

Tutorial for a Basic Snort/MySQL install on FreeBSD 4.4 Stable

by twigles

Purpose of document

This document is based on FreeBSD 4.4 Stable, Snort 1.8.3 and MySQL 3.23.42. The intention is to give users that are new to any of the three pieces of software the opportunity to build an enterprise-class system based completely on free, open-source tools. Following the instructions in this document will get you the following:

- A headless FreeBSD box (no X, no mouse)
- A pretty secure box
 - netstat -a will show you SSH and MySQL listening
 - No root logins
 - SFTP instead of FTP
- Snort logging to MySQL
- The fastest NIDS for your money

Following my instructions will NOT give you the following:

- The only possible way to get this done
- The most secure box possible (out-of-scope, do a google search)
- An output method to view the MySQL logs – I'm still looking for a scalable, easy and secure way to do this on a headless machine.

Assumptions

Although this document helps you through the install procedure, I assume that you have compatible hardware. If you suspect otherwise, please check here:

http://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/hardware.html.

I also assume that you have a bootable CD with FreeBSD 4.4 Stable on it and BIOS that allow you to boot to cdrom. If that is not the case, go here:

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/install.html.

Or buy the FreeBSD Power Pack (make sure it's for version 4.4). If you plan on using FreeBSD a lot, you should definitely buy this package as it comes with the FreeBSD Handbook and more third-party software than you can shake a stick at.

Another assumption is that you will use this machine as a dedicated Snort sensor, which implies simplicity and security.

Install FreeBSD 4.4 Stable

Skip kernel configuration and continue with installation

Choose standard installation

ok

Use entire disk in one slice (type 165)

FreeBSD bootloader

ok

This is my file system layout on a 9 Gigabyte hard drive.

<u>Size</u>	<u>Mount Point</u>
300M	/
1000M	swap
400M	/usr
300M	/tmp
6746M	/var

Choose minimal install

Choose from CD or FTP...

ok

ok after congratulations

Choose yes to configure ethernet card

Configure your ethernet card. For example my 3com card is fxp0

Choose no to ip6

Choose no to dhcp

Enter your IP information, make sure you choose a correct name server for later

Choose yes bring the interface up now

Choose no as gateway

Choose yes to inetd (all off by default) ****See below****

Choose yes to confirm inetd

Choose no to use current settings

Choose no to anon ftp

Choose no to nfs server

Choose no to nfs client

Choose no, use moderate security

ok

Choose no to customize console settings

Choose yes to set time zone

Choose no

Choose your time zone

Yes to 'PST'

Choose no to Linux compatibility

Choose no to USB mouse

Choose exit this menu, this is a headless station

Choose no, don't configure X

Choose no, don't browse/install ports collection

Choose yes, add user account – this is who you will SSH into the box as initially

Choose user - add new user to the system

Login id is snort

uid is 1001

group is wheel

password - snortman

all else blank, ok

exit this menu

ok to set root passwd – snortman5000

Choose no, don't do any last minute options
exit install
Choose yes, you're sure, remove all bootable media

That's it!

inetd

**You can choose to install inetd if you want and simply turn everything off. This way if you need an FTP server for some reason you can turn it on and then turn it off when you're done. Personally I do the base install from the console and then SSH into the box from my Windows machine (nice graphics card, 21' monitor) using this client: <http://www.ssh.com/products/ssh/download.cfm>. This way I have multiple windows and the ability to scroll up and down. Please note that although this is a free download, there are license restrictions. I AM NOT RESPONSIBLE FOR YOUR COMPLIANCE WITH SSH.COM'S LICENSE RESTRICTIONS. If you don't think you are eligible to use this client freely, buy it or use Putty.

Your first boot

On first boot BSD will generate SSH keys and sendmail will hang boot for about a minute

```
mv /etc/motd /etc/motd.default
```

vi motd, insert your warning banner (leave 2 empty lines at top, or they WILL be erased)
edit /etc/rc.conf, comment out sendmail and usbd (change to NO)

If you installed inetd, leave inetd.conf alone-everything is disabled by default. Or for peace of mind, check it out yourself and make sure everything has a pound sign in front of it.

MySQL – Downloading the necessary packages

Personally I like to put all of the packages into /usr so I make sure I'm in /usr when I start my FTP session.

Goto <ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-4.4-release/>

Grab from databases:

```
mysql-client-3.23.42.tgz
```

```
mysql-server-3.23.42.tgz
```

```
p5-DBI-1.19.tgz
```

```
p5-Mysql-modules-1.2216.tgz
```

Grab from devel:

```
p5-Data-ShowTable-3.3
```

MySQL – adding the packages

Do the pkg_add in this order (other orders may work, but I know this one does):

```
pkg_add p5-DBI-1.19.tgz
```

```
pkg_add p5-Data-ShowTable-3.3.tgz
```

```
pkg_add mysql-client-3.23.42.tgz
```

```
pkg_add p5-Mysql-modules-1.2216.tgz
```

```
pkg_add mysql-server-3.23.42.tgz
```

The user and group "mysql" are added with the server package, and a startup script is automatically put in /usr/local/etc/rc.d. MySQL will now start on boot.

