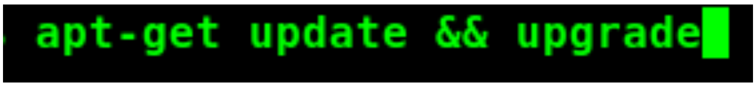
snort installation in linux mint

step1

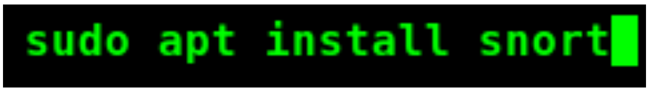
update to system before installing snort
comaand: apt-get update && upgrade



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

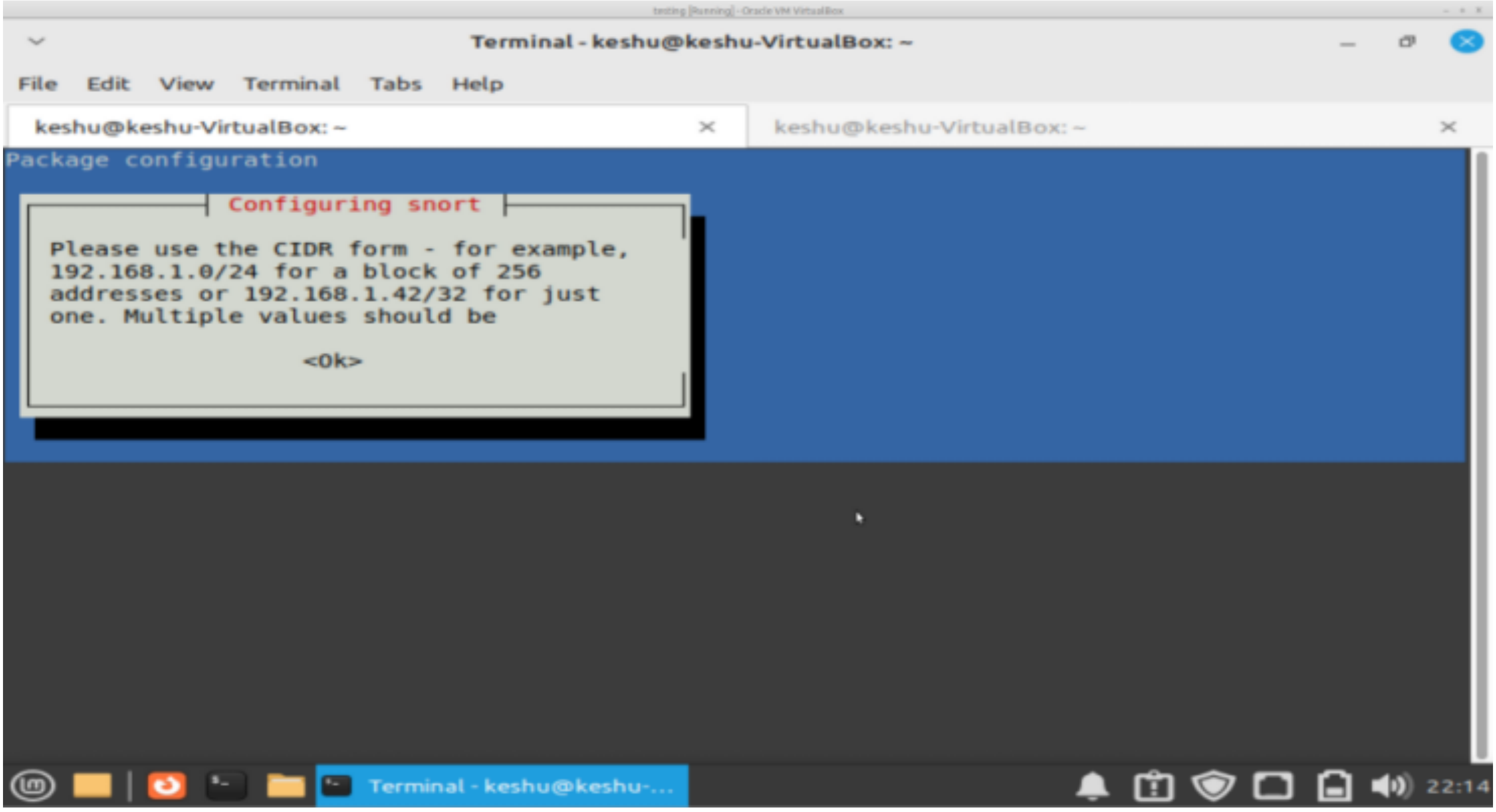
step2

install snort 2 (there are two version of snorrt avilable , (snort2, snort3), we are going to install snort2)
command: apt install snort



```
sudo apt install snort
```

step3
