Snort 3 on Ubuntu 14 and 16

(Snort 3.0.0-a4 build 223

Noah Dietrich
`Noah@SublimeRobots.com`

January 7, 2017

Contents

1 Introduction

This guide is will walk you through installing Snort3 Alpha on Ubuntu 14 and 16. These instructions will Not work on Ubuntu 12 (although an old guide can be found on my website.

Please Note that Snort3 is alpha software. It does contain bugs, and new releases can have different prerequisites than when this guide was released. This guide has been written and tested against Snort 3.0.0-a4 build 223, released on December 22, 2016. You may be able to follow this guide to install later releases of Snort, but the requirements may change.

Since Snort++ is alpha software, you should not use it in production systems. This software has been released by the Snort team to solicit feedback and for users to test.

This guide will not discuss how to configure Snort as an NIPS or NIDS, how to install additional supporting software (barnyard2, PulledPork, GUIs), how to setup network interfaces to capture data, Snort sensor design considerations, descriptions of specific preprocessors, or OpenAppID, but you can read other articles I have written about these items, and how to configure Snort 2 as a full NIDS or NIPS system: SublimeRobots.com.

Feedback on this guide is welcome: **Noah@SublimeRobots.com**.

You can also ask for help on the Snort distribution lists:
Snort Users
Snort Developers
Snort OpenAppID

2 Begin

First, ensure the system is up to date and has the latest list of packages:

```
sudo apt-get update && sudo apt-get dist-upgrade -y
```

Install the Snort3 prerequisites (details of these packages can be found in the requirements section of the Snort3 Manual:

```
sudo apt-get install -y build-essential autotools-dev libdumbnet-dev libluajit-5.1-dev libpcap-dev \
       libpcre3-dev zlib1g-dev pkg-config libhwloc-dev cmake
```

Next install the optional (but recommended software):

```
sudo apt-get install -y liblzma-dev openssl libssl-dev cpputest
```

If you want to build the latest documentation when you build snort, install the following (purely optional) packages. These packages are nearly 800 MB in size:

```
sudo apt-get install -y asciidoc dblatex source-highlight
```

Since we will install Snort from the github repository, we need a few tools:

```
sudo apt-get install -y libtool git autoconf
```

The Snort DAQ (Data AcQuisition library)has a few pre-requisites that need to be installed:

```
sudo apt-get install -y bison flex
```

We will be downloading a number of source tarbals and other source files, we want to store them in one folder:

```
mkdir ~/snort_src
cd ~/snort_src
```

Download and install safec for runtime bounds checks on certain legacy C-library calls (this is optional but recommended):

```
cd ~/snort_src
wget http://downloads.sourceforge.net/project/safeclib/libsafec-10052013.tar.gz
tar -xzvf libsafec-10052013.tar.gz
cd libsafec-10052013
./configure
make
sudo make install
```

Snort3 will use Hyperscan for fast patern matching. Hyperscan requires Ragel and the Boost headers:

Download and install Ragel:

```
cd ~/snort_src
wget http://www.colm.net/files/ragel/ragel-6.9.tar.gz
tar -xzvf ragel-6.9.tar.gz
cd ragel-6.9
./configure
make
sudo make install
```

Hyperscan requires the Boost C++ Libraries. Note that we are not using the Ubuntu repository version of the boost headers (libboost-all-dev) because Hyperscan requires boost libraries at or above version number 1.58, and the Ubuntu repository version is too old. Download the Boost 1.63 libraries, but do not install:

```
cd ~/snort_src
wget http://downloads.sourceforge.net/project/boost/boost/1.63.0/boost_1_63_0.tar.gz
tar -xvzf boost_1_63_0.tar.gz
```

Install Hyperscan 4.2.0 from source, referencing the location of the Boost headers source directory:

```
cd ~/snort_src
wget https://github.com/01org/hyperscan/archive/v4.2.0.tar.gz
tar -xvzf v4.2.0.tar.gz
mkdir ~/snort_src/hyperscan-4.2.0-build
cd hyperscan-4.2.0-build/

cmake -DCMAKE_INSTALL_PREFIX=/usr/local -DBOOST_ROOT=~/snort_src/boost_1_63_0/ ../hyperscan-4.2.0

make
sudo make install
```

If you want to test that Hyperscan works, from the build directory, run:

```
cd ~/snort_src/hyperscan-4.2.0-build/
./bin/unit-hyperscan
```

Next, download and install Data AcQuisition library (DAQ) from the Snort website. Note that Snort 3 uses a different DAQ than the Snort 2.9.x.x series:

```
cd ~/snort_src
wget https://www.snort.org/downloads/snortplus/daq-2.2.1.tar.gz
tar -xvzf daq-2.2.1.tar.gz
cd daq-2.2.1
./configure
make
sudo make install
```

