Prajwal Kamath **(230948028)**

Week 2- Installation of Snort tool

1. **Installing Required Dependencies:**
   To initiate the installation process, you must install various dependencies on your Ubuntu 22.04 server. Open a terminal and execute the following command to install all the necessary dependencies:

   >>sudo apt install -y build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdnet-dev libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev libfl-dev

2. **Installing Snort DAQ:**
   Next, install the Data Acquisition (DAQ) library, a prerequisite for Snort. Since the DAQ library is not available in the default Ubuntu repository, compile it from source with the following steps:

   >>git clone https://github.com/snort3/libdaq.git
   >>cd libdaq
   >>./bootstrap
   >>./configure
   >>make
   >>sudo make install

3. **Installing Gperftools**
   Gperftools, a set of performance analysis tools used by Snort, can be installed as follows:

   >>cd wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.9.1/gperftools-2.9.1.tar.gz>>tar xzf gperftools-2.9.1.tar.gz
   >>cd gperftools-2.9.1/
   >>./configure
   >>make
   >>sudo make install

4. **Installing Snort:**
   Now, proceed to install Snort itself with the following steps

   >>cd wget https://github.com/snort3/snort3/archive/refs/tags/3.1.43.0.tar.gz
   >>tar -xvzf 3.1.43.0.tar.gz
   >>cd snort3-3.1.43.0

>>./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc
>>make
>>sudo make install
>>sudo ldconfig
>>snort -V

5. **Configuring Snort:**
   Before utilizing Snort, configure it using the following steps:
   Set your network interface to promiscuous mode to enable Snort to analyze all network traffic:

   >>sudo ip link set dev eth0 promisc on

   Verify the interface is in promiscuous mode:

   >>ip add sh eth0

   Disable Interface Offloading to ensure accurate packet analysis:

   >>sudo ethtool -K eth0 gro off lro off

6. **Creating a Systemd Service File for Snort NIC:**
   For automatic startup on boot, create a systemd service file for Snort NIC with the following steps:

   >>sudo nano /etc/systemd/system/snort3-nic.service

   Add the following lines to the file:

   [Unit]
   Description=Set Snort 3 NIC in promiscuous mode and Disable GRO, LRO on boot
   After=network.target

   [Service]
   Type=oneshot
   ExecStart=/usr/sbin/ip link set dev eth0 promisc on
   ExecStart=/usr/sbin/ethtool -K eth0 gro off lro off
   TimeoutStartSec=0
   RemainAfterExit=yes

   [Install]
   WantedBy=default.target

Save and close the file. Then, reload the systemd daemon:
>>sudo systemctl daemon-reload
Start and enable the Snort NIC service:
>>sudo systemctl start snort3-nic.service
>>sudo systemctl enable snort3-nic.serv
Check the service status:
>>sudo systemctl status snort3-nic.service

7. **Installing Snort Rules**
   Snort relies on rules to detect and respond to network-based attacks. Follow these steps to install Snort rules:

   >>sudo mkdir /usr/local/etc/rules
   wget -qO-
   https://www.snort.org/downloads/community/snort3-community-rules.tar.gz |
   sudo tar xz -C /usr/local/etc/rules/
   >>sudo nano /usr/local/etc/snort/snort.lua

   Edit the Snort main configuration file, defining your network and rules path as needed. Save and close the file.