By Andrew Riesel
Published: 2007-11-19 18:06

Intrusion Detection: Snort, Base, MySQL, and Apache2 On Ubuntu 7.10 (Gutsy Gibbon)

In this tutorial I will describe how to install and configure Snort (an intrusion detection system (IDS)) from source, BASE (Basic Analysis and Security Engine), MySQL, and Apache2 on Ubuntu 7.10 (Gutsy Gibbon). Snort will assist you in monitoring your network and alert you about possible threats. Snort will output its log files to a MySQL database which BASE will use to display a graphical interface in a web browser.## 1. Prerequisites

The first thing I like to do is grab all the dependant packages that I can from Synaptic.

From the Desktop go to *System > Administration > Synaptic Package Manager*. Enter your password and select *Search*.

Search for the following packages and install them:

- *Libpcap0.8-dev*
- *libmysqlclient15-dev*
- *mysql-client-5.0*
- *mysql-server-5.0*
- *bison*
- *flex*
- *apache2*
- *libapache2-mod-php5*
- *php5-gd*
- *php5-mysql*
- *libphp-adodb*
- *php-pear*## 2. Gain root privileges

From the Desktop go to *Applications > Accessories > Terminal* and type:

```
$ sudo -i
```

```
$ Then your password.
```

We need to get one more package here,

```
# apt-get install libc6-dev g++ gcc
```

3. Time to download and untar packages

We want to create a temp directory to download and untar files. I'm going to use edge's structure here. In the terminal window type the following:

```
# cd /root

# mkdir snorttmp

# cd /root/snorttmp
```

Let's get snort. The latest version of snort at the time of writing is 2.8.0.

Open a web browser and navigate to **http://www.snort.org/dl**; right click on the most recent release and copy link location.

In the terminal type:

```
# wget http://www.snort.org/dl/current/snort-2.8.0.tar.gz
```

It's time to untar the Snort package and remove the tar file.

```
# tar -xzvf /root/snorttmp/snort-2.8.0.tar.gz

# rm /root/snorttmp/snort-2.8.0.tar.gz
```

4. Get some Snort rules.

Change directories into the new snort-2.8.0 folder.

```
# cd /root/snorttmp/snort-2.8.0
```

Open a web browser and navigate to **http://www.snort.org/pub-bin/downloads.cgi**.

Scroll down to the "Sourcefire VRT Certified Rules - The Official Snort Rule set (unregistered user release)" section. Right click on the most recent release and copy link location.

If you are a forum member you can get newer rules which are under the "registered user release".

In the terminal type:

```
# wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz
```

Untar the Snort Rules and remove the tar file.

```
# tar -xzvf /root/snorttmp/snort-2.8.0/snortrules-pr-2.4.tar.gz

# rm /root/snorttmp/snort-2.8.0/snortrules-pr-2.4.tar.gz
```

5. Get PCRE - Perl Compatible Regular Expressions.

Change directory back into the snorttmp folder.

```
# cd /root/snorttmp
```

Open a web browser and go to **http://www.pcre.org**.

Click on the link for the newest release, right click on the newest tar.gz package and select copy link (at the time of writing this is pcre-7.4).

In the terminal type:

```
# wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-7.4.tar.gz
```

Untar PCRE and remove the tar file.

```
# tar -xzvf /root/snorttmp/pcre-7.4.tar.gz

# rm /root/snorttmp/pcre-7.4.tar.gz
```

6. Get BASE (Basic Analysis and Security Engine).

Change directory back into the snorttmp folder.

```
# cd /root/snorttmp
```

Open a web browser and go to **http://sourceforge.net/project/showfiles.php?group_id=103348**.

Click on download then right click on the newest tar.gz package and select copy link (at the time of writing this is base-1.3.8).

In the terminal type:

```
# wget http://downloads.sourceforge.net/secureideas/base-1.3.8.tar.gz?modtime=1183896336&big_mirror=0
```

Untar BASE and remove the tar file.

```
# tar -xzvf /root/snorttmp/base-1.3.8.tar.gz

# rm /root/snorttmp/base-1.3.8.tar.gz
```

7. Get ADOdb (database abstraction library for PHP).

Change directory back into the *snorttmp* folder.

```
# cd /root/snorttmp
```

Open a web browser and go to **http://sourceforge.net/project/showfiles.php?group_id=42718**.

Click on the download link for adodb-php5-only then right click on the *adodb502a.tgz* package and select copy link (adodb502a is the most recent package at the time of writing).

In the terminal type:

```
# wget http://downloads.sourceforge.net/adodb/adodb502a.tgz?modtime=1191343792&big_mirror=0
```

Untar ADOdb and remove the tar file.

```
# tar -xzvf /root/snorttmp/adodb502a.tgz

# rm /root/snorttmp/adodb502a.tgz
```

Do an ls to be sure you have all the packages.

```
# ls /root/snorttmp
```

You should see the following folders,

- *adodb5*
- *base-1.3.8*
- *pcre-7.4*
- *snort-2.8.0*

8. Installation.a. PCRE install.

```
# cd /root/snorttmp/pcre-7.4
```

Here we will do a make/install

```
# ./configure

# make

# make install
```

b. Snort install.

```
# cd /root/snorttmp/snort-2.8.0
```

Here we will do a make/install

```
# ./configure -enable-dynamicplugin --with-mysql

# make

# make install
```

9. Copying files.

We need to create some folders in `/etc` for snort to function correctly and copy some files over to them.

```
# mkdir /etc/snort /etc/snort/rules /var/log/snort
```

Let's move some files.

```
# cd /root/snorttmp/snort-2.8.0/rules
```

```
# cp * /etc/snort/rules/
```

Let's get the */etc* snort files also.

```
# cd /root/snorttmp/snort-2.8.0/etc

# cp * /etc/snort/
```

One more file.

```
# cp /usr/local/lib/libpcre.so.0 /usr/lib
```

10. Snort Configuration

We need to modify the snort.conf file to suite our needs.