Update shared libraries:

```
sudo ldconfig
```

Install snort master from github

```
cd ~/snort_src
wget https://github.com/snortadmin/snort3/archive/master.tar.gz
tar -xvzf master.tar.gz
cd snort3-master/
autoreconf -isvf

./configure --prefix=/opt/snort
make
sudo make install
```

test that Snort runs:

```
noah@snort3:~$ /opt/snort/bin/snort -V

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.0.0-a4 (Build 223) from 2.9.8-383
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 2.2.1
           Using libpcap version 1.5.3
           Using LuaJIT version 2.0.2
           Using PCRE version 8.31 2012-07-06
           Using ZLIB version 1.2.8
           Using LZMA version 5.1.0alpha
           Using OpenSSL 1.0.1f 6 Jan 2014
           Using Hyperscan version 4.2.0 2017-01-07
```

Finally it's good practice to create a link to snort in /usr/sbin:

```
sudo ln -s /opt/snort/bin/snort /usr/sbin/snort
```

3 Running Snort

Snort 3 requires a few environmental variables in order to run correctly. We store these variables temporarily in the current session and save them permanently to the our local .bashrc file (note that LUA_PATH can't be stored in /etc/profile because it won't load correctly. You'll need to run these lines for every user who needs to run Snort on this system):

```
export LUA_PATH=/opt/snort/include/snort/lua/\?.lua\;\;
export SNORT_LUA_PATH=/opt/snort/etc/snort

sh -c "echo 'export LUA_PATH=/opt/snort/include/snort/lua/\?.lua\;\;' >> ~/.bashrc"
sh -c "echo 'export SNORT_LUA_PATH=/opt/snort/etc/snort' >> ~/.bashrc"
```

To make these environmental variables available when you use sudo, add them to the /etc/sudoers file:

```
sudo visudo
```

add the following line to the end:

```
Defaults env_keep += "LUA_PATH SNORT_LUA_PATH"
```

use ctrl-x to exit, save when prompted by pressing y, then press enter to save the file to /etc/sudoers.tmp (which will get copied automatically to /etc/sudoers).

Now lets test Snort with the default configuration file and ruleset:

```
/opt/snort/bin/snort -c /opt/snort/etc/snort/snort.lua -R /opt/snort/etc/snort/sample.rules
```

You should see output that finishes with the following:

```
Snort successfully validated the configuration.
o")~   Snort exiting
```

4 Install Locations

A note on install locations:

When we ran **./configure –prefix=/opt/snort** we were telling snort to install all files under the /opt/snort folder. If you omit this configuration option, snort will be installed to the same set of folders, only this time at the root folder. For example the files installed under /opt/snort/bin would instead be installed to /bin, and files installed to /opt/snort/etc would be installed to /etc. These locations is more common for a normal install, rather than a testing install.

The files that are installed when you use /opt/snort as your install location are as follows:

```
/opt/snort
 bin
    snort
    snort2lua
    u2boat
    u2spewfoo
 etc
    snort
        file_magic.lua
        sample.rules
        snort_defaults.lua
        snort.lua
 include
    snort
        actions
        codecs
        daqs
        decompress
        detection
        events
        file_api
        filters
        flow
        framework
        hash
        latency
        log
        lua
        main
        managers
        mime
        profiler
        protocols
        search_engines
        sfip
        sfrt
        stream
        time
        utils
 lib
    pkgconfig
       snort.pc
    snort
        daqs
 share
     doc
         snort

37 directories, 9 files
```

The bin folder contains the following files:
snort: The Snort binary.
snort2lua: Tool to convert a Snort 2.9.7.x configuration file into a 3.x configuration file. More notes here.
u2boat: U2boat is a tool for converting unified2 files into different formats.
u2spewfoo: U2SpewFoo is a lightweight tool for dumping the contents of unified2 files to stdout.

Additionally, the following folders are created / used:
/opt/snort/bin: Binaries for Snort and supporting software.
/opt/snort/etc/snort: The configuration files for Snort.
/opt/snort/include/snort: All include files for Snort.
/opt/snort/lib/pkgconfig: The pkgconfig file for Snort (compilation details for Snort).
/opt/snort/share/doc/snort: The documentation for the installed version of Snort.

5 Where to Go from Here

See the Snort 3 manual for more information about running Snort 3 and compilation options.

I have tutorials available on my website for configuring a fully-featured Snort system on Ubuntu, including Barnyard2, PulledPork, and BASE, configuring Snort to run as a NIPS (dropping / blocking malicious traffic), and configuring OpenAppID for layer 7 application detection. These tutorials and more are available at SublimeRobots.com.

Feedback: Please send me feedback with issues you encountered and recommendations for changes to this guide: Noah@SublimeRobots.com. Feedback helps me to update these guides, and helps me identify common issues and questions that people encounter when running through these instructions.