% Security topics
%
% Snort Exercise - Setting up a web front-end

Introduction

We will set up Snort together with BASE (Basic Analysis and Security Engine). This application provides a web front-end to query and analyze the alerts coming from a SNORT IDS system. BASE is the evolution of a previous project called ACID.

Notes

* Commands preceded with "$" imply that you should execute the command as a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

Goals

* Learn how to install the Snort package with MySQL support
* Learn how to install and configure the acidbase package on Ubuntu
* Set up authentication
* Set up e-mail exports

Snort-MySQL Installation

Log in to the PC assigned to you, and install the the lamp-server group of packages:

```
$ sudo apt-get install tasksel
$ sudo tasksel install lamp-server
```

The above command is a shortcut to install a set of predefined packages, that offer the "Linux Apache Mysql PHP" services, i.e. LAMP. Some or most of these packages may have already been installed during previous labs, but it doesn't hurt to run it.

If you are curious which packages this "set" includes, you can run:

```
$ tasksel --task-packages lamp-server
```

If you haven't already done so before, you will be prompted to create a MySQL root password during the installation process. Please use the same password you used to log in to your virtual PC, and which was given in class.

Now, create the database to be used by Snort:

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

Type the password you provided earlier while installing. Then, at the mysql

prompt, type the following:

```
mysql> create database snort;
mysql> GRANT ALL PRIVILEGES ON snort.* TO 'snort'@'localhost' IDENTIFIED BY
'snortpwd';
mysql> FLUSH PRIVILEGES;
mysql> quit
```

NOTE: Notice that we used 'snortpwd' here. This is the password that Snort will use to connect to the Mysql database. We will also use it later for the web front-end. Instead of 'snortpwd', you may want to use the default password used to log in to your machine.

Install Snort with mysql support:

```
$ sudo apt-get -y install snort-mysql
```

If you see a window prompting you to provide the "Address range for the local network". Type the network address of your particular group.

For example, for group 1, the network block is: 10.10.1.0/24

Following this, you will be asked if you wish to set up a database for use with Snort. Choose No. We will manually configure Snort to connect to our previously created database.

You will receive a warning like the following: "Snort will not start as its database is not yet configured". That's OK. Go on.

Create the database table structure:

```
$ zcat /usr/share/doc/snort-mysql/create_mysql.gz |  mysql -u snort -p snort
```

  type the snort database password: "snortpwd"

Edit the Snort configuration to include the database parameters:

```
$ sudo editor /etc/snort/snort.conf
```

  find this line:

```
output log_tcpdump: tcpdump.log
```

  and comment it out like this:

```
#output log_tcpdump: tcpdump.log
```

Save and exit the editor.

Now, edit the snort database configuration file:

```
$ sudo editor /etc/snort/database.conf
```

Then, add this line at the end of the file.

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

Remember to use the SAME password here that you picked during database creation earlier!

Save and exit the editor.

Remove the pending Snort database configuration file.

```
$ sudo rm -rf /etc/snort/db-pending-config
```

Start the Snort service.

```
$ sudo service snort start
```

Verify that the Snort daemon successfull started:

```
$ sudo /etc/init.d/snort status
$ tail /var/log/daemon.log
```

BASE Installation

Next we will install a web front-end (BASE) to monitor Snort's output.

```
$ sudo apt-get -y install acidbase
```

During the installation process you will be prompted a couple of times where you just have to accept (Ok) and continue. You will then be asked to configure a database for acidbase. Choose "MySQL" for the database type when asked.

You may be prompted for the password of the database administrator. This is the same password we used when MySQL was initially installed.

Upon entering the database administrator password, you will be prompted to create a MySQL password for acidbase to connect to the database. In this exercise we will use the same password as the snort user: "snortpwd" (please double check that you are using the correct password, write it down if necessary for now!)

BASE (acidbase) Configuration

When installed, the acidbase web front-end is configured to only allow access from the localhost. Modify acidbase's configuration to allow other workstations to connect:

```
$ sudo editor /etc/acidbase/apache.conf
```

  find this line:

```
allow from 127.0.0.0/255.0.0.0
```

  and change it to match your group's network. For example, for pc1:

```
allow from 10.10.1.0/255.255.255.0
```

Save the file and exit the editor. Then restart Apache:

```
$ sudo service apache2 restart
```

You may need to verify the acidbase configuration file for the database.

