Assignments:-4

Module:- NDC(SNORT_Ubuntu)

Name:- Prithviraj Nikam

Lab Assignment :-

Install and configure SNORT-2.9.20 on following OS:

3. Ubuntu 22.04

Step-1:- sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet autoconf libtool

```
Processing triggers for man-db (2.10.2-1) ...
root@Ubunut:~# sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev
ap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev
bison flex libdnet autoconf libtoollibpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev
Reading package lists... Doneibtool
Building dependency tree... Done
Reading state information... Done
```

Step-2:-

```
root@Ubunut: ~
root@Ubunut:~# apt-get install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snort is already the newest version (2.9.15.1-6build1).
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 145 not upgraded.
root@Ubunut:~#
```

Step-2:-Start by making a temporary download folder to your home directory and then changing into it with the command below.

mkdir ~/snort_src && cd ~/snort_src

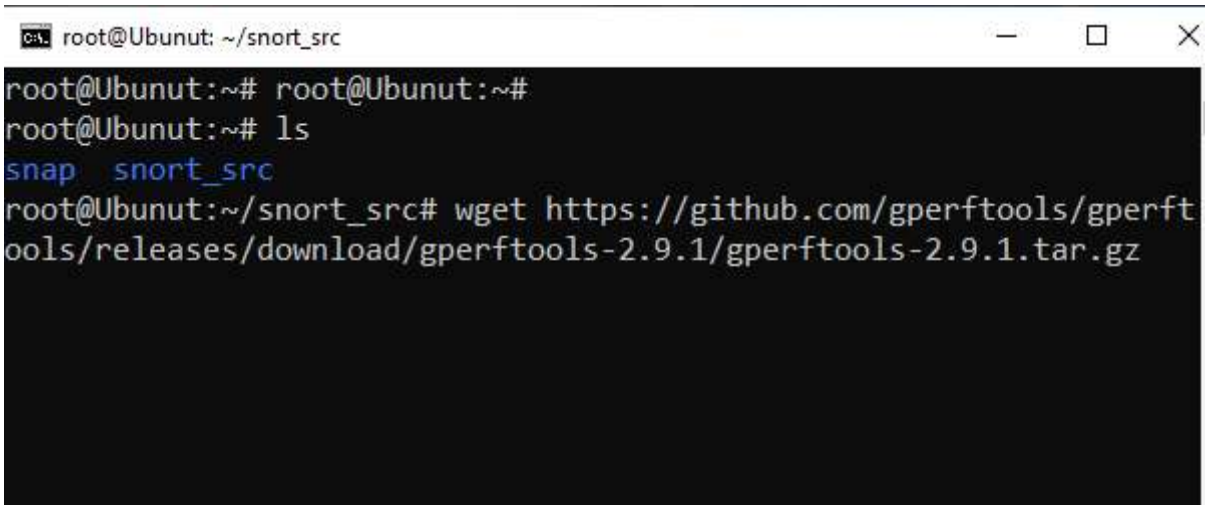
```
root@Ubunut:~# mkdir ~/snort_src && cd ~/snort_src
root@Ubunut:~/snort_src#
root@Ubunut:~/snort_src#
```

Step-3:- Start by downloading the snort version you want to install from the snort release page using wget and ensure you are in the ../ directory where you want to install snort.

```
root@Ubunut:~/snort_src# apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  systemd-hwe-hwdb
```

```
root@Ubunut:~/snort_src# git clone https://github.com/snort3/libdaq.git
Cloning into 'libdaq'...
remote: Enumerating objects: 2358, done.
remote: Counting objects: 100% (93/93), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 2358 (delta 82), reused 80 (delta 78), pack-reused 2265
Receiving objects: 100% (2358/2358), 1.04 MiB | 3.05 MiB/s, done.
Resolving deltas: 100% (1715/1715), done.
```

Step-4:- download the gpreftools from git hub



Step-5:-updating the shared libraries using the command underneath.