Open */etc/snort/snort.conf* with your favorite text editor (nano, vi, vim, etc.).

```
# vim /etc/snort/snort.conf
```

Change "**var HOME_NET any**" to "**var HOME_NET 192.168.1.0/24**" (your home network may differ from 192.168.1.0)
Change "**var EXTERNAL_NET any**" to "v**ar EXTERNAL_NET !$HOME_NET**" (this is stating everything except HOME_NET is external)
Change "**var RULE_PATE ../rules**" to "**var RULE_PATH /etc/snort/rules**"

Scroll down the list to the section with "**# output database: log, mysql, user=**", remove the "**#**" from in front of this line.
Leave the "**user=root**", change the "**password=password**" to "**password=YOUR_PASSWORD**", "**dbname=snort**"
Make note of the username, password, and dbname. You will need this information when we set up the Mysql db.
Save and quit.

11. Setup the Mysql database.

Log into the mysql server.

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

Sometimes there is no password set so just hit enter.

If you get a failed logon, try the above command again and enter *YOUR_PASSWORD*.

If there is no password you need to create a password for the root account.

Note: Once you are in mysql the # is now a *mysql>*

```
mysql> SET PASSWORD FOR root@localhost=PASSWORD('YOUR_PASSWORD');
```

Create the snort database.

```
mysql> create database snort;

mysql> exit
```

We will use the snort schema for the layout of the database.

```
# mysql -D snort -u root -p < /root/snorttmp/snort-2.8.0/schemas/create_mysql
```

We need to comment out a few lines in the web rules before we can test snort, I am unsure if this has been fixed in the subscriber version.

Open up */etc/snort/rules/web-misc.rules* with your favorite text editor.

```
# vim /etc/snort/rules/web-misc.rules
```

Comment out line's 97, 98, and 452 with a "#" (no quotes).

12. Time to test Snort

In the terminal type:

```
# snort -c /etc/snort/snort.conf
```

If everything went well you should see an ascii pig.

To end the test hit `ctrl + c`.

12. Base and Apache2

We have already installed both Apache2 and BASE, all we have to do now is move some files and modify a config file.
Create a file called `test.php` in `/var/www/` with your favorite text editor.

```
# vim /var/www/test.php
```

write in it:

```
<?php
phpinfo();
?>
```

Save and close this file

We need to edit `/etc/php5/apache2/php.ini` file.

```
# vim /etc/php5/apache2/php.ini
```

You need to add the following under "Dynamic Extensions".

```
extension=mysql.so

extension=gd.so
```

Restart Apache2.

```
# /etc/init.d/apache2 restart
```

Get the ip address of the machine you are working on.

```
# ifconfig -a
```

Open a web browser and go to *http://YOUR.IP.ADDRESS/test.php*.

If everything went well, you will have PHP information displayed.

13. Moving more files.

We need to move ADOdb into the */var/www* directory.

```
# mv /root/snorttmp/adodb5 /var/www/
```

Let's make a directory in *www* and move BASE.

```
# mkdir /var/www/web

# mv /root/snorttmp/base-1.3.8 /var/www/web/
```

We need to temporarily enable writing to the *base-1.3.8* folder for setup.

```
# chmod 757 /var/www/web/base-1.3.8
```

We also need to modify a PHP setup file using your favorite text editor.

```
# vim /var/www/web/base-1.3.8/setup/setup1.php
```

Find the line that says "base_header" and change it to "header".

Save and exit.

We want the graphs in base to work so we need to install a few pear extensions.

```
# pear install Image_Color

# pear install Image_Canvas-alpha

# pear install Image_Graph-alpha
```

14. BASE Setup via the web.

Open a web browser and navigate to *http://YOUR.IP.ADDRESS/web/base-1.3.8/setup*.

Click continue on the first page.

- Step 1 of 5: Enter the path to ADODB.
This is */var/www/adodb5*.
- Step 2 of 5:
Database type = *MySQL*, Database name = *snort*, Database Host = *localhost*, Database username = *root*, Database Password = *YOUR_PASSWORD*
- Step 3 of 5: If you want to use authentication enter a username and password here.
- Step 4 of 5: Click on *Create BASE AG*.
- Step 5 of 5: one step 4 is done at the bottom click on *Now continue to step 5.*

Bookmark this page.

Change the permissions back on the */var/www/web/base-1.3.8* folder.

```
# chmod 775 /var/www/web/base-1.3.8
```

We are done. Congrats!!!

To start Snort in the terminal type:

```
# snort -c /etc/snort/snort.conf -i eth0 -D
```

This starts snort using eth0 interface in a daemon mode.

To make sure it is running you can check with the following command:

```
# ps aux | grep snort
```

If it's running you will see an entry similar to *snort -c /etc/snort/snort.conf -i eth0 -D*.

If you would like to learn how to write your own Snort rules there is a guide at **http://www.snort.org/docs/snort_manual/node16.html**.
Good luck.