Getting SNORT working in OpenBSD 5.x and VirtualBox 5.x.x

Last Revised on December 24, 2015

The document below uses the following color codes for items/steps the user should be aware of during the configuration and installation of DAQ-2.0.x and Snort-2.9.8.x:

Blue - informational messages and comments
Orange – These are commands that the user types at the shell prompt
Red – **Read carefully before proceeding**.

This document describes the manual configuration, compiling, and installation of DAQ-2.0.x and Snort 2.9.8.x using the Hardware and Operating System(s) listed below

Microsoft Windows 7 Professional Edition w/SP1 as the HOST operating system
VirtualBox 5.x.x with Oracle Extension Pack 5.x.x (I use version 5.x.1x)
OpenBSD 5.x (64-bit version) as the GUEST operating system (which runs SNORT)
SNORT 2.9.8.x, DAQ 2.0.x, and a set of snort rules (www.snort.org)

The hardware in the HOST system listed above is a Turion TL-58 processor (AMD) @ 2.0Ghz, 4GB of 667Mhz SO-DIMM RAM, and a onboard Marvel Yukon PCIe Gigabit Ethernet Controller.

*** NOTE ***

Before replacing a WORKING production copy of Snort with a new version of Snort and updated Snort rules, it is STRONGLY recommended that users set up a test environment to install the latest versions of DAQ and Snort (along with updated Snort rule snapshots) and to fully test any potential modifications in this environment.

I prefer to use a Virtual Machine inside of VirtualBox 4.x.x/5.x.x when installing and/or upgrading Snort, so if something goes wrong, I can simply remove the virtual machine and reload the operating environment from scratch, without damaging any production systems that may be running Snort or other critical services.

*** NOTE ***

In the OpenBSD 5.x Virtual Machine, you will need to set the NETWORK section to BRIDGED mode to allow the assignment of a static IP to your OpenBSD 5.x VM (if you are using a standalone system running OpenBSD 5.x you can ignore this step).

In OpenBSD 5.x. configure your IP address and network mask in /etc/hostname.em<x> where <x> is the interface number (i.e. - em0 for ethernet0), the gateway IP address can be configured in /etc/mygate, the DNS IP address in /etc/resolv.conf, and the hostname in /etc/myname.

If you're doing an initial install of OpenBSD 5.x will ask you for the above information (in my case, I used ethernet 0 (em0) as the port to monitor traffic on) and stop/start or restart the em0 interface on OpenBSD 5.x via /etc/netstart.

After completing the step above, ensure your network connectivity is working (try ping www.cisco.com, you should get a response), also try surfing a few web pages from OpenBSD 5.x, but www.snort.org would be a good site to visit (shameless plug here).

Make sure the following packages are installed in your OpenBSD 5.x system before attempting to configure/compile DAQ 2.0.x and SNORT 2.9.8.x:

gcc version 4.2.x (including libraries) (or greater)
zlib version 1.2.3 (or greater)
pcre version 8.21 (or greater), DAQ and Snort require a PCRE version of 6 or higher
libpcap version 1.0.0 (or greater)
libiconv version 1.14 (needed by **bison** version 2.3)
gettext version 0.18.1 (needed by **bison** version 2.3)
bison version 2.3 (or greater)
flex 2.5.4 (or greater)
libdnet version 1.12 including **libdnet-devel**
tcpdump version 4.0.0 (or greater)

Versions of these packages already installed may be newer than what is listed here, but should NOT cause any issues when compiling DAQ and/or SNORT.

I downloaded the following packages from www.openbsd.org using a HTTP mirror located on the website and going to the Packages directory for the specific type of install I did (in this case, OpenBSD 5.x and amd64):

libiconv-1.14.tgz	(OpenBSD 5.1 or 5.2)
gettext-0.18.1p1.tgz	(OpenBSD 5.1)
bison-2.3.tgz	(OpenBSD 5.1)
libdnet-1.12p4	(OpenBSD 5.1 or 5.2)
pcre-8.21.tgz	(OpenBSD 5.1)
gettext-0.18.1p3.tgz	(OpenBSD 5.2)
bison-2.3p0.tgz	(OpenBSD 5.2 or 5.3)
pcre-8.30.tgz	(OpenBSD 5.2)
libiconv-1.14p0.tgz	(OpenBSD 5.3)
gettext-0.18.2p1.tgz	(OpenBSD 5.3)
libdnet-1.12p5	(OpenBSD 5.3)
pcre-8.31.tgz	(OpenBSD 5.3)