 # cd ldconfig

```
root@Ubunut:~/snort_src# cd libdaq
root@Ubunut:~/snort_src/libdaq#
```

Step-6:- #./bootstrap

```
root@Ubunut:~/snort_src/libdaq# ./bootstrap
+ autoreconf -ivf --warnings=all
autoreconf: export WARNINGS=all
autoreconf: Entering directory '.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
autoreconf: configure.ac: tracing
```

Step-7:- # ./configure

```
autoreconf: Leaving directory '.'
root@Ubunut:~/snort_src/libdaq# ./configure
```

Step-8:- # make

```
root@Ubunut:~/snort_src/libdaq# make
```

Step-9:- # make install

```
root@Ubunut:~/snort_src/libdaq# sudo make install
```

Step-10:- # tar xzf gpertools-2.9.1.tar.gz

 # cd gpertools-2.9.1.tar.gz

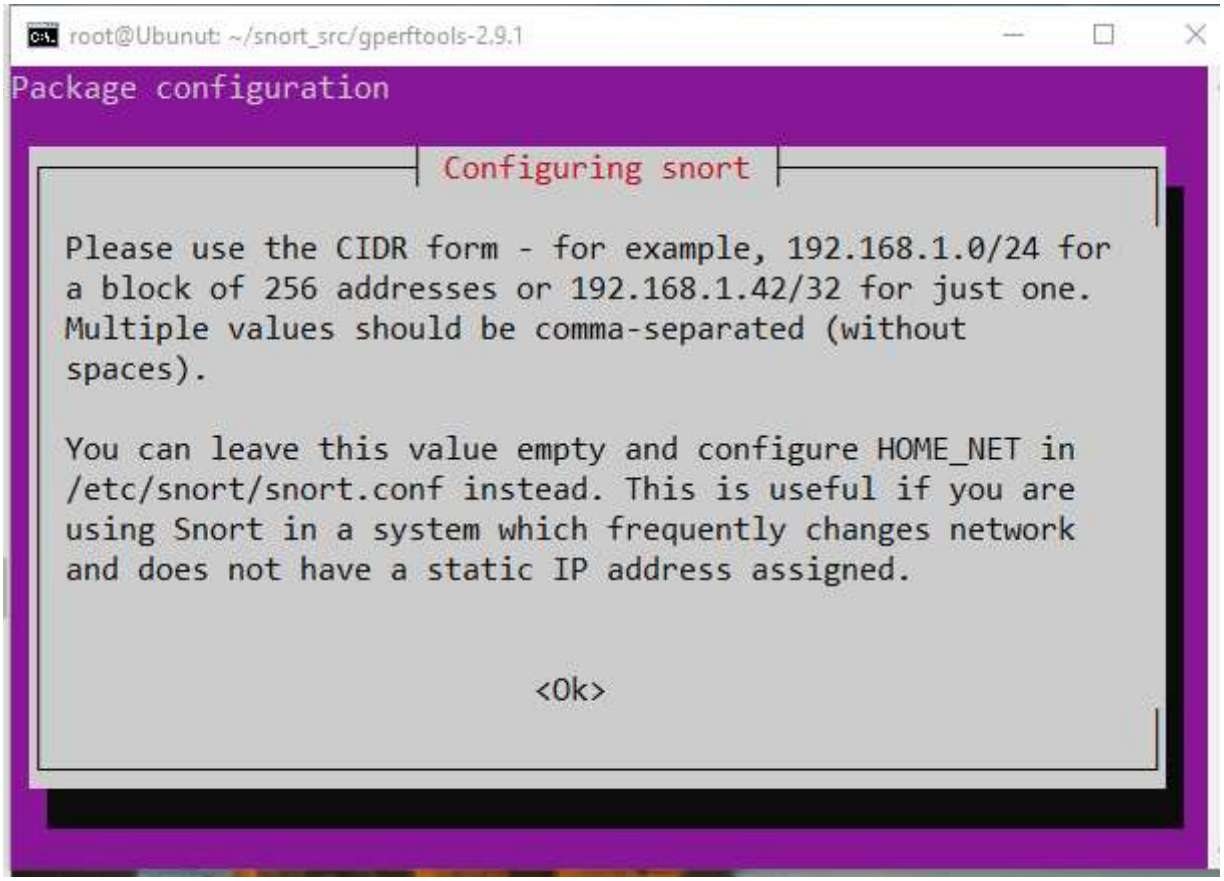
 # ./configure

```
root@Ubunut:~/snort_src# tar xzf gperftools-2.9.1.tar.gz
root@Ubunut:~/snort_src# cd gperftools-2.9.1/
root@Ubunut:~/snort_src/gperftools-2.9.1# ./configure
```