Setting up basic MySQL functionality

Run the following commands as root:

```
/usr/local/bin/mysql_install_db  
/usr/local/etc/rc.d/mysql-server.sh start
```

Do a "netstat -a". It should show port 3306 listening.

Do a "ps -aux". It should show "/usr/local/libexec/mysqld --basedir=/usr/local --datadir=/var/db/mysql --user=mysql"

Kill mysqld process – "/usr/local/etc/rc.d/mysql-server.sh stop"

Change directory to /usr/local/share/mysql. Look through the four different .cnf files to see which one matches your situation best. Personally I used "my-large.cnf" so I did the following:

```
cp /usr/local/share/mysql/my-large.cnf /etc/my.cnf  
restart mysqld
```

As root at shell type "/usr/local/bin/mysql"

To change the root passwd to "snortman", at mysql prompt type:

```
SET PASSWORD FOR root@localhost=PASSWORD('snortman');
```

For the changes to take affect type

```
FLUSH PRIVILEGES;
```

```
quit
```

* Don't forget the semi-colon at the end of every command in MySQL except quit.

Now type "/usr/local/bin/mysql" and you should get rejected.

Type "/usr/local/bin/mysql -p" and enter the password when prompted.

Quit again, it's time to install Snort

Downloading and installing Snort

Again, I happen to like having these things in /usr so that's where I sit when I start my FTP session. This is strictly preference.

Libpcap

download libpcap-0.6.2.tar.gz (www.tcpdump.org)

```
gunzip libpcap-0.6.2.tar.gz
```

```
tar -xf libpcap-0.6.2.tar
```

```
ln -s libpcap-0.6.2 libpcap
```

```
cd libpcap
```

```
./configure
```

```
make
```

```
make install
```

Snort

download snort-1.8.3.tar.gz. There isn't an FTP site so get it somehow.

```
gunzip snort-1.8.3.tar.gz
tar -xf snort-1.8.3.tar
ln -s snort-1.8.3 snort
cd snort
./configure --with-mysql=/usr/local/libexec
make
make install
```

Type "snort -v" to test if Snort is working. This starts snort in sniffer mode.
Stop Snort with [ctrl-c]

*** Note that mysql is only in /usr/local/libexec because I used the FreeBSD package. If you install it from binary, it will be in a different place.

Telling Snort to log to MySQL

vi /usr/snort/snort.conf and edit it to reflect your network. I will not go into this here since it is covered in wonderful detail in the Snort User's Manual. However I will tell you what to change to log to MySQL.

In Section 3 change the following:

Under the database section add or modify existing line to read:

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

*** Note: If you edit the rules files in Notepad you MUST go into vi and remove the "^M"s

Setting up MySQL to accept data from Snort

Set up the mysql database for snort with the included scripts:

```
As root at shell type "echo "CREATE DATABASE snort;" | /usr/local/bin/mysql -u root -
p"
```

```
Log into mysql and type "grant INSERT,SELECT on snort.* to root@localhost;"
```

```
Quit mysql
```

```
Change directory to /usr/snort, then type "/usr/local/bin/mysql -p <
```

```
./contrib/create_mysql snort"
```

```
Type "mkdir /var/log/snort"
```

Log into mysql and verify your snort tables:

```
mysql> use snort
Database changed
mysql> show tables;
+-----+
| Tables_in_snort |
+-----+
| data            |
```

```

| detail      |
| encoding    |
| event       |
| icmp_hdr    |
| ip_hdr      |
| opt         |
| reference   |
| reference_system |
| schema      |
| sensor      |
| sig_class   |
| sig_reference |
| signature   |
| tcp_hdr     |
| udp_hdr     |
+-----+
16 rows in set (0.00 sec)

```

mysql>

This is my snort startup script. Put this in /usr/local/etc/rc.d.
Don't forget to chmod 750 it.

```
#!/bin/sh
```

```
sleep 5
```

```
case "$1" in
  start)
```

```
    if [ -x /usr/local/bin/snort ]; then
```

```
        /usr/local/bin/snort -c /usr/snort/snort.conf -D > /dev/null & && echo -n '
snort'
```

```
    fi
```

```
    ;;
```

```
stop)
```

```
    /usr/bin/killall snort > /dev/null 2>&1 && echo -n ' snort'
```

```
    ;;
```

```
*)
```

```
    echo ""
```

```
    echo "Usage: `basename $0` { start | stop }"
```

```
    echo ""
```

```
    exit 64
```

```
    ;;
```

```
esac
```

Reboot your box

As root type “shutdown -r now” or “reboot”