SNORT INSTALLATION

Follow the steps :

1. Obtain the local IP of your computer using **“ifconfig”** command. If command won’t run, you will need to install the **“net-tools”** package.

```
shantanu@shantanu:~$ ifconfig

Command 'ifconfig' not found, but can be installed with:

sudo apt install net-tools

shantanu@shantanu:~$ _
```

2. Download the package :

```
shantanu@shantanu:~$ sudo apt install net-tools
[sudo] password for shantanu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 626 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 5s (39.0 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 143265 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
shantanu@shantanu:~$ _
```

3. Obtain the Local IP Now. The highlighted text shows the local IP. We will need this IP while installing SNORT. Usually it automatically detects the Local IP and Interface, but still may require if auto capture not works.

Hint : inet 10.0.2.15 – Local IP, enp0s3 – Interface Name

```
shantanu@shantanu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::25e8:b66e:3f21:b386  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ac:3a:f1  txqueuelen 1000  (Ethernet)
        RX packets 245  bytes 224108 (224.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 291  bytes 24866 (24.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 148  bytes 12402 (12.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 148  bytes 12402 (12.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

shantanu@shantanu:~$
```

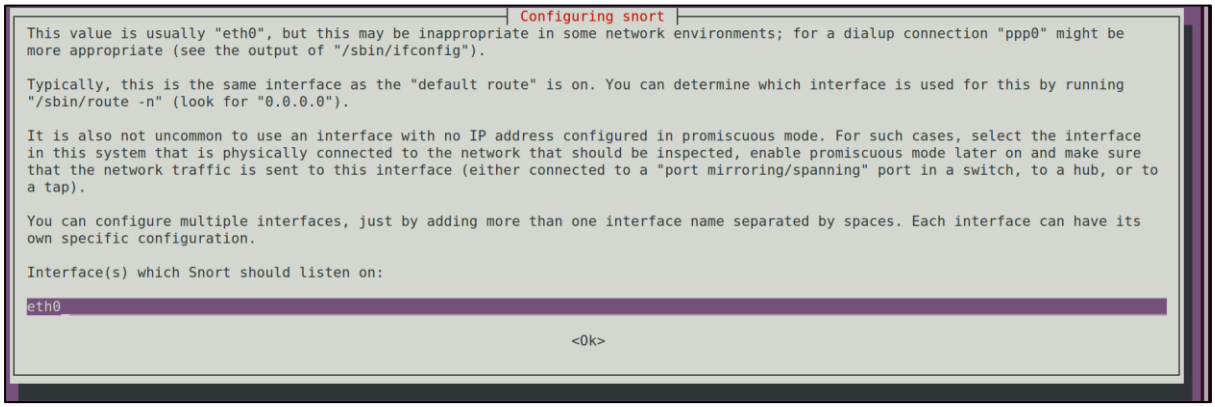
4. Now check is SNORT is installed or not ?

```
shantanu@shantanu:~$ snort --version

Command 'snort' not found, but can be installed with:

sudo apt install snort

shantanu@shantanu:~$ _
```

5. If not install the SNORT using **“sudo apt install snort”** :

```
shantanu@shantanu:~$ sudo apt install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 626 not upgraded.
Need to get 1,424 kB of archives.
After this operation, 7,338 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 snort-common-libraries amd64 2.9.7.0-5build1 [413 kB]
9% [1 snort-common-libraries 158 kB/413 kB 38%]
```

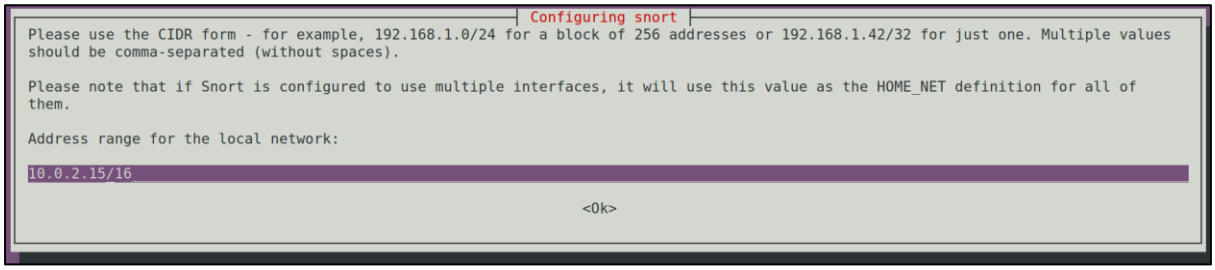
6. SNORT Configuration during Installation :



In above screenshot, we need to enter the name of interface that we collected in step 3.

