to mailto:Patrick@internetsecurityguru.com

The latest version of this document may be found at http://www.internetsecurityguru.com/documents/snort_acid_rh8.pdf I will do my best to keep it updated.

Info for the install:

IP Address	
Subnet Mask	
Gateway	
DNS Servers	
Hostname	

Other important reading:

Snort users manual http://www.snort.org/docs/writing_rules/
Snort FAQ http://www.snort.org/docs/faq.html

The snort user's mailing list http://lists.sourceforge.net/lists/listinfo/snort-users
(The place to get help, AFTER you read the FAQ, and ALL the documentation on the Snort website, AND have searched Google). Also make sure to read the link below before sending questions so you know the rules. ☺
The Snort drinking game
http://www.theadamsfamily.net/~erek/snort/drinking_game.txt (Thanks Erek)
ACID FAQ http://www.andrew.cmu.edu/~rdanyliw/snort/acid_faq.html
ACID install guide http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html
RedHat Support documents for 8.0 -
http://www.redhat.com/support/resources/howto/rhl80.html

Websites to visit:
http://www.snort.org
http://www.cert.org/kb/acid/
http://www.mysql.com
http://www.php.net
http://www.redhat.com
http://www.chiark.greenend.org.uk/~sgtatham/putty/ (the putty ssh client)
http://www.internetsecurityguru.com (my homepage)

Installing RedHat 8.0:

Install the minimal amount of packages with the install, after the install turn off anything you do not want to use. This install is for a system that is not used only as an IDS, but can easily be converted to a dedicated IDS by only installing what is needed for Snort to run, hardening the OS, and further securing the system. There are a lot of good articles on how to secure a RedHat box on the web, just hit http://www.google.com and search for "securing redhat".

Mouse Configuration:
I always use the generic PS/2 drivers for my mice, but I am almost always working on a KVM. If you are on a KVM use the generic drivers, if not see if your mouse is in the list.

Install Type:
Choose custom

Disk Partitioning:
Choose to automatically partition the hard drive
Choose to remove all partitions from this hard drive (I am assuming that this not a dual boot box)
Make sure the review button is checked
The following is approximately how RedHat will set it up:
SWAP is twice the amount of ram
/boot is about 100 Meg
/ is the rest of the hard drive

Boot Loader:
Go with the default (if this is a dual boot system then go to google and search for info on how to install grub for dual booting)

Network Configuration:
Hit edit
Uncheck "Configure with DHCP"
Set a static IP and subnet mask for your network
Then set a gateway and DNS address's
Manually set the hostname

Always try to assign an IP here, I think it is best not to run snort off of a Dynamic IP, if you need to though, go ahead and do so, just make sure to point your HOME_NET variable in your snort.conf to the interface name, you can get more info on that in the Snort FAQ. If this is a dedicated IDS then you do not need to have an IP on the interface that snort is monitoring, this is not covered in this document but there is lots of info on how to do that out on the web)

Firewall:
Set this to open only SSH and port 80 for Apache

Time Setup:
Set the time and date correctly
On the UTC offset tab set the time zone and choose whether to update you for daylight savings

Root Password:
Set a strong root password here
You should also create another user account here. It is always suggested that you do as little on the system as possible as root, and to su when you need to have root access

Authentication:
Use both MD5 and Shadow passwords

Suggested Packages:
Take the defaults with the following exceptions. (DEFAULT IS WHAT EVER IT HAS WHEN YOU CHOOSE CUSTOM, FOR EXAMPLE GNOME OS CHECKED BY DEFAULT AND KDE IS NOT SELECTED)

Desktops:
X Window System – Accept the default

Gnome Desktop Environment – Accept the default

KDE Desktop Environment - Accept the default

Applications:
Editors – Choose your favorites (pico is a very easy to use editor and is installed by default

Engineering and Scientific – Uncheck this one

Graphical Internet – If this is also going to be a desktop machine as well as IDS then install what you want from here.

