Segurança em Tecnologias da Informação 2022/2023

Snort with "nfq" DAQ for inline mode // Installation notes

1. Please note:

- The following installation notes illustrate the process for installing: Snort 2 on:
  - Snort 2 on CentOS 7
  - Snort 3 on CentOS 8

- For your particular Linux installation additional steps may be required (e.g., the installation of additional missing packages), thus the described steps are merely indicative.

2. Snort DAQ packages required for inline mode support

The inline mode in Snort may be enabled using either the DAQ (Data Acquisition) module "afpacket" or the module "nfq". The former is used when the Linux firewall is configured with two adapters in bridging mode, while the latter is appropriate to operate with netfiler/IPTables. Thus, for the purpose of the Practical Assignment #2, the "nfq" DAQ may be enabled and used with Snort.

3. Snort 2 installation steps for CentOS 7

```
# Install required packages (additional packages may be required for your system)
yum install libpcap-devel pcre-devel libdnet-devel zlib-devel libnetfilter_queue
     libnetfilter_queue-devel gcc make perl luajit-devel openssl openssl-devel
     libnghttp2-devel bison flex

# Download required sources for libdaq and Snort 2
cd /usr/local/src
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
wget https://www.snort.org/downloads/snort/snort-2.9.20.tar.gz

# Compile and install libdaq with support for the "nfq" DAQ
tar zxvf daq-2.0.7.tar.gz
cd daq-2.0.7

# As the result of the following command you should make sure that the "nfq"
# module is enabled for compilation
./configure --enable-nfq

# Compile and install the DAQ
make
make install

# Please note:
# - Installed DAQs are available in /usr/local/lib/daq
# - To enable the usage of the compiled modules, add the line "/usr/local/lib/daq"
#    to /etc/ld.so.conf and run "ldconfig"
```

```
# Configure Snort for compilation
cd /usr/local/src
tar zxvf snort-2.9.20.tar.gz
cd snort-2.9.20
./configure --with-daq-includes=/usr/local/lib --with-daq-libraries=/usr/local/lib
     --prefix=/usr/local/snort

# Compile and install Snort
make
make install
ln -s /usr/local/snort/bin/snort /usr/sbin/snort

# Please note:
# - To verify if Snort is available: /usr/sbin/snort -v
# - To check the available DAQs: /usr/sbin/snort --daq-list
```

4. Snort 3 installation steps for CentOS 8

```
# Install support for the EPEL repository:
dnf install epel-release -y
dnf config-manager --add-repo /etc/yum.repos.d/CentOS-Linux-PowerTools.repo
dnf config-manager --set-enabled powertools
dnf upgrade -y
(reboot Linux system after upgrade)

# Install required dependencies (packages)
dnf install flex bison gcc gcc-c++ make cmake autoconf libtool git nano unzip wget
     libpcap-devel pcre-devel libdnet-devel hwloc-devel openssl-devel zlib-devel
     luajit-devel pkgconfig libnfnetlink-devel libnetfilter_queue-devel
     libmnl-devel xz-devel libuuid-devel -y

# Download the libdaq source for compilation
cd /usr/local/src
git clone https://github.com/snort3/libdaq.git

# Configure libdaq with “nfq” support
cd libdaq
./bootstrap

# As the result of the following command you should make sure that the “nfq”
# module is enabled for compilation
./configure --enable-nfq

# Compile and install libdaq
make
make install


# Download Snort 3 for compilation

cd /usr/local/src
git clone https://github.com/snort3/snort3.git
cd snort3
export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig:$PKG_CONFIG_PATH
export PKG_CONFIG_PATH=/usr/local/lib64/pkgconfig:$PKG_CONFIG_PATH
```

```
# Compile and install Snort
./configure_cmake.sh --prefix=/usr/local/snort
cd build/
make -j$(nproc)
make -j$(nproc) install


# Please note:
# - To enable the usage of the compiled nfq module, add the line “/usr/local/lib/”
#    to /etc/ld.so.conf and run “ldconfig”
Ldconfig

ln -s /usr/local/snort/bin/snort /usr/sbin/snort

# Please note:
# - To verify if Snort is available: /usr/sbin/snort -v
# - To check available DAQs in Snort: /usr/sbin/snort --daq-list
```