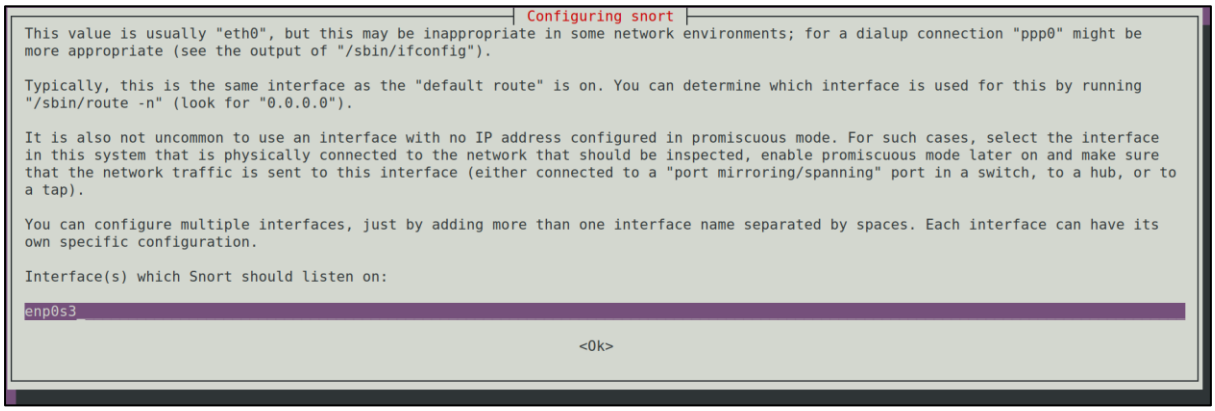
7. Now we need to pass the Local IP from step 3 :

Note : Keep port number as it is.



Now, again it will continue to installation.

8. Interface Configuration



9. Now we will check if the SNORT is successfully installed or not, by checking it's version.

```
shantanu@shantanu:~$ snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

shantanu@shantanu:~$ _
```

SNORT Configuration

Follow the steps :

1. Now we need to continue as root user **“sudo su”** :

2. Now locate to **“/etc/snort”** using cd command :

```
root@shantanu:/etc/snort# ls
classification.config  gen-msg.map       rules       snort.debian.conf  unicode.map
community-sid-msg.map  reference.config  snort.conf  threshold.conf
root@shantanu:/etc/snort# _
```

3. We need to modify the **“snort.conf”** configuration file, but before it we must have a backup copy of it.

```
root@shantanu:/etc/snort# cp snort.conf snort_copy.conf
root@shantanu:/etc/snort# ls
classification.config  gen-msg.map       rules       snort_copy.conf    threshold.conf
community-sid-msg.map  reference.config  snort.conf  snort.debian.conf  unicode.map
root@shantanu:/etc/snort#
```

4. Now we will edit the original file in our editor to change the **“Network Variable”** :

```
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ################################################
43
44 # Setup the network addresses you are protecting
45 #
46 # Note to Debian users: this value is overriden when starting
47 # up the Snort daemon through the init.d script by the
48 # value of DEBIAN_SNORT_HOME_NET s defined in the
49 # /etc/snort/snort.debian.conf configuration file
50 #
51 ipvar HOME_NET 10.0.2.15/16
52
```

