

Install-Snort

snort installation in linux mint

step1

update to system before installing snort

command: apt-get update && upgrade

```
apt-get update && upgrade
```

step2

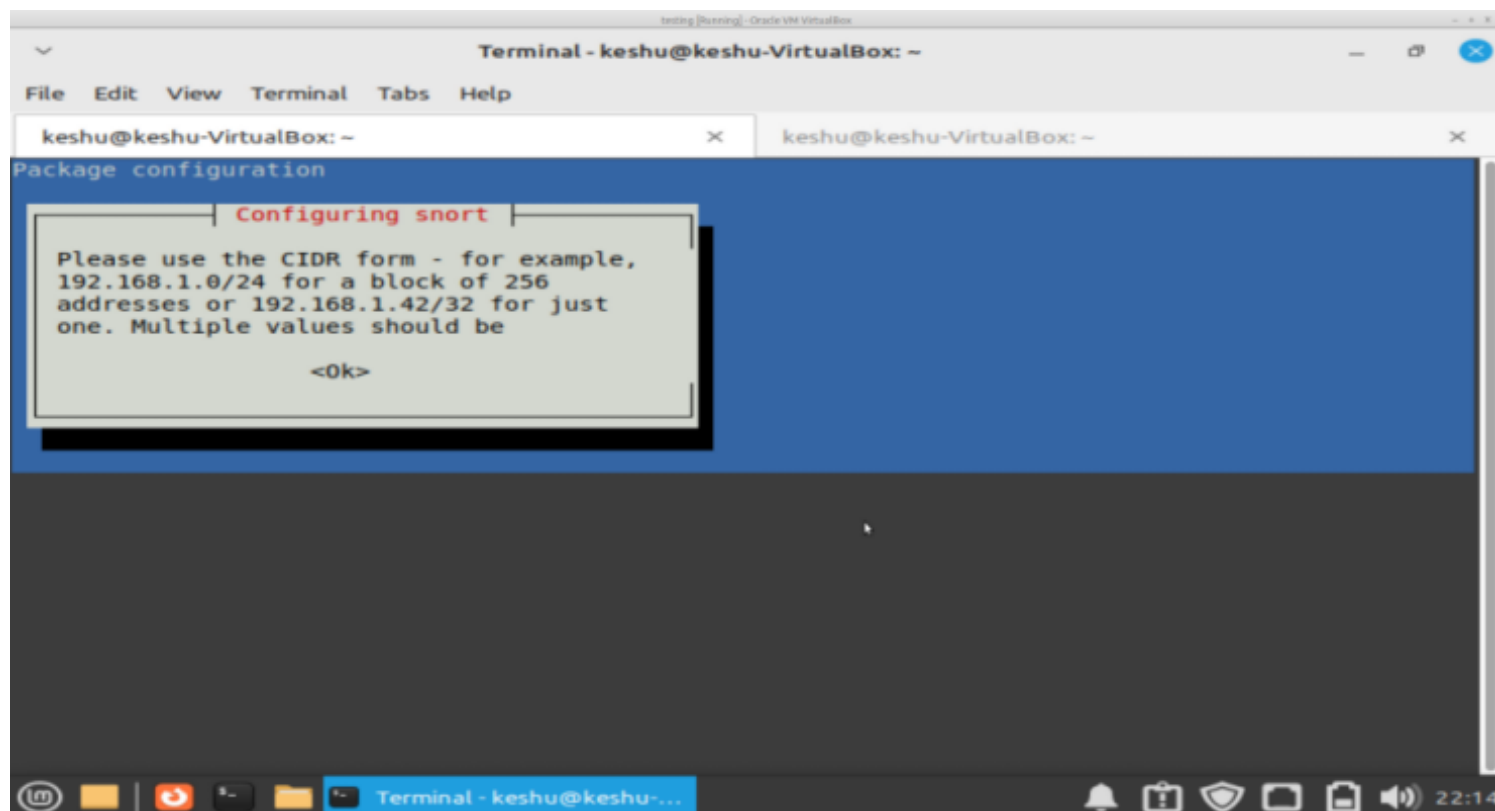
install snort 2 (there are two version of snort available , (snort2, snort3), we are going to install snort2)

command: apt install snort

```
sudo apt install snort
```

step3

while installing you'll see this below screen



If you get this above screen then,
type your ip address with CIDR notation

step4

if you not get a screen which ask for interface value, then use (ip a) command
you get your interface name, example given below

```

keshu@keshu-VirtualBox:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 08:00:27:6c:a8:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.5/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 418sec preferred_lft 418sec
    inet6 fe80::eefc:8854:9f80:58ad/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
keshu@keshu-VirtualBox:~$

```

enp0s3 is interface name of my machine,

NOTE: in you it may be diffrent

=====

step5

lets verify our interface name is correctly set or not

use this command to edit your interface name ,

if it's not correct , if correct then just verify it.

```

sudo vim snort.debian.conf