Text based internet – Install lynx (a text based browser, you will use this to get the programs that need to be installed)

Office/Productivity – Only xpdf should be selected

Sound and Video – None of this is needed

Authoring and Publishing – None of this is needed

Graphics – Install gimp is you are installing Gnome as your desktop

Games and Entertainment – None of this is needed

Server Section:
Choose nothing from this entire section

Development:
Development tools – Choose everything here

Kernel development – You will want this if you decide to go playing with the kernel later

X Software Development – Check this

Gnome Software Development – Check this

KDE Software Development – Leave this unchecked

System:
Administration – Leave this unchecked

System Tools – Choose nmap and ethereal

Printing support – Leave this unchecked

Miscellaneous:

Choose nothing from this entire section

Remember - Do not install Apache, PHP or MySQL, we will install these from source. You will be walked through every step.

Hit next, then next again
The install will start; this will take a little while so some coffee is good right about here. You have a few hours ahead of you depending on the speed of your system.

You can install almost anything as long as it is not one servers section of the package page. But remember if this system is located outside your firewall, is you main production IDS, or if you want it really secure you will need to install the least amount of software possible to get everything running. Everything you ever install and forget to update and maintain is a vulnerability waiting to happen, and that goes for all systems. To me this is one of the biggest rules for systems administration, make sure you know what you have, and make sure you keep it patched so you do not contribute to the next worm or virus that threatens to shut down major portions internet.

If this is a system for you to learn Snort, Linux, and all the other cool Linux type things, and is not directly on the Internet (i.e. NAT'd behind a firewall), then just have fun. Linux is a great operating system, it can fully replace a windows desktop or server with what is on it the 3 RedHat 8.0 CD's (most other distributions too), you have everything you need right there, and its free.

Boot Disk Creation:
Choose no

X Configuration:
Choose your card, monitor, then resolution and color depth you desire. Most everything is supported; I have not had anything that was not supported by what was listed yet. Make sure you test your settings before moving on.

Install complete:
Hit the exit button and the system will reboot.

After the system reboots login as root, you will be placed in the gnome desktop.

Go to the RedHat Network http://rhn.redhat.com and create a new account. This will give you a demo entitlement for your system. After you do this, click on the red explanation mark on the right hand side of the toolbar, it will turn green while it checks what updates are needed for your system. Then when it turns red again click it, choose register with RHN, and click OK. It will ask you if you want to use GPG for the signatures, click yes. Choose forward until you can enter your information to register your system with RHN. It will then determine what updates you need and will offer them for install. This is an easy way to update your system to the latest versions. (This will not

update what you install from source and you should update those manually as new versions come out)

You can also take this opportunity to disable services that you will not need for this system, Hit the RedHat on the bottom left of the toolbar, then server settings, services and you will have a list of services that start with the system. Disable the following:
apmd, autofs, firstboot, isdn, lpd (unless you plan to use lpr), netfs, nfslock, pcmcia, portmap, sgi_fam

Then hit "Save" on the top of that window, close the service configuration.

Now reboot your system and you will be up to date with all the latest packages and you can start the install.

Now you can get ready to start installing Snort and all of the software it needs. You can either use the desktop or SSH into the server from another box, either way will work fine, but for the novice it might be easier for them to do this from SSH so they can cut and paste the commands from this document into the session instead of typing what are some long strings.

Download all the needed files:

Place all the downloaded files in a directory for easy access and consolidation. This directory will not be needed when done with the install and may be deleted if you wish. I just created a directory under /root called snortinstall. Use the mkdir command from the shell. Make sure you are in the /root directory. You can check where you are at using the pwd command. If you are not root then you will need to execute su ("su –" takes you to the super user or root account, the "–" loads the environmental variables of the root account for you) and then enter the root password.

If you're SSH'd in to the box you can use either lynx (to open a specific URL type lynx "the URL you want") or wget (wget will place the file your downloading into the directory where your at) to download these files. If you can't seem to get lynx or wget down (hint, type "man <command>" i.e. "man wget" and you will get the man page, the manual) then you can download all of this to a box with FTP and then download it to the RedHat box. If you need an SSH client then you can go to the PuTTY home page and download a free one, you can also get a scp (secure copy) client there for windows.