Hint : Scroll down the file to see the rules defined in the file

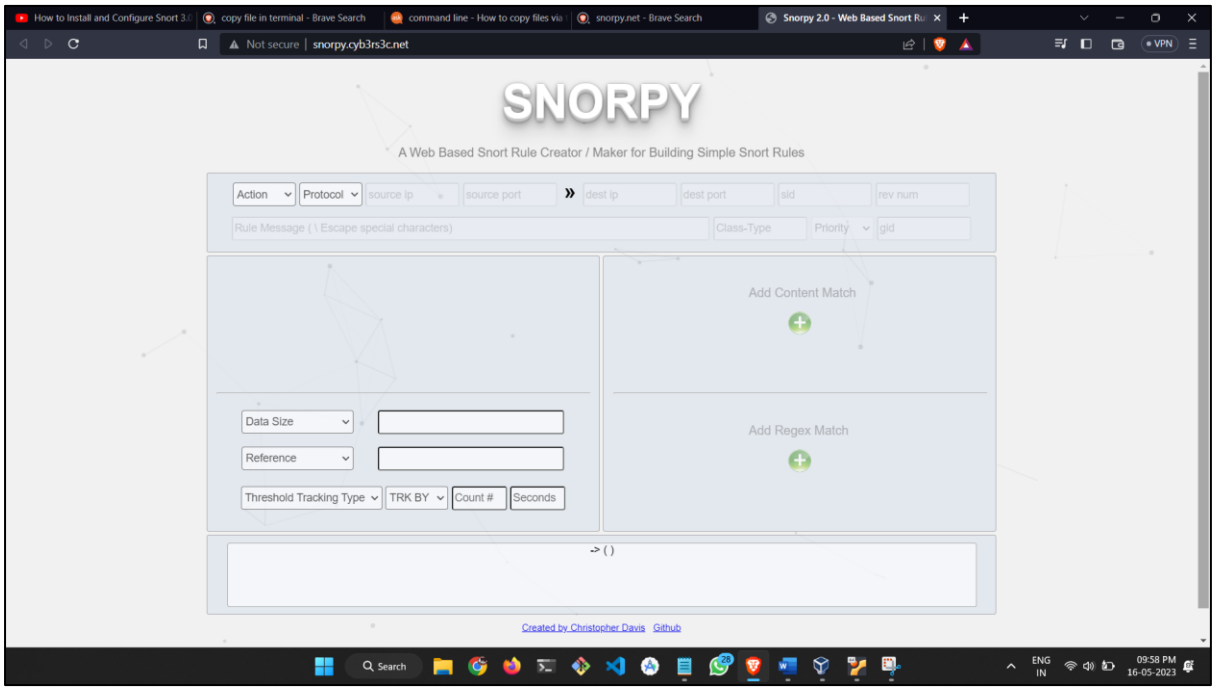
5. To see which are the default rules that are active right now go to “Rules” Folder in the same directory :

Hint : If you wish, you may read the rules by simply opening any one rules file.

```
root@shantanu:/etc/snort/rules# ls
attack-responses.rules          community-nntp.rules           deleted.rules       netbios.rules     sql.rules
backdoor.rules                  community-oracle.rules         dns.rules           nntp.rules        telnet.rules
bad-traffic.rules               community-policy.rules         dos.rules           oracle.rules      tftp.rules
chat.rules                      community-sip.rules            experimental.rules  other-ids.rules   virus.rules
community-bot.rules             community-smtp.rules           exploit.rules       p2p.rules         web-attacks.rules
community-deleted.rules         community-sql-injection.rules  finger.rules        policy.rules      web-cgi.rules
community-dos.rules             community-virus.rules          ftp.rules           pop2.rules        web-client.rules
community-exploit.rules         community-web-attacks.rules    icmp-info.rules     pop3.rules        web-coldfusion.rules
community-ftp.rules             community-web-cgi.rules        icmp.rules          porn.rules        web-frontpage.rules
community-game.rules            community-web-client.rules     imap.rules          rpc.rules         web-iis.rules
community-icmp.rules            community-web-dos.rules        info.rules          rservices.rules   web-misc.rules
community-imap.rules            community-web-iis.rules        local.rules         scan.rules        web-php.rules
community-inappropriate.rules   community-web-misc.rules       misc.rules          shellcode.rules   x11.rules
community-mail-client.rules     community-web-php.rules        multimedia.rules    smtp.rules
community-misc.rules            ddos.rules                     mysql.rules         snmp.rules
root@shantanu:/etc/snort/rules# _
```

6. If you want to write your own rules, you may write those rules in **“local.rules”** file present in the rules folder.

7. You can write rules using SNORPY Website http://snorpy.cyb3rs3c.net/



8. Now we have to checked if we have configured SNORT properly using **“snort -T -c /etc/snort/snort.conf”** :

```
Snort successfully validated the configuration!
Snort exiting
root@shantanu:~# _
```

It is successfully configured.

9. Now we will activate the SNORT in our machine :

Command - sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3

-A : to display

-q : display only necessary data

-c : configuration parameter

-i : interface name

```
root@shantanu:~# sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3
_
```

If it keeps on blinking, it means it's listening now.