Installing Snort, MYSQL, and ACID in an Enterprise Environment with a Centralized Logging Console and Distributed Sensors.

Wayne Freeman, MCSE, GSEC
Glamdring@inetsecurity.info

DRAFT

In this document I will outline the basic installation steps for setting up a distributed Intrusion Detection System. We will be using Snort, MYSQL, Apache, and ACID to create IDS sensors which will log to a centralized IDS console. Administrators will be able to access the console and centrally view and administer the IDS.

This document assumes you know how to install FreeBSD, and set up the networking and other related necessary items. You also need to have your System Admins add the necessary information for your BSD machines into your internal DNS, DHCP, ad WINS if you are in a Windows environment. The DHCP entries should be address reservations for each BSD machine, and the WINS entries should be static. <u>DO NOT</u> add your sensors or the console to any externally available machines such as your public DNS.

In our network our intrusion detection sensors are running on single pentium 166mhz machines with 96 meg of RAM, and a 4 gig SCSI hard drive and dual NICS. Our central console is a single Pentium 500, 128 meg of ram, and a 9gig SCSI drive with a single NIC.

Each sensor is monitoring an incoming 10meg pipe, with no performance problems to date.

This paper will not discuss how to administer or secure the operating system, MySQL, or Apache. I know there are many papers out there already dealing with these issues. Hopefully some of this can be incorporated in the future, but for now I am focusing on the installation of the IDS and its dependencies.

Installing the Snort Logging Console Machine

1) Install the latest stable version of FreeBSD
2) Create any necessary user accounts and create a root password
3) Under the /home directory create a subdirectory called software. Move all the tarballs into this subdirectory. You need the following tarballs. Get the latest versions. You may run into some issues with newer versions, I have dealt with those I ran into here when using these versions.

   -Mysql-3.23.49.tar.gz
   -Snort-1.8.6.tar.gz
   -httpd-2.0.39.tar.gz (Apache Web server)
   -php-4.2.1.tar.gz
   -phplot-4.4.6.tar.gz
   -adodb-2.0.tar.gz
   -acid-0.9.6b20.tar.gz
   -pth-1.4.1.tar.gz
   -phpMyAdmin-2.2.6.tar.gz

4) Untar all the above files:

-tar zxf filename.tar.gz

-each file will create its own subdirectory under /home/software/ and will be called app-x.x.x (ie mysql-3.23.49)

5) The order of installation matters when it comes to this due to dependencies and modules. Please note we are altering the default install directories for these programs. The -prefix=/home/xxxx is where we will be installing the programs. MySQL will be in /home/mysql, Apache will be in /home/www and so forth. We did this to make it easier to administer. Install in the following order:

A) Mysql

```
# cd /home/software/mysql-3.23.49
# ./configure --prefix=/home/mysql
# make
# make install
```

- add a mysql group # pw groupadd mysql
- add a mysql user #adduser -g mysql mysql
- create the main system tables

```
    # /home/mysql/mysql_install_db
```

- from # /home/mysql/share/mysql select the template that suits your needs best (my-medium.cnf etc) and copy it as my.cnf under the /etc directory

```
    # cp /home/mysql/share/mysql/my-medium.cnf /etc/my.cnf
```

-Change the owners of the mysql directories

```
    # chown -R root /home/mysql
    # chown -R mysql /home/mysql/data
    # chgrp -R mysql /home/mysql
```

-Start the mysql server

```
    # /home/mysql/bin/safe_mysqld --user=mysql &
```

- set the password for root in mysql (this can be done later using phpmysqladmin)

B) PTH

```
# cd /home/software/pth-1.4.1
# ./configure
# make
# make install
```

C) You need to edit one of the PHP files after you untar it but before installing Apache or PHP.

```
# cd /home/software/php-4.2.1/sapi/apache2filter/
# ee php_functions.c (edit this file, I use ee)
```

- You must change wording MODULE_MAGIC_AT_LEAST with AP_MODULE_MAGIC_AT_LEAST (about line 93) save the changes.