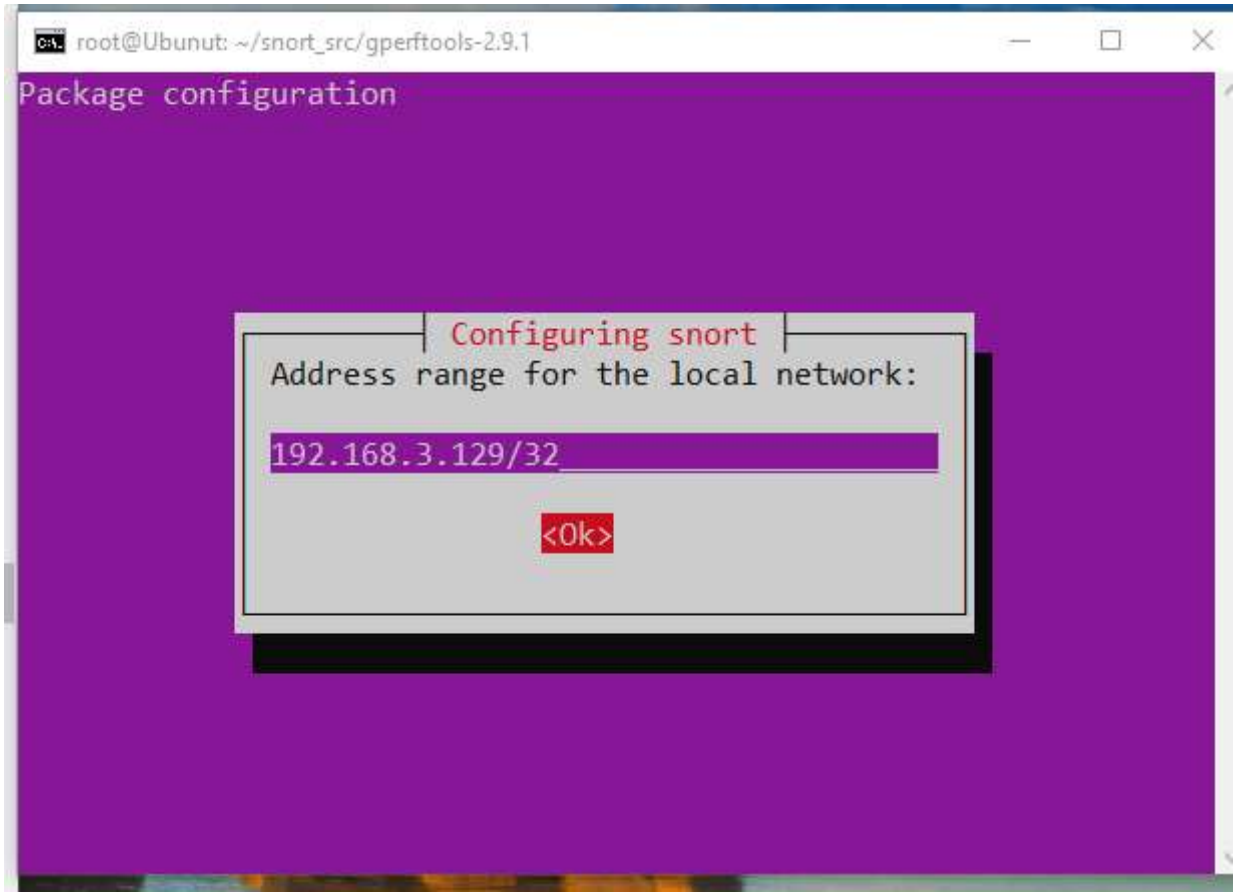
Step-11:- # make && sudo make install

```
root@Ubunut:~/snort_src/gperftools-2.9.1# make && sudo make instal
l
```