Download MySQL 3.23.56 Source tarball
http://www.mysql.com/downloads/download.php?file=Downloads%2FMySQL-3.23%2Fmysql-3.23.56.tar.gz&pick=mirror

Download Snort 1.9.1
http://www.snort.org/dl/snort-1.9.1.tar.gz

Download Snort Rules (get latest stable)

http://www.snort.org/dl/rules/snortrules-stable.tar.gz

Download apache 1.3.27
http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz

Download PHP 4.3.1
http://www.php.net/get/php-4.3.1.tar.gz/from/a/mirror

Download ADODB v3.30
http://phplens.com/lens/dl/adodb330.tgz

Download Acid 0.9.6b23
http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz

Download Zlib 1.1.4
http://flow.dl.sourceforge.net/sourceforge/libpng/zlib-1.1.4.tar.gz

Download JPGraph 1.11
http://jpgraph.techuk.com/jpgraph/downloads/jpgraph-1.11.tar.gz

Download LibPcap 0.7.2
http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz

Preparing to begin the install:

If you are not logged in as root you will need to su to root ("su -" will load the environmental variables of root, use that when you su)

Go to your directory where you downloaded all your files (download them all before you start the install, it will go smother, trust me), then start with the following procedure.

This document will walk you through extracting the source files of the applications then compiling, installing, and configuring them for use with Snort.

Install zlib 1.1.4:

```
tar -xvzf zlib-1.1.4.tar.gz
cd  zlib-1.1.4
./configure; make test
make install
cd ..
```

Install LibPcap 0.7.2:

tar –xvzf libpcap.tar.gz
cd libpcap
./configure
make
make install
cd ..

Install MySQL 3.23.56:

Create the user and group for MySQL with the following commands:
groupadd mysql
useradd -g mysql mysql
Go to the directory you downloaded everything to and use the following commands to install and configure MySQL.

tar –xvzf mysql-3.23.56.tar.gz
cd mysql-3.23.56
./configure --prefix=/usr/local/mysql
make
make install

scripts/mysql_install_db

chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var
chgrp -R mysql /usr/local/mysql

cp support-files/my-medium.cnf /etc/my.cnf

Next add the line /usr/local/mysql/lib/mysql and /usr/local/lib to /etc/ld.so.conf
After you add the line, run ldconfig as root

Test to see if it worked.
/usr/local/mysql/bin/safe_mysqld --user=mysql &

If you get no errors type "ps –ef |grep mysql" you should see something like this:
root   31701   705 0 19:02 pts/0   00:00:00 /bin/sh /usr/local/mysql/bin/saf
mysql   31723 31701 0 19:02 pts/0   00:00:00 [mysqld]
mysql   31725 31723 0 19:02 pts/0   00:00:00 [mysqld]
mysql   31726 31725 0 19:02 pts/0   00:00:00 [mysqld]
root   31728   705 1 19:02 pts/0   00:00:00 grep mysql

If it all worked then go to the next step which is to make MySQL start when the system boots up.

Set MySQL to start automatically.

Copy the file mysql.server from the support-files subfolder (it is under the source for mysql, if you downloaded everything to /root/snortinstall then the path will be /root/snortinstall/mysql-3.23.56/support-files) to the /etc/init.d folder and call it mysql (the command to copy it from the support-files directory would be "cp mysql.server /etc/init.d/mysql")

Use the following to create symbolic links to the startup folders for run levels 3 and 5 MySQL will now start automatically when you boot up.

```
cd /etc/rc3.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd /etc/rc5.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd ../init.d
chmod 755 mysql
```

Installing and setting up Apache 1.3.27 with PHP 4.3.1:

This procedure installs the Apache web server in "/www" this is where I prefer to install it; you can modify it for whatever location you wish.