D) Install Apache

```
# cd /home/software/apache-2.0.39
# ./configure --prefix=/home/www --enable-module=so
# make
# make install
```

E) Install PHP

```
# cd /home/software/php-4.2.1
# ./configure --with- mysql --with-tsrm-pth --with-apxs2=/home/www/bin/apxs
# make
# make install
# copy the php.ini-dist file to /usr/local/bin/php.ini
        cp php.ini-dist  /usr/local/bin/php.ini
```

- edit the php.ini file and rem out error reporting
- edit the httpd.conf file and add
    - -AddType application/x- httpd-php .php
    - - make sure your server root, document root and any other settings are set as needed

F) Go to your browser and point it to http://localhost or from another machine point it to http://servername and you should see the apache default page.

G) Create the snort database and tables. The script to create the tables is in the /contrib subdirectory under /home/software/snort-1.8.6

```
# /home/mysql/bin/mysql -u root -p
- input the password for root account on mysql
>CREATE DATABASE snort;
>grant INSERT, SELECT on snort.* to root@localhost;
>quit
# /home/mysql/bin/mysql -u root -p < /home/software/snort-1.86/contrib/create_mysql snort
- log in to mysql and check the tables exist
        >use snort
        >show tables;
```

H) install ACID, ADODB, and PHPLOT

- delete everything in the subdirectory /home/www/htdocs
- In /home/www/htdocs create a subdirectory called adodb, another called phplot-4.4.6 and a third called phpmyadmin
- copy the files and subdirectories from /home/software/adodb to /home/www/htdocs/adodb
- copy the files and subdirectories from /home/software/phplot-4.4.6 to /home/www/htdocs/phplot-4.4.6
- copy the files and subdirectories from /home/software/acid to /home/www/htdocs
- copy the files and subdirectories from /home/software/phpMyAdmin-2.2.6 to /home/www/htdocs/phpmyadmin

-go to /home/www/htdocs and edit the file acid_conf.php. You need to provide a user ID and password, as well as the correct database name.

- use your browser and go to http://localhost/ You should see the first page of the ACID browser. You will be asked if you want to create the acid tables in the database. Choose to do so. Upon refreshing you should see the ACID page.

-go to /home/www/htdocs/phpmyadmin and edit the file config.inc.php. You need to provide a user ID and password, as well as the correct full url to the phpmyadmin subdirectory.

- Browse to http://localhost/phpmyadmin/index.php and you will see all the options for configuring your MySQL database. Choose the users option.

-Make certain the account you are going to use for your snort logging has the necessary permissions on the snort database.

TO DO:

- deal with user access restrictions (should be intranet access only)
- SSL from sensors to Console

Installing Snort as a sensor on FreeBSD

1) Install FreeBSD 4.6 or latest version with dual network cards.

2) Download the following source files:

Mysql-3.23.49.tar.gz (or latest from www.mysql.com)
Snort-1.8.6.tar.gz (or latest from www.snort.org)
Snortrules.tar.gz (the latest rules from www.snort.org)
Libpcap-0.7.1.tar.gz (or latest from www.tcpdump.org)

3) Move the above files to a central storage area. We use /home/software

```
# mv *.tar.gz  /home/software
```

4) Change to /home/software and untar Libpcap, mysql, snort rules, and snort

```
# cd /home/software
# tar zxf libpcap-0.7.1.tar.gz (untars to subdirectory called libpcap-0.7.1)
# tar zxf snort-1.8.6.tar.gz (untars to subdirectory called snort-1.8.6)
# tar zxf snortrules.tar.gz (untars to subdirectory called rules)
# tar zxf mysql-3.23.49.tar.gz (untars to subdirectory called mysq-3.23.49)
```

5) install Libpcap

```
# cd libpcap-0.7.1
# ./configure
# make
# make install
```

6) Install Mysql client

```
# cd ..
# cd mysql-3.23.49
# ./configure --without-server
# make
# make install
```

7) Install snort with MySql support

```
# cd ..
# cd snort-1.8.6
# ./configure --with- mysql
# make
# make install
```

8) Create a snort subdirectory under /etc

```
# cd /etc
# mkdir snort
```

9) copy or move all the .rules files from /rules to /etc/snort

```
# cd /home/software/rules
# cp *.rules /etc/snort/
```

