

Samantha Jackson
CSCI4406
11-15-2024

Lab 9 - Snort

Observations/Issues: I'm attempting to run Snort on Garuda Linux, because I just moved to this OS. Being that this is an Arch-Based system it uses pacman as a packet manager, so apt-get is not available for these distributions. I obtained a tarball of snort from their official website and attempted to configure it in /usr/share/snort3/snort-2.9.20. Had to download the dependencies libpcap and libdnet.

```
erossore@erossore in /usr/share/snort3 as 🐼 took 0s
λ sudo tar xzf snort-2.9.20.tar.gz

erossore@erossore in /usr/share/snort3 as 🐼 took 0s
λ cd snort-2.9.20/

erossore@erossore in /usr/share/snort3/snort-2.9.20 via 🍌 v5.40.0 as 🐼
λ export my_path=/path/to/snorty

erossore@erossore in /usr/share/snort3/snort-2.9.20 via 🍌 v5.40.0 as 🐼
λ sudo ./configure_cmake.sh --prefix=$my_path
sudo: ./configure_cmake.sh: command not found

erossore@erossore in /usr/share/snort3/snort-2.9.20 via 🍌 v5.40.0 as 🐼 took 0s
[●] * sudo ./configure.sh --prefix=$my_path
sudo: ./configure.sh: command not found

erossore@erossore in /usr/share/snort3/snort-2.9.20 via 🍌 v5.40.0 as 🐼 took 0s
[●] * sudo ./configure --prefix=$my_path
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking whether make supports the include directive... yes (GNU style)
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
```

```
ERROR! dnet header not found, go get it from
http://code.google.com/p/libdnet/ or use the --with-dnet-*
options, if you have it installed in an unusual place
```

```
erossore@erossore in /usr/share/snort3/snort-2.9.20 via v5.40.0 as 🧑 took 0s
λ sudo pacman -S libdnet
resolving dependencies...
looking for conflicting packages ...

Package (1)      New Version  Net Change  Download Size
extra/libdnet    1.18.0-1     0.16 MiB   0.06 MiB

Total Download Size: 0.06 MiB
Total Installed Size: 0.16 MiB

:: Proceed with installation? [Y/n] y
```

After attempting to download it again snort wants the daq_static library so that tar file had to be configured as well. After that the configuration of Snort was finally successful. However, making the file was not successful.

```
ERROR! daq_static library not found, go get it from
http://www.snort.org/.
```

```
erossore@erossore in /usr/share/snort3🔒 as 🧑 took 0s
λ cd daq-2.0.7/

erossore@erossore in /usr/share/snort3/daq-2.0.7🔒 as 🧑
λ sudo ./configure
```

This is a view of the snort.conf file. Many of the files referred to in the PDF documentation do not exist in my version of snort, likely because I couldn't complete a cmake command. Snort's documentation didn't provide me any further direction and troubleshooting hasn't worked so far. There were several recommendations saying that the libtirpc-dev package should be installed and a few of the files modified however I cannot find these packages in Garuda and I cannot find them on the Arch Linux website or a github. I'm at a loss.

```
opts.o sf_snort_plugin_hdropts.c
sp_rpc_check.c:32:10: fatal error: rpc/rpc.h: No such file or directory
  32 | #include <rpc/rpc.h>
      |           ^~~~~~
compilation terminated.
make[3]: *** [Makefile:489: sp_rpc_check.o] Error 1
make[3]: *** Waiting for unfinished jobs....
```

```
GNU nano 8.2                                etc/snort.conf
#
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
#   http://www.snort.org                Snort Website
#   http://vrt-blog.snort.org/         Sourcefire VRT Blog
#
#   Mailing list Contact:      snort-users@lists.snort.org
#   False Positive reports:    fp@sourcefire.com
#   Snort bugs:                bugs@snort.org
#
#   Compatible with Snort Versions:
#   VERSIONS : 2.9.20
#
#   Snort build options:
#   OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-...
#
#   Additional information:
#   This configuration file enables active response, to run snort in
#   test mode -T you are required to supply an interface -i <interface>
#   or test mode will fail to fully validate the configuration and
#   exit with a FATAL error
#
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####
# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

erossore@erossore in /usr/share/snort3/snort-2.9.20 via C v14.2.1-gcc via o v5.40.0 as  took 0s
[●] * sudo snort -T -c /etc/snort/snort.conf
sudo: snort: command not found
```