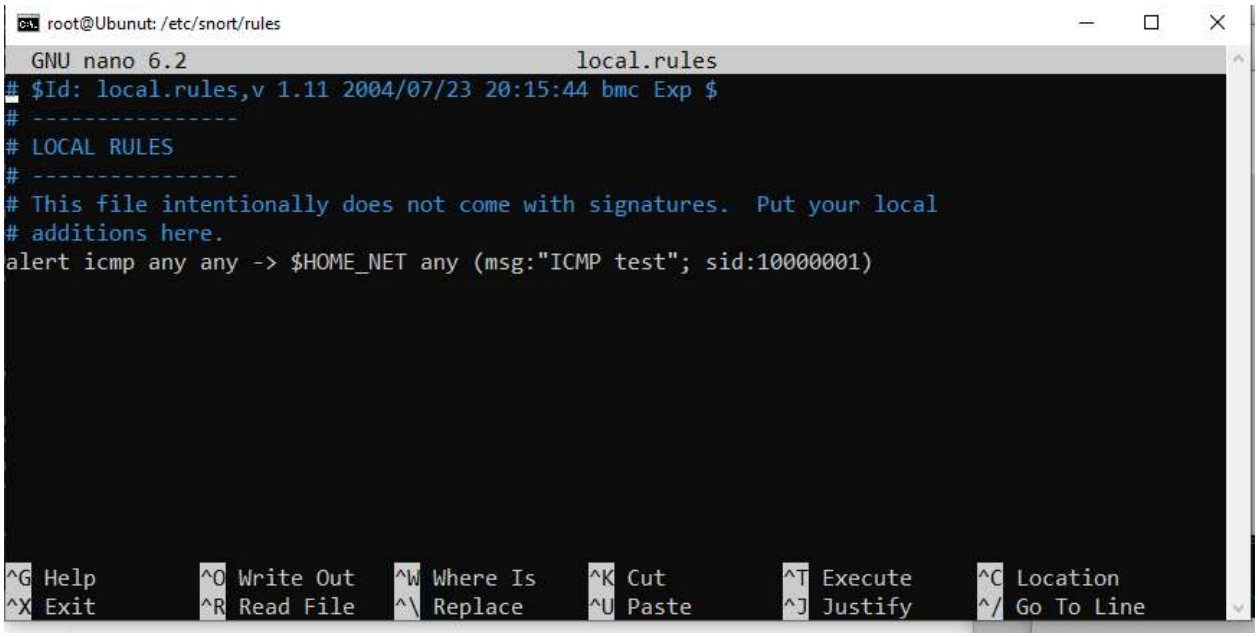
Step-12:- Configure Snort



Step-13:- Give System IP



Step-14:- Go to local rules and set rules



Step-15:- Check snort Version

```
root@Ubunut:~/snort_src/gperftools-2.9.1# snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org
/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. Al
l rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

root@Ubunut:~/snort_src/gperftools-2.9.1#
```

```
root@Ubunut: /etc/snort/rules
root@Ubunut:/etc/snort/rules# root@Ubunut:/etc/snort/rules# snort
-v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org
/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. Al
l rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
```

Step-16:- Check ip port status

```
root@Ubunut:~# ip link set dev enp0s3 promisc on
root@Ubunut:~#
```

Step-17:- Run Console rule

```
================================================================================
Snort exiting
root@Ubunut:/etc/snort/rules# snort -A console -i enp0s3 -c /etc/snort/snort.conf
```

Step-18:- Go to Windows and ping the system

```
Select Command Prompt
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cdac>ping 192.168.3.129

Pinging 192.168.3.129 with 32 bytes of data:
Reply from 192.168.3.129: bytes=32 time<1ms TTL=64
Reply from 192.168.3.129: bytes=32 time<1ms TTL=64
Reply from 192.168.3.129: bytes=32 time<1ms TTL=64
Reply from 192.168.3.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\cdac>
```

Step-19:- Check the out Put

```
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build
 1>
Commencing packet processing (pid=62228)
12/14-16:29:17.935265  [**] [1:10000001:0] ICMP test [**] [Priorit
y: 0] {ICMP} 192.168.3.232 -> 192.168.3.129
12/14-16:29:18.937704  [**] [1:10000001:0] ICMP test [**] [Priorit
y: 0] {ICMP} 192.168.3.232 -> 192.168.3.129
12/14-16:29:19.945356  [**] [1:10000001:0] ICMP test [**] [Priorit
y: 0] {ICMP} 192.168.3.232 -> 192.168.3.129
12/14-16:29:20.948502  [**] [1:10000001:0] ICMP test [**] [Priorit
y: 0] {ICMP} 192.168.3.232 -> 192.168.3.129
```