10) Copy the classification.config file to the root of /etc

```
# cp classification.config /etc/
```

11) Copy the snort.conf file to the root of /etc

```
# cp snort.conf /etc/
```

12) Copy the MySQL libraries file from /usr/local/lib/mysql to /usr/lib

```
# cd /usr/local/lib/mysql
# cp libmysqlclient.so.10 /usr/lib/
```

13) Create a script file in the /root directory to run snort.

```
# cd /root
# ee snort.sh
```

There should be one line in the file.....

```
snort -D -d -i fxp1 -c /etc/snort.conf
```

The -i defines the interface you want snort to listen on. As you have 2 nic's, one will plug into your internal network to communicate with the console and Mysql database, and the other will plug into your tap, hub, or spanning port to monitor the traffic.

If you run ifconfig at the prompt you will see a listing of your interfaces. They will be fxp0 and fxp1. Normally the interface which you used to do the install will be fxp0. It will have will show inet <ip address netmask broadcast> where the ip address will be the one you assigned during setup. The fxp1 should have nothing in it. This is ok as snort does not need an ip address or stack to see the traffic.

Once you start snort you will see that fxp1 shows as <Up,Broadcast,Running,Promisc,Simplex,multicast> with an active status. The Promisc is the important item, your nic must be in promiscuous mode for snort to work.

14) edit snort.conf to reflect your setup.

```
# cd /etc
# ee snort.conf
```

Set var HOME_NET to your internal network

Set var RULE_PATH

```
Var RULE_PATH /etc/snort/
```

Set your output plugins in section 3. This is where you tell it to log to the database. You need to uncomment the line:
Output database: log, mysql, user=snort password=snort dbname=snort host=192.168.1.1 sensor_name=TAC_Pipe_1

Replace the word snort in all 3 places with the appropriate user id, password and database name for your system (these were created when you installed the console) and replace the IP with the internal IP of your central logging console. I added the sensor_name= item because if you don't assign a sensor name snort assigns its own and it will likely mean little to you as you review log items. Also replace the word log with the word alert to log portscans to the database.
Review the included rules at the bottom and make any necessary changes.

15) Start snort

```
# cd /root
# sh snort.sh
```

.
We use the one way cable on our external facing NICS. Here is the pin out we based our cables on.

One way Ethernet Cable Pinout Diagram*

Clip pins 3 and 10 for one way (receive-only) Cable

```
 1               8
___________________
\ . . . . . . . . /
 \ . . . . . . . /
  \-------------/
   9          15
```

Pin	Signal	Description
1	GND	
2	CI-A	Control In Circuit A
3	DO-A	Data Out Circuit A
4	GND	
5	DI-A	Data In Circuit A
6	VC	Voltage Common
7	-	
8	GND	
9	CI-B	Control In Circuit B
10	DO-B	Data Out Circuit B
11	GND	
12	DI-B	Data In Circuit B
13	VP	+12 Volts DC
14	GND	
14	GND	

*From www.silicondefense.com (with edits)

Updating Apache to version 2.0.39 from 2.0.36 (chunking vulnerability)

Download the latest tars and put them in /home/software. You need to recompile php-4.2.1 as well in this process due to changes. Then in /home/software

```
1) # tar zxf httpd-2.0.39.tar.gz
2) # tar zxf php-4.2.1.tar.gz
3) # cd php-4.2.1/sapi/apache2filter/
4) # ee php_functions.c (edit this file, I use ee)
5) You must change wording MODULE_MAGIC_AT_LEAST with
AP_MODULE_MAGIC_AT_LEAST (about line 93) save the changes.
6) # cd /home/software/apache-2.0.39
7) # ./configure --prefix=/home/www --enable-module=so
8) # make
9) # make install
10) recompile PHP
11) # cd ..
12) # cd php-4.2.1
13) # ./configure --with- mysql --with-tsrm-pth --with-apxs2=/home/www/bin/apxs
14) # make
15)#  make install
```

Points 3, 4, and 5 correct the "sapi_apache2.c" version is incorrect error you receive when trying to run ./apachectl start after making these.