Task-3:- Network Intrusion Detection System

STEP 0 - INSTALL PRE-REQS:-

sudo apt-get install -y build-essential autotools-dev libdumbnet-dev libluajit-5.1-dev libpcap-dev \ zlib1g-dev pkg-config libhwloc-dev cmake liblzma-dev openssl libssl-dev cpputest libsqlite3-dev \ libtool uuid-dev git autoconf bison flex libcmocka-dev libnetfilter-queue-dev libunwind-dev \ libmnl-dev ethtool libjemalloc-dev

STEP 1 – Install pcre

cd ~/snort :-

wget <https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz>

tar -xzvf pcre-8.45.tar.gz

cd pcre-8.45

./configure

make

sudo make install

STEP 3 – Install gperftools:-

cd ~/snort:-

wget <https://github.com/gperftools/gperftools/releases/download/gperftools-2.9.1/gperftools-2.9.1.tar.gz>

tar xzvf gperftools-2.9.1.tar.gz

cd gperftools-2.9.1

./configure

make

sudo make install

STEP 4 – Install Ragel:-

cd ~/snort

wget <http://www.colm.net/files/ragel/ragel-6.10.tar.gz>

tar -xzvf ragel-6.10.tar.gz

cd ragel-6.10

./configure

make

sudo make install

STEP 5 - download (but don’t install) the Boost C++ Libraries:-

cd ~/snort

wget <https://boostorg.jfrog.io/artifactory/main/release/1.77.0/source/boost_1_77_0.tar.gz>

tar -xvzf boost\_1\_77\_0.tar.gz

STEP 6 – Install Hyperscan:-

cd ~/snort

wget <https://github.com/intel/hyperscan/archive/refs/tags/v5.4.2.tar.gz>

tar -xvzf v5.4.2.tar.gz

mkdir ~/snort/hyperscan-5.4.2-build

cd hyperscan-5.4.2-build/

cmake -DCMAKE\_INSTALL\_PREFIX=/usr/local -DBOOST\_ROOT=~/snort/boost\_1\_77\_0/ ../hyperscan-5.4.2

make

sudo make install

STEP 7 – Install flatbuffers:-

cd ~/snort

wget https://github.com/google/flatbuffers/archive/refs/tags/v2.0.0.tar.gz -O flatbuffers-v2.0.0.tar.gz

tar -xzvf flatbuffers-v2.0.0.tar.gz

mkdir flatbuffers-build

cd flatbuffers-build

cmake ../flatbuffers-2.0.0

make

sudo make install

STEP 8 - Install Data Acquistion (DAQ) from Snort:-

cd ~/snort

wget [https://github.com/snort3/libdaq/archive/refs/tags/v3.0.13.tar.gz -O libdaq-3.0.13.tar.gz](https://github.com/snort3/libdaq/archive/refs/tags/v3.0.13.tar.gz%20-O%20libdaq-3.0.13.tar.gz)

tar -xzvf libdaq-3.0.13.tar.gz

cd libdaq-3.0.13

./bootstrap

./configure

make

sudo make install

STEP 9 - Update shared libraries:-

sudo ldconfig

STEP 10 – Download latest version of Snort 3:-

cd ~/snort

wget https://github.com/snort3/snort3/archive/refs/tags/3.1.74.0.tar.gz -O snort3-3.1.74.0.tar.gz

tar -xzvf snort3-3.1.74.0.tar.gz

cd snort3-3.1.74.0

./configure\_cmake.sh --prefix=/usr/local --enable-jemalloc

cd build

make

STEP 11 sudo make install:-

Disable LRO & GRO using a service

[Unit]

Description=Ethtool Configration for Network Interface

[Service]

Requires=network.target

Type=oneshot

ExecStart=/sbin/ethtool -K <network adapter> gro off

ExecStart=/sbin/ethtool -K <network adapter> lro off

[Install]

WantedBy=multi-user.target

STEP 12:-

git clone https://github.com/shirkdog/pulledpork3.git

cd ~/snort/pulledpork3

sudo mkdir /usr/local/bin/pulledpork3

sudo cp pulledpork.py /usr/local/bin/pulledpork3

sudo cp -r lib/ /usr/local/bin/pulledpork3

sudo chmod +x /usr/local/bin/pulledpork3/pulledpork.py

sudo mkdir /usr/local/etc/pulledpork3

sudo cp etc/pulledpork.conf /usr/local/etc/pulledpork3/