while installing yot this below screen



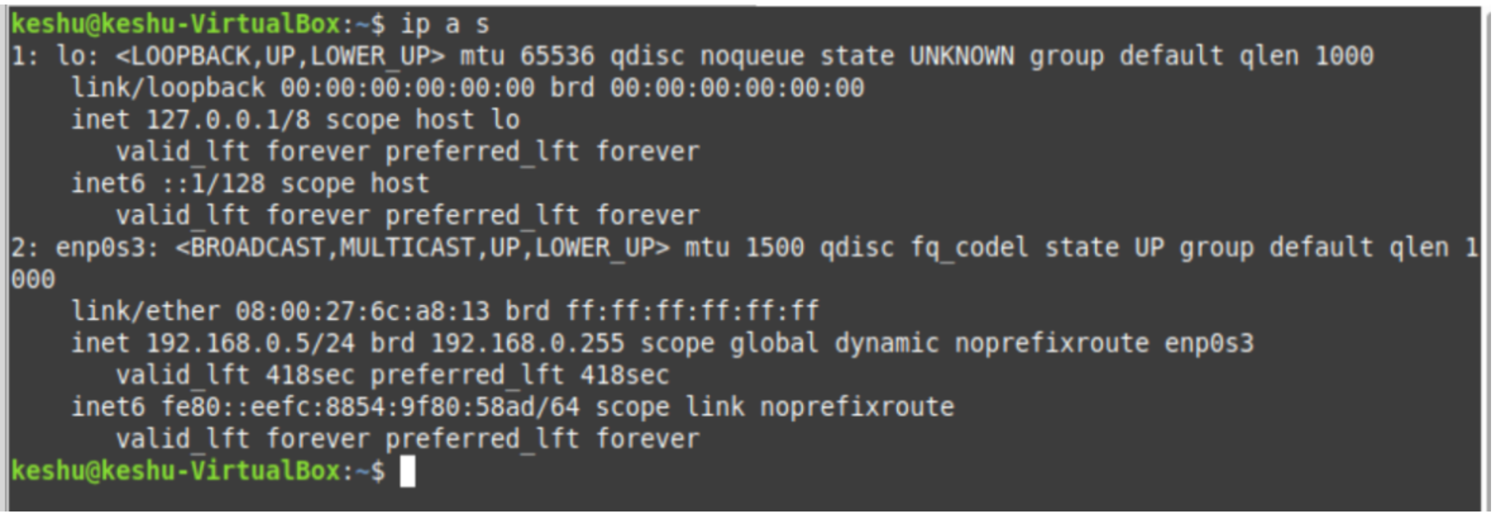
Terminal - keshu@keshu-VirtualBox: ~
File
Edit
View
Terminal
Tabs
Help
keshu@keshu-VirtualBox: ~
keshu@keshu-VirtualBox: ~
Terminal - keshu@keshu-...
22:14

```
Package configuration

Configuring snort

Please use the CIDR form - for example,
192.168.1.0/24 for a block of 256
addresses or 192.168.1.42/32 for just
one. Multiple values should be

                  <Ok>
```

If you get this above