Go to the directory you downloaded all the needed files to and perform the following actions. This method will setup the PHP module to be installed with Apache, then install Apache with PHP.

```
tar -xvzf apache_1.3.27.tar.gz
cd apache_1.3.27
./configure
cd ..
tar -xvzf php-4.3.1.tar.gz
cd php-4.3.1
./configure --with-mysql --with-apache=../apache_1.3.27 --enable-sockets --with-zlib-dir=/usr/local --with-gd (this is one line)
make
make install
cd ../apache_1.3.27
./configure --prefix=/www --activate-module=src/modules/php4/libphp4.a
make
make install
cd ../php-4.3.1
cp php.ini-dist /usr/local/lib/php.ini
```

Now edit your httpd.conf files (it's in /www/conf) and add:

AddType application/x-httpd-php .php

IT WILL LOOK SOMETHING LIKE THIS WHEN YOU ARE DONE

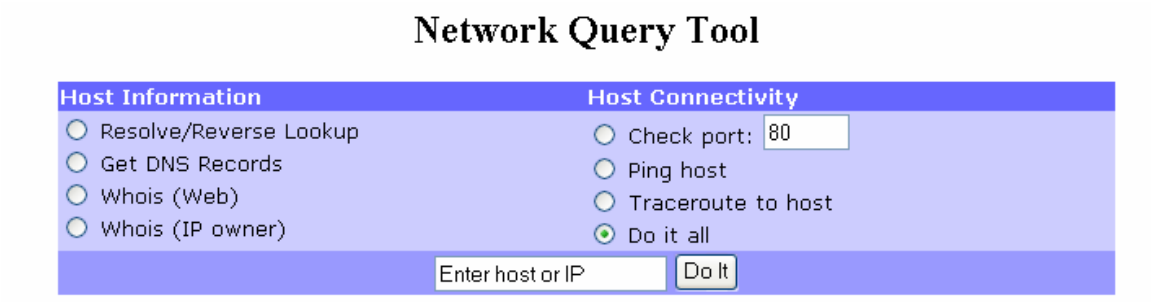
```
#
# AddType allows you to tweak mime.types without actually editing it, or $
# make certain files to be certain types.
#
AddType application/x-tar .tgz
AddType image/x-icon .ico
AddType application/x-httpd-php .php
```

Apache 1.3.27 is now installed in the /www dir. Go into the /www/bin dir and do the following commands:

```
cp apachectl /etc/init.d/httpd
cd /etc/rc3.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
cd /etc/rc5.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
```

(The above lines will add a start up script to the system for both run level 3 and 5)

To test the Apache – PHP install I always install a useful script. (you will need to start apache first, use /etc/rc5.d/S85httpd start) http://shat.net/php/nqt/nqt.php.txt It is a Network Query Tool, go to the page, copy all of the contents to a file called nqt.php, place it in /www/htdocs and then pull it up in a browser as http://hostname/nqt.php. If it looks like this Then you have Apache and PHP installed correctly.



Installing and setting up Snort and the Snort rules:

mkdir /etc/snort
mkdir /var/log/snort
tar -xvzf snort-1.9.1.tar.gz
cd snort-1.9.1
./configure --with-mysql=/usr/local/mysql
make
make install

Installing the rules and conf file:
cd ..
tar -xvzf snortrules-stable.tar.gz
cd rules
cp * /etc/snort

Modify your snort.conf file:
The snort.conf file is located in /etc/snort

var HOME_NET 10.2.2.0/24 (make this what ever your internal network is)

Change the rule path variable
var RULE_PATH /etc/snort/

Tell it to log to the database (make sure this is on one line)
output database: log, mysql, user=root password=your_password dbname=snort host=localhost

Set snort to start automatically:

Copy the following text to a file named snort in the /etc/init.d directory (it is a modified version of the one that comes with the snort source. It is located in the contrib. folder and is called S99snort)

```
#!/bin/bash
# $Id: S99snort,v 1.1 2001/12/18 22:14:37 cazz Exp $
# /etc/init.d/snort : start or stop the SNORT Intrusion Database System
#
# Written by Lukasz Szmit <ptashek@scg.gliwice.pl>
#
# Configuration

# set config file & path to snort executable
SNORT_PATH=/usr/local/bin
CONFIG=/etc/snort/snort.conf
```

```
# set interface
IFACE=eth0

# set GID/Group Name
# SNORT_GID=nogroup

# other options
OPTIONS="-D"

# End of configuration


test -x $SNORT_PATH/snort || exit 0

case "$1" in
    start)
       echo "Starting Intrusion Database System: SNORT"
       $SNORT_PATH/snort -c $CONFIG -i $IFACE $OPTIONS
       if [ "`pidof $SNORT_PATH/snort`" ]; then
             echo "SNORT is up and running!"
       else
            exit 0
       fi
       echo -n "."
       ;;

    stop)
       echo "Stoping Intrusion Database System: SNORT"
       if [ "`pidof $SNORT_PATH/snort`" ] ; then

          kill -TERM `pidof $SNORT_PATH/snort`

          # Wait until the timeout
          count=120
          numdots=0
          while ([ $count != 0 ]) do
             let count=$count-1
             if [ "`pidof $SNORT_PATH/snort`" ] ; then
                echo -n .
                let numdots=$numdots+1
                sleep 1
             else
                count=0
             fi
          done
```

```
            # If it's not dead yet, kill it.

            if [ "`pidof $SNORT_PATH/snort`" ] ; then
               echo " TIMEOUT!"
               kill -KILL `$SNORT_PATH/snort`
            else
               case $numdots in
                 0) echo "." ;;
                 1) echo ;;
                 *) echo " done." ;;
               esac
            fi
         else
            echo "SNORT is  not running!";
         fi
         ;;
      restart)
         $0 stop
         $0 start
         ;;
      *)
         echo 'Usage: /etc/init.d/snort {start|stop|restart}'
         exit 1
         ;;
esac
exit 0
;;
```

Then:
chmod 755 snort (the file you just created, or copied from the contrib folder and modified)
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort

Setting up the database in MySQL:

Add /usr/local/mysql/bin to your path. (Use “PATH=$PATH:/usr/local/mysql/bin”) then type “echo $PATH” to make sure it is there.

I will put a line with a > in front of it so you will see what the output should be

```
mysql
mysql>  set password for ‘root’@’localhost’ = password(‘your_password’);
>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 snort.* to root@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql>  exit
>Bye
```

From the Snort 1.9.1 source directory execute the following command

```
/usr/local/mysql/bin/mysql -p  < ./contrib/create_mysql snort
>Enter password:
```

Now you need to check and make sure that the snort DB was created correctly

```
mysql –p
>Enter password:
mysql>  SHOW DATABASES;
(you should see the following)
+------------+
| Database
+------------+
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)

mysql>  use snort
>Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
| event
| icmphdr
| iphdr
| opt
| reference
| reference_system
| schema
```

```
| sensor
| sig_class
| sig_reference
| signature
| tcphdr
| udphdr
+------------------+
16 rows in set (0.00 sec)
mysql> exit
>Bye
```

Install JPGraph 1.11:

Go back to your downloads directory

```
cp jpgraph-1.11.tar.gz /www/htdocs
cd /www/htdocs
tar –xvzf jpgraph-1.11.tar.gz
rm –rf jpgraph-1.11.tar.gz
cd jpgraph-1.11
rm -rf README
rm -rf QPL.txt
```

Installing ADODB:

Go back to your download directory

```
cp adodb330.tgz /www/htdocs/
cd /www/htdocs
tar -xvzf adodb330.tgz
rm –rf adodb330.tgz
cd ..
```

Installing and configuring Acid:

Go back to your downloads directory

```
cp acid-0.9.6b23.tar.gz /www/htdocs
cd /www/htdocs
tar –xvzf  acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz
```