```

after using above command, you see like this below screen

```

keshav@inquisitive: ~
File Edit View Search Terminal Help
1 # snort.debian.config (Debian Snort configuration file)
2 #
3 # This file was generated by the post-installation script of the snort
4 # package using values from the debconf database.
5 #
6 # It is used for options that are changed by Debian to leave
7 # the original configuration files untouched.
8 #
9 # This file is automatically updated on upgrades of the snort package
10 # *only* if it has not been modified since the last upgrade of that package.
11 #
12 # If you have edited this file but would like it to be automatically updated
13 # again, run the following command as root:
14 #   dpkg-reconfigure snort
15
16 DEBIAN_SNORT_STARTUP="boot"
17 DEBIAN_SNORT_HOME_NET="192.168.43.4/24"
18 DEBIAN_SNORT_OPTIONS=""
19 DEBIAN_SNORT_INTERFACE="wlo1"
20 DEBIAN_SNORT_SEND_STATS="true"
21 DEBIAN_SNORT_STATS_RCPT="root"
22 DEBIAN_SNORT_STATS_THRESHOLD="1"
~
"/etc/snort/snort.debian.conf" 22L, 805C 1,1 All

```

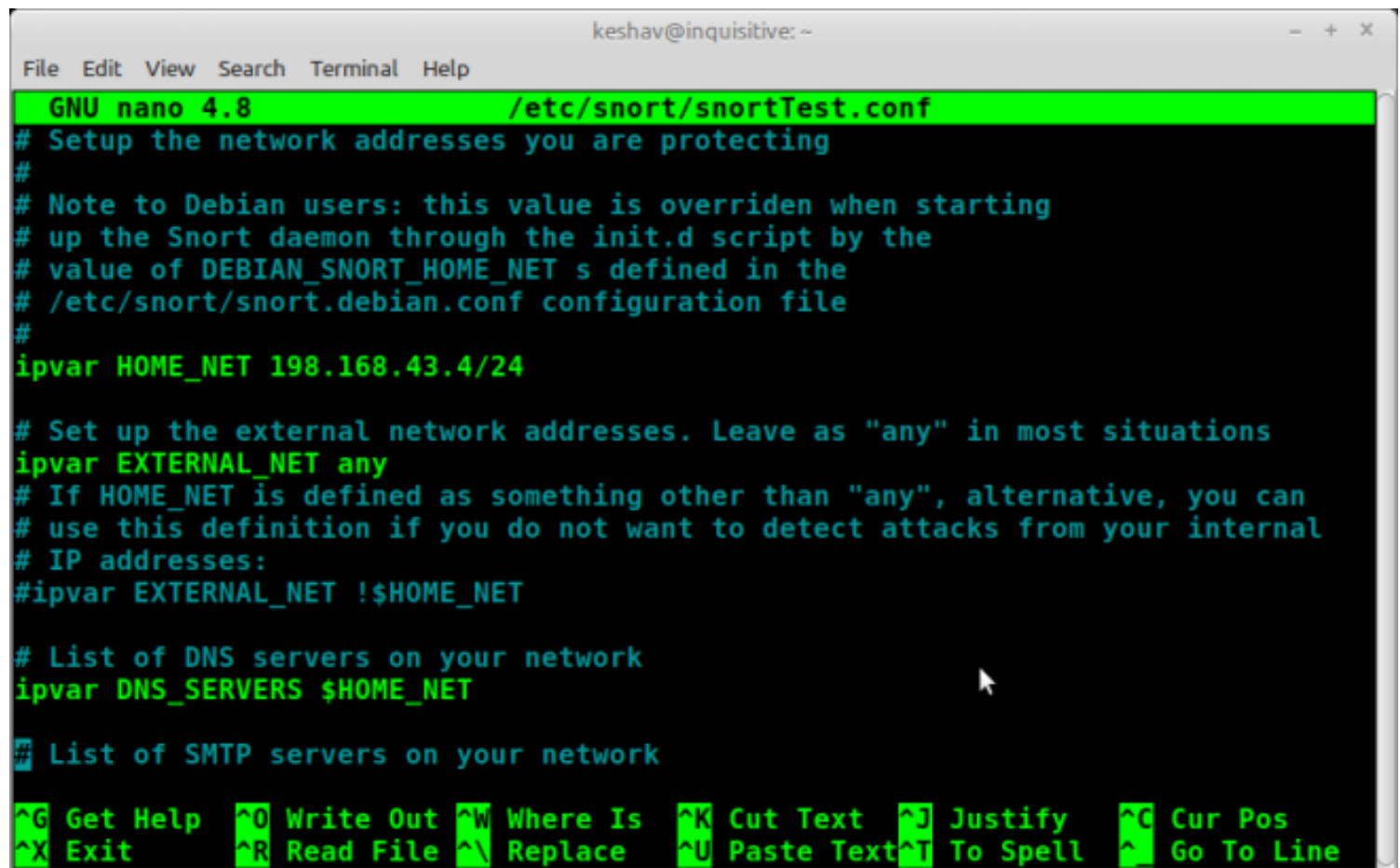
match you ip and interface id name.

STEP6

now all set , lets start changing our config file,
open config file of snort.conf,
command given below

```
sudo vim /etc/snort/snort.conf
```

change the HOME_NET Value, it should be you ip address with its range



```
keshav@inquisitive: ~
File Edit View Search Terminal Help
GNU nano 4.8 /etc/snort/snortTest.conf
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 198.168.43.4/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^N Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

after changing save it.

Step7

Open rule file of snort
command

```
sudo vim /etc/snort/rules/local.rules
```

write rule for ping and ssh attempt detection

```
keshav@inquisitive: ~  
File Edit View Search Terminal Help  
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $  
2 # -----  
3 # LOCAL RULES  
4 # -----  
5 # This file intentionally does not come with signatures.  Put your local  
6 # additions here.  
7  
8  
9  
10 alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:100002; rev:1;)  
11  
~  
~  
~  
~  
~  
~  
~  
-- INSERT --
```