Snort, MySQL 5, Apache, and BASE for Gentoo Linux

This guide should help anyone who is looking to run Snort with a MySQL 5 backend, and BASE as a reporting tool.

This guide is for Gentoo Linux specifically, but I'm sure it will help out users of any distro.

Edit your /etc/make.conf and include these options.

Code:

```
USE="gd jpeg png hardenedphp apache2 innodb php perl mysql hardened"
```

Packages needed:

Snort
MYSQL
Mod_PHP (will also install PHP which is needed)
Apache
Base (http://secureideas.sourceforge.net/index.php)
Adodb
GD
(You may already have the ones below installed. Please double check)
Libpng
jpeg
zLib

\\Let's get all the needed packages

MySQL
dev-db/mysql-5.0.15

Code:

```
ACCEPT_KEYWORDS="~x86" emerge mysql
```

Apache
net-www/apache-2.0.54-r31

Code:

```
emerge apache
```

Mod_php
dev-php/mod_php-4.4.0-r9

Code:

```
emerge mod_php
```

Snort
net-analyzer/snort-2.4.3

Code:

```
ACCEPT_KEYWORDS="~x86" emerge snort
```

BASE
base-1.2.1.tar.gz
Download from http://secureideas.sourceforge.net/index.php

Adodb
dev-php/adodb-4.65

Code:

```
emerge -f adodb
```

GD
media-libs/gd-2.0.32

Code:

```
emerge media-libs/gd
```

Libpng
media-libs/libpng-1.2.8

Code:

```
emerge media-libs/libpng
```

jpeg
media-libs/jpeg-6b-r5

Code:

```
emerge media-libs/jpeg
```

zLib
sys-libs/zlib-1.2.3

Code:

```
emerge zlib
```

Let's setup Apache and PHP

Edit your /etc/conf.d/apache file

Code:

```
 nano -w /etc/conf.d/apache
```

Edit the 'APACHE2_OPTS' line as shown below:

Code:

```
APACHE2_OPTS="-D PHP4 -D SSL -D DEFAULT_VHOST"
```

This gives us PHP and SSL support.

Now start Apache:

Code:

```
/etc/init.d/apache2 start
```

Watch /var/log/messages for errors.

Let's add apache to the default run level:

Code:

```
rc-update add apache default
```

Let's get MySQL going

Important info for upgrading MySQL:

Code:

```
If you're upgrading from MySQL-3.x to 4.0, or 4.0.x to 4.1.x, you
must recompile the other packages on your system that link with
libmysqlclient after the upgrade completes.  To obtain such a list
of packages for your system, you may use:
revdep-rebuild --library=libmysqlclient.so.14
from app-portage/gentoolkit.

the value of "innodb_log_file_size" into /etc/mysql/my.cnf file
```

```
has changed size from "8M" to "5M".
To start mysql either revert the value back to "8M" or backup and
remove the old ib_logfile* from the datadir
```

Let's create the default tables in MySQL:

Code:

```
# /usr/bin/mysql_install_db
```

Now let's start MySQL:

Code:

```
/etc/init.d/mysql start
```

Set a root password for MySQL:

Code:

```
/usr/bin/mysqladmin -u root password 'passwordhere'
```

Let's add Mysql to the default run level:

Code:

```
rc-update add mysql default
```

Let's create the Snort database

First log into Mysql as root:

Code:

```
mysql -u root -p
```

Now create the database, user, and security.

Code:

```
create database snort;
grant INSERT,SELECT on root.* to snort@localhost;
SET PASSWORD FOR snort@localhost=PASSWORD('passwordhere');
grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to snort@localhost;
grant CREATE,INSERT,SELECT,DELETE,UPDATE on snort.* to snort;
exit
```

Now we need to create the database structure for Snort by issuing this command:

Code:

```
zcat /usr/share/doc/snort-2.4.3/schemas/create_mysql.gz | mysql -p snort
```

This will create the database structure in MySQL.

To double check that the structure was created:

Code:

```
 mysql -u root -p snort
```

Once logged in, issue this command:

Code:

```
show tables;
```

You should see this:

Code:

```
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)
```

Now your database has the correct table structure.

\\Ok now to get Snort logging to the newly created database

Now we need to configure Snort to report to the database and not to log files.

Edit the snort.conf file:

Code:

```
nano -w /etc/snort/snort.conf
```

Find this line shown below (line 382 for me), uncomment it, and change it to reflect your setup:

Code:

```
output database: log, mysql, user=snort password=password dbname=snort
host=localhost
```

Now Snort will log all logs and alerts to the MySQL database.

Start Snort with:

Code:

```
  /etc/init.d/snort start
```

Add to default run level with:

Code:

```
rc-update add snort default
```

Watch your /var/log/messages for errors.

First off I recieved this error in /var/log/messages:

Code:

```
snort[25905]: FATAL ERROR: Unable to open rules file:
/etc/snort/rules/local.rules or /etc/snort//etc/snort/rules/local.rules
```

To fix this go to www.snort.org and register.
Download the latest rules and put them in /etc/snort/rules.
Then run:

Code:

```
/etc/init.d/snort zap
```

This will zap the state of Snort back to a stopped state.
Start Snort again, and watch /var/log/messages. You should see this:

Code:

```
 snort[26024]: Snort initialization completed successfully (pid=26024)
```

\\Let's get prepared to install BASE

Here's where we use the Adodb we downloaded:

Code:

```
cp /usr/port/distfiles/adodb465.tgz /var/www/localhost/htdocs/
```

Extract the source:

Code:

```
cd /var/www/localhost/htdocs
```

Code:

```
 tar -zxvf adodb465.tgz
```

Install some Pear stuff:

Code:

```
pear install Image_Color
pear install Log
pear install Numbers_Roman
pear install http://pear.php.net/get/Numbers_Words-0.13.1.tgz
pear install http://pear.php.net/get/Image_Graph-0.3.0dev4.tgz
```

Let's get Base going
Extract the source in /var/www/localhost/htdocs/

Code:

```
mv base-1.2.1.tar.gz /var/www/localhost/htdocs/
```

Code:

```
cd /var/www/localhost/htdocs/
```

Code:

```
tar -zxvf base-1.2.1.tar.gz
```

Rename folder to just 'base':

Code:

```
mv base-1.2.1 base
```

Code:

```
cd base
```

Let's edit the base config file, first copying it to the correct name:

Code:

```
 cp base_conf.php.dist base_conf.php
```

Code:

```
nano -w base_conf.php
```

Here is what you'll have to change:

Set your URL to your base installation:
DO NOT INCLUDE A TRAILING SLASH

Code:

```
$BASE_urlpath = "mybox.mydomain.com/base";
```

Adodb Path:

Code:

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

Snort database info:
Change to what you need. You should only have to change the password.

Code:

```
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "mypassword";
```

Save that file and open the base_main.php in your web browser.

For me the address was:

Code:

```
http://lappy.mydomain.com/base/
```

You will then be prompted to make specific changes to the Mysql database. Don't worry, base will do it all for you

After that page hit the "CREATE BASE AG" button to finish the database changes.

After that is all done, click on the link near the bottom that says "Goto main page to use the application".

That's all you should need to get this up and running.

For good measure restart MySQL, Snort, and Apache.

Chris Vespermann
Chris.vespermann@gmail.com