Configuring Acid:
Go to the /www/htdocs/acid/ directory and edit the acid_conf.php file, it should look like this (except of course you will need your password)

```
$DBlib_path = "/www/htdocs/adodb";

/* The type of underlying alert database
 *
 *  MySQL            : "mysql"
 *  PostgresSQL      : "postgres"
 *  MS SQL Server : "mssql"
 */
$DBtype = "mysql";

/* Alert DB connection parameters
 *   - $alert_dbname   : MySQL database name of Snort alert DB
 *   - $alert_host         : host on which the DB is stored
 *   - $alert_port         : port on which to access the DB
 *   - $alert_user         : login to the database with this user
 *   - $alert_password : password of the DB user
 *
 *  This information can be gleaned from the Snort database
 *  output plugin configuration.
 */
$alert_dbname   = "snort";
$alert_host         = "localhost";
$alert_port         = "";
$alert_user         = "root";
$alert_password = "Your_Password";

/* Archive DB connection parameters */
$archive_dbname   = "snort";
$archive_host      = "localhost";
$archive_port      = "";
$archive_user      = "root";
$archive_password = "Your_Password ";
```

And a little further down

```
$ChartLib_path = "/www/htdocs/jpgraph-1.11/src";

/* File format of charts ('png', 'jpeg', 'gif') */
$chart_file_format = "png";
```

Then go to http://your host/acid/acid_main.php

You will get a message that says

The underlying database snort@localhost appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: acid_ag) is not present. Use the Setup page to configure and optimize the DB.

Click on the "Setup Page" hyperlink

Then click the button that says "Create Acid AG"

Now when you go to http://yourhost/acid/ (you need the trailing / in IE) you should see the ACID homepage

Check to see if everything is working:

Reboot your system; watch to make sure everything starts.

If you want the machine to start at a text prompt instead of X, then change the default in the inittab file (/etc/inittab) from 5 to 3. Go to a shell as root and check everything important to see if it is running.

Enter this command:
ps -ef |grep http && ps –ef |grep mysql && ps -ef |grep snort

You should get something like this:

```
root      596    1  0 20:32 ?        00:00:00 /www/bin/httpd
nobody    600  596  0 20:32 ?        00:00:00 [httpd]
nobody    601  596  0 20:32 ?        00:00:01 [httpd]
nobody    602  596  0 20:32 ?        00:00:00 [httpd]
nobody    604  596  0 20:32 ?        00:00:00 [httpd]
nobody    605  596  0 20:32 ?        00:00:04 [httpd]
nobody    804  596  0 20:34 ?        00:00:00 [httpd]
nobody    806  596  0 20:34 ?        00:00:00 [httpd]
nobody    807  596  0 20:37 ?        00:00:00 [httpd]
nobody    808  596  0 20:37 ?        00:00:00 [httpd]
nobody    809  596  0 20:37 ?        00:00:00 [httpd]
root      607    1  0 20:32 ?        00:00:00 /bin/sh /usr/local/mysql/bin/saf
mysql     639  607  0 20:32 ?        00:00:00 [mysqld]
mysql     655  639  0 20:32 ?        00:00:00 [mysqld]
mysql     657  655  0 20:32 ?        00:00:00 [mysqld]
mysql     719  655  0 20:32 ?        00:00:00 [mysqld]
mysql     805  655  0 20:34 ?        00:00:00 [mysqld]
mysql     810  655  0 20:39 ?        00:00:00 [mysqld]
mysql     811  655  0 20:41 ?        00:00:00 [mysqld]
root      819  760  0 20:44 pts/0    00:00:00 grep mysql
root      691    1  0 20:32 ?        00:00:01 /usr/local/bin/snort -c /etc/sno
```

```
root       821   760  0 20:44 pts/0    00:00:00 grep snort
```

Now it's time to test snort. I suggest using something free like CIS Scanner (http://www.cerberus-infosec.co.uk/CIS-5.0.02.zip) or Nessus (http://www.nessus.org) if you have it, and running it against your snort box. Check ACID when you're done and it should have a bunch or alerts. If you are on DSL or cable then you could already have a bunch in there right after you start it up.

Congratulations, you did it. You now have a fully functional IDS running and logging to a database and being viewed through a PHP script running on apache, and you did it all from source. Good Work ☺