Install Snort on FreeBSD

Step-By-Step instructions on how to Install snort on FreeBSD.

1. Login to your computer as **root** or elevate to **su**

2. First we have to compile snort form the ports tree by running this command:

make -C /usr/ports/security/snort install all

You will be asked about which support you want to add to snort here you can pick MySQL if you are going to use the server as traffic monitor or instruction detection system. For me I took the defaults only because I capture the files and export them to log file using **snort –dev –l . /log** then I read them with **tcpdump –r**. But again it really depends on your needs.

3. Next you need oinkmaster to update your snort rules so run this command

make -C /usr/ports/security/oinkmaster install all

4. You can update your snort rules using this command:

oinkmaster -o /usr/local/etc/snort/rules/

5. If you decided to install MySQL you will need to create a database so login to mySQL

mysql -u root –p password

6. After you enter the root username and password you are going to be dropped to this prompt

mysql>

7. Type the following two commands

CREATE DATABASE `snort`;

GRANT ALL PRIVILEGES ON snort.* TO 'snort'@'localhost' IDENTIFIED BY 'snortpassword';

8. Next control +C to exit mysql server you will now need to create the tables but lucky for us snort can do that for you so type this command

mysql -u snort -psnortpassword snort < /usr/local/share/examples/snort/create_mysql

9. We need to uncomment 3 lines from the snort config file so run this command

Vi /usr/local/etc/snort/snort.conf

10. Then uncomment meaning remove the # from in front of the line

config detection: search-method lowmem

output alert_syslog: LOG_AUTH LOG_ALERT

output database: log, mysql, user=root password=test dbname=db host=localhost

11. If you want snort to run at startup type which if you're running snort at either a traffic monitor or instruction detection system you're going to want to happen.

Vi /etc/rc.conf

12. Add this line

snort_enable="YES"

Now restart your computer and snort will be running at startup and logging to MySQL.