All of the **commands that follow** should be issued as the '**root**' user:

To install the above packages (which should be done in descending order), type the following commands (if successful, you'll see an 'OK' message printed):

For OpenBSD 5.1 or 5.2

pkg_add -v <path to>libiconv-1.14.tgz <enter>
pkg_add -v <path to>libdnet-1.12p4.tgz <enter>

For OpenBSD 5.1

pkg_add -v <path to>gettext-0.18.1p1.tgz <enter>
pkg_add -v <path to>bison-2.3.tgz <enter>
pkg_add -v <path to>pcre-8.21.tgz <enter>

For OpenBSD 5.2

pkg_add -v <path to>gettext-0.18.1p3.tgz <enter>
pkg_add -v <path to>bison-2.3p0.tgz <enter>
pkg_add -v <path to>pcre-8.30.tgz <enter>

For OpenBSD 5.3

pkg_add -v <path to>libiconv-1.14p0.tgz <enter>
pkg_add -v <path to>bison-2.3p0.tgz <enter>
pkg_add -v <path to>gettext-0.18.2p1.tgz <enter>
pkg_add -v <path to>libdnet-1.12p5 <enter>
pkg_add -v <path to>pcre-8.31.tgz <enter>

cd /usr/local/lib <enter>
ldconfig -r -m -v /usr/local/lib <enter>

When upgrading to the newest version of snort, it is **strongly recommended** to **back up local.rules, snort.conf, threshold.conf**, **white_list.rules**, and **black_list.rules** before any snort upgrade is installed.

Note: The steps in this document should apply to compiling DAQ 2.0.x and SNORT 2.9.7.x without any changes in actual configuration or makefiles (except the paths to the actual source files, etc).

I decided to download libpcap 1.3.0 from www.tcpdump.org since the default install of OpenBSD 5.x did not contain the necessary version of libpcap or libpcap-devel to allow DAQ-2.0.x or Snort 2.9.8.x to compile properly.

Also, the ‘src’ directory under ‘/usr/local’ does NOT exist after an OpenBSD 5.x install is completed, to make this directory, type the following command (as the root user):

cd /usr/local <enter>
mkdir -p src <enter>

After obtaining libpcap-1.3.0, unpack, configure, and compile it as follows:

cd /usr/local/src <enter>
tar -zvxf <path to>libpcap-1.3.0.tar.gz <enter>
./configure <enter>

Note any errors which may cause the 'configure' step to abort, also, you can check the file ‘**config.log**’ which is generated from the ‘configure’ line above.

make <enter>
make install <enter>

The ‘make install’ will place the **pcap** libraries in directory ‘/usr/local/lib’ and the **pcap** header files in directory ‘/usr/local/include’

cd /usr/local/lib <enter>
ldconfig -m -r -v /usr/local/lib <enter>

Obtain **SNORT** (version 2.9.8.x), **DAQ** (version 2.0.x), and the latest available snort rule set from www.snort.org and download them to your OpenBSD 5.x box.

The steps below also apply to compiling **Snort 2.9.6.x**.

The steps below will require '**root**' access and terminal/console access in order to successfully complete the compilation, installation, and running of SNORT on your OpenBSD 5.x box.

First, unpack the source code for DAQ 2.0.x and Snort 2.9.8.x:

cd /usr/local/src <enter>
tar -zxvf <path to>daq-2.0.x.tar.gz <enter>
tar -zxvf <path to>snort-2.9.8.x.tar.gz <enter>

Do the following to configure and compile DAQ 2.0.x:

cd /usr/local/src/daq-2.0.x <enter>
./configure --with-libpcap-libraries=/usr/local/lib --with-libpcap-includes=/usr/local/include <enter>

Note any errors which may cause the 'configure' step to abort, also, you can check the file '**config.log**' which is generated from the 'configure' line above.

make <enter>
sudo make install <enter>
ldconfig -m -v -r /usr/lib /usr/local/lib <enter>

Do the following to configure and compile Snort 2.9.8.x:

cd /usr/local/src/snort-2.9.8.x <enter>

I **strongly recommend** that you read the INSTALL file under the '**snort-2.9.8.x/doc**' directory for potential issues regarding the OpenBSD operating system (esp. the **–disable-static-daq** option, and **symlinks for libsf_engine.so.0 or libsf_engine.so.0.0**) before proceeding with the steps below.