To do this:

```
$ sudo editor /etc/acidbase/database.php
```

Make sure that the following variables are set in the same way in the file:

```
$alert_user='snort';
$alert_password='snortpwd';
$alert_dbname='snort';
$DBtype='mysql';
```

If you make any changes, save and exit.

Navigate to your new BASE webpage (substitute X with the number of your group)

```
http://10.10.X.10/acidbase
```

You will now see a message like the following:

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

The database version is valid, but the BASE DB structure (table: acid_ag)
```

```
is not present. Use the Setup page to configure and optimize the DB.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Follow the directions in that page to update the database (Create BASE AG)
Then, use the link in the top left to navigate to the "Home" page.

You will see a dashboard containing the following:

* On the top left corner, a list of links to alert reports, classified by
  various criteria
* Below that, alert statistics, including percent bars of traffic by type
* At the bottom, a menu with several administrative options.

## Set up authentication

In a production install, Snort alerts are very sensitive information, so
we need to add authentication to this web front-end. Let's create a user
for us to log in with.

* Go to the bottom menu and click on "Administration"
* Click on "Create a User"
* Login: "sysadm"
* Full Name: "System Administrator"
* Password: Type the sysadm password you used to log in to the PC
* Role: "Admin"
* Click on "Submit Query"

Now, we need to configure BASE so that it requires authentication.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# sudo editor /etc/acidbase/base_conf.php
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

  find this line

$Use_Auth_System = 0;

  and change it to:

$Use_Auth_System = 1;
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Save and exit.

From now on, if you try and access your acid installation, it will require
a login + password.

## Setup Apache2 SSL

We have set up acidbase to require authentication. However, we are now
vulnerable to password sniffing because the web server is not encrypting
the communications channel. To fix that, let's enable SSL for Apache2:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo a2enmod ssl
$ sudo a2ensite default-ssl
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Then, tell Apache that SSL is required for the acidbase pages:
```

~~~~~~
sudo editor /etc/acidbase/apache.conf

  add the following line inside the <DirectoryMatch> section:

SSLRequireSSL
~~~~~~

Save and restart Apache:

~~~~~~
$ sudo service apache2 restart
~~~~~~

You should be able to view your BASE using the https:// method in the URL:

~~~~~~
https://10.10.X.10/acidbase
~~~~~~

(Since we are using the default self-signed certificate, you will probably have
to create an exception in your browser).

You will be asked to authenticate. Log in with the "sysadm" account you created.

Operation

Exporting to e-mail for collaboration

BASE does not send automatic e-mail alerts, but you can set it up so that
you can select one or more alerts and send their details to your colleagues
in an e-mail message.

For this to work, you will need to install a mail transfer agent. For example:

~~~~~~
$ sudo apt-get -y install postfix
~~~~~~

* When asked about the type of mail configuration, select "Internet Site".
* System mail name: It should be the full name of your server, for example
  "pc1.ws.nsrc.org"

Also, make sure that you have the PHP mail module installed:

~~~~~~
$ sudo apt-get -y install php-mail
~~~~~~

Then, proceed to set some necessary variables in the BASE configuration file.
The following values should work (substitute pc# with you actual pc name):

~~~~~~
sudo editor /etc/acidbase/base_conf.php

$action_email_smtp_host = 'localhost';
$action_email_smtp_localhost = 'localhost';
$action_email_smtp_auth = 0;
~~~~~~

```
$action_email_smtp_user = 'username';
$action_email_smtp_pw = 'password';
$action_email_from = 'snort@pc#.ws.nsrc.org';
$action_email_subject = 'BASE Incident Report';
$action_email_msg = '';
$action_email_mode = 0;
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Now, let's test it sending e-mails.

* In the dashboard, click on "Today's Alerts: unique"
* Select one or more alerts.
  (if you don't have any alerts today, ask the members of a different group
  to scan your computer's ports with nmap, for example).
* In the drop-down menu on the bottom, select "Email alerts (full)"
* In the ACTION box, type "sysadm@pc#.ws.nsrc.org"
* Click on the "Selected" button

Check your mail. Either use a mail client like mutt, or simply type:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo cat /var/mail/sysadm
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

More information

The BASE project homepage includes links to mailing lists, online forums,
etc:

http://base.secureideas.net/