Do the following to configure, compile, and install SNORT on your OpenBSD 5.x system:

./configure --enable-sourcefire --with-libpcap-libraries=/usr/local/lib --with-libpcap-includes=/usr/local/include --with-daq-includes=/usr/local/include --with-daq-libraries=/usr/local/lib --disable-static-daq <enter>

Note: Joel Esler at sourcefire.com recommends using the 'enable-sourcefire' option

Note any errors which may cause the 'configure' step to abort, also, you can check the file '**config.log**' which is generated from the 'configure' line above.

make <enter>
sudo make install <enter>
ldconfig -m -v -r /usr/lib /usr/local/lib <enter>

Per the INSTALL document in the snort-2.9.8.x source code tree (under the **doc** directory), OpenBSD 5.x **does not create** the necessary **symbolic links** (symlinks) for **libsf_engine.so** (which is a **shared library**), so type the following commands below to create the symlinks on your system:

cd /usr/local/lib/snort_dynamicengine <enter>
ln -s libsf_engine.so.0.0 libsf_engine.so <enter>

In order to download snort rules from www.snort.org, you must be a **registered user** or have a **paid subscription** to download rule sets or VRT rules. Information can be found at www.snort.org on how to become a **registered user**. **Registered users** will be able to download rule sets which are **approximately one month behind** what is available to paid subscription holders.

Issue the commands below:

cd /etc <enter>
mkdir -p snort <enter>
cd snort <enter>
cp /usr/local/src/snort-2.9.8.x/etc/* . <enter>
tar -zvxf <path to>snortrules-snapshot-<nnnn>.tar.gz <enter>
touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules <enter>

Note - this will place the configuration files from the snort 2.9.8.x unpack and the rules snapshot under the /etc/snort directory. If the rules snapshot file is newer, this is not an issue (since rules are updated on a periodic basis by the snort team).

Also, the configuration files (e,g, - snort.conf, threshold.conf, etc) are residing in /etc/snort and the rules files will be in /etc/snort/rules and for the so_ and preprocessor rules, these will be located in /etc/snort.

Add the following line to file /etc/passwd (or use the 'useradd' or 'adduser' command. Note – I used the 'adduser' command as it allows you to set shell, login, group, etc):

snort:*:40000:0:Snort IDS:/var/log/snort:/usr/sbin/nologin

Add the following line to file /etc/group: (or use the 'groupadd' command):

snort:*:40000:snort

Issue the commands below in order to take ownership of all files in /etc/snort:

cd /etc/snort <enter>
chown -R snort:snort * <enter>

Locate and modify the following variables in your snort.conf file (in directory /etc/snort) as follows (found between lines 40 and 120 in snort.conf):

This assumes the network you are going to monitor is 192.168.1.0/24

var RULE_PATH /etc/snort/rules
ipvar HOME_NET 192.168.1.0/24
ipvar EXTERNAL_NET !$HOME_NET
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

Also, at www.snort.org/docs there are a set of initialization scripts which are available for various operating systems, including OpenBSD 5.x. These scripts are available due to the fact that some users have reported problems copying and pasting the script below when it is in the form of a PDF document.

I have fixed the snort startup script in OpenBSD 5.x, as the items which were preventing the script from working was the lack of ‘rc_’ in front of start, stop, status, and restart.

Place the shell script below into the /etc/rc.d directory on your OpenBSD 5.x box:

----- CUT HERE -----

```
#!/bin/sh
#
#       Snort Startup Script modified for OpenBSD 5.1/5.2
#
#       Original Script from Spanish Honeywell Project (2004)
#
#       Script modified to add status parameter to 'usage'
#
#       Added prefix of 'rc_' on 10/17/2012 to each option in the script
#       (i.e. - start becomes rc_start, stop becomes rc_stop, etc)
#

# Script variables (modify to match your system layout)

LAN_INTERFACE=em0
RETURN_VAL=0
BINARY=/usr/local/bin/snort
PATH=/bin:/usr/local/bin
PID=/var/run/snort_${LAN_INTERFACE}_ids.pid
LOGDIR=/var/log/snort
DATE=`/bin/date +%Y%m%d`
CONFIG_FILE=/etc/snort/snort.conf
PROG=snort
USER=snort
GROUP=snort
DAQDIR=/usr/local/lib/daq

if [ ! -x "$BINARY" ]; then
   /bin/echo "ERROR: $BINARY not found."
   exit 1
fi

if [ ! -r "$CONFIG_FILE" ]; then
   /bin/echo "ERROR: $CONFIG_FILE not found."
   exit 1
fi

rc_start()
{
```

```
   # Check if log directory is present. Otherwise, create it.
   if [ ! -d $LOGDIR/$DATE ]; then
      mkdir $LOGDIR/$DATE
      /usr/sbin/chown -R $USER:$GROUP $LOGDIR/$DATE
      /bin/chmod -R 700 $LOGDIR/$DATE
   fi

   /bin/echo "Starting $PROG: "
   # Snort parameters
   # -D Run Snort in background (daemon) mode
   # -i <if> Listen on interface <if> (i.e. - em0, em1, etc)
   # -u <uname> Run snort uid as <uname> user (or uid)
   # -g <gname> Run snort uid as <gname> group (or gid)
   # -c Load configuration file
   # --daq-dir=<directory where daq libraries are>
   # -N Turn off logging (alerts still work) (removed to enable logging) :)
   # -l Log to directory
   # -t Chroots process to directory after initialization
   # -R <id> Include 'id' in snort_intf<id>.pid file name

   $BINARY -D -i $LAN_INTERFACE --daq-dir=$DAQDIR -u $USER -g $GROUP -c
$CONFIG_FILE -l $LOGDIR/$DATE -t $LOGDIR/$DATE -R _ids
   /bin/echo "$PROG startup complete."
   return $RETURN_VAL
}

rc_stop()
{
   if [ -s $PID ]; then
      /bin/echo "Stopping $PROG with PID `cat $PID`: "
      kill -TERM `cat $PID` 2>/dev/null
      RETURN_VAL=$?
      /bin/echo "$PROG shutdown complete."
      rm -f $PID
   else
      /bin/echo "ERROR: PID in $PID file not found."
      RETURN_VAL=1
   fi
   return $RETURN_VAL
}

rc_status() {
      if [ -s $PID ]; then
            /bin/echo "$PROG is running as pid `cat $PID`:"
      else
```

```
                /bin/echo "$PROG is not running."
        fi
}

rc_restart()
{
    stop
    start
    RETURN_VAL=$?
    return $RETURN_VAL
}

case "$1" in
 start)
        rc_start
    ;;
 stop)
        rc_stop
    ;;
 status)
        rc_status
    ;;
 restart|reload)
        rc_restart
    ;;
 *)
    /bin/echo "Usage: $0 {start|stop|status|restart|reload}"
    RETURN_VAL=1
esac

exit $RETURN_VAL
----- CUT HERE -----
```

Note - On the above script, I made a symlink in /usr/sbin to point to where the actual snort binary was compiled on my system (you could also copy the snort binary to /usr/sbin as well).

To make the symbolic link (symlink) above, issue the commands below:

cd /usr/sbin <enter>
ln -s /usr/local/bin/snort snort <enter>
chmod 700 snort <enter>

If the directory '**/var/log/snort**' does not exist on your system, issue the following commands as '**root**' (permissions should be 700), when you use the '**adduser**' command in OpenBSD 5.x, it will make this directory for you, if you supply the directory during the questions being asked:

cd /var/log <enter>
mkdir snort <enter>
chmod 700 snort <enter>

Then issue the command below to change the user and owner of /var/log/snort to 'snort':

chown -R snort:snort snort <enter>
cd /usr/local/lib <enter>
mkdir snort_dynamicrules <enter>
chown -R snort:snort snort_* <enter>

At this point, you should be ready to do some testing of snort to see if it actually starts up and reads in the rules (you can check /var/log/messages to catch any fatal errors or crashes).

If you want to test snort startup, issue the following commands:

cd /usr//local/bin <enter>
./snort -T -i em0 -u snort -g snort --daq-dir=/usr/local/lib/daq -c /etc/snort/snort.conf <enter>

The above command will cause SNORT to start up in self-test mode, checking all the supplied command line switches and rules files that are passed to it and indicating that everything is ready to proceed. If all the tests are passed, you should see the following:

Snort successfully validated the configuration!
Snort exiting

If no errors are returned, proceed with the steps below (otherwise check /var/log/messages for more information):

To manually start snort, issue the following commands:

cd /usr/local/bin <enter> (if you are already in this directory, skip this command)

./snort -D -i em0 –A fast –b –d -u snort -g snort --daq-dir=/usr/local/lib/daq -c /etc/snort/snort.conf -l /var/log/snort <enter>

Make sure that snort initializes properly before proceeding below, you can check /var/log/messages for more information in the event of an error in initialization.

To see if snort is actually running on your system, issue the following command:

ps aux | grep -i "snort" <enter>

If snort is working, it should return something that looks like the output below:

snort 10622 0.0 0.8 369616 8272 ?? Ss 1:24PM 0:00.86 ./snort -D -i em0 –A fast –b –d -u snort -g snort --daq-dir=/usr/local/lib/daq –c /etc/snort/snort.conf –l /var/log/snort

Tips to improve the security of SNORT while running on OpenBSD:

OpenBSD 5.x is by definition is a very secure operating system and after an initial install has fewer than 25 processes running after the system is fully booted.

Here are some suggestions to lessen the impact that a vulnerability discovered in SNORT would give potential unauthorized access to a privileged account:

1. When running SNORT in daemon (-D) mode, the '-u' (user) and '-g' (group) switches should be used. This will allow SNORT to run as a given user and group after it is initialized. Typically, most system administrators prefer to add the 'snort' user and group to their systems, and that the 'snort' user should be unable to login or initiate shell privileges. Here is an example of a 'snort' user on a OpenBSD system:

snort:*:40000:40000:Snort IDS:/var/log/snort:/sbin/nologin

In the above example, the line is broken down as follows:

Columns 1-5 (the username, in this case 'snort')
Column 7 (the '*' indicates the password is encrypted)
Columns 9-13 (the user id (UID) 40000)
Columns 15-19 (the group id (GID) 40000, in this case the group is 'snort')
Columns 21-29 (the full name of the user, in this case 'Snort IDS')
Columns 31-44 (the default directory for this user, in this case /var/log/snort)
Columns 46-58 (the login shell for this user, in this case, logins are disabled)

The /sbin/nologin at the end of the line indicates that logins are disabled for the 'snort' user on this system.

2. The source code for SNORT/DAQ, binaries, logging directories, shared/static libraries, and configuration files should all be owned by the ‘snort’ user and group with appropriate permissions (mode 700 is preferred, though the default installation permissions are fine as well).

3. All binaries which are produced by the compiling and installation process of SNORT and DAQ should be verified using a hash function (i.e. - MD5, SHA-1, etc) and the output stored on removable media. A cron job could be used to run this process on a regular basis with results emailed to a system administrator. Another alternative would be the use of a utility called 'tripwire' for auditing installed software on a given computer.

I have separated the information for mirroring and/or copying packets from a home router to a snort sensor to a separate document located at the following URL:

www.snort.org/docs

Under the section marked 'Deployment Guides' and the link is marked:

How to make some home routers mirror traffic to Snort

Finally, if you have snort working in test mode (-T option), try starting snort with /etc/rc.d/snort start <enter> (you should get a running message if all is well), if there is a problem, check the output in /var/log/messages for additional details as to why snort failed to start.

Also, you can check the status of snort by issuing the command below (while still in /etc/rc.d):

./snort status <enter>

If it's working, you should see the output below:

Checking for service snort running

Next, change directory to /var/log/snort and issue the command 'ls -al' if everything is working properly, you should see two (or more) files, one marked 'alert' and 'snort.*' files (which are binary captures which can be read with tcpdump or wireshark). If you use 'tail -f alert' in your terminal/console window, you should see alerts coming into your snort IDS (as they occur).

If you have any questions, comments, or suggestions, please email me at:

wp02855@gmail.com (wp02855 at gmail dot com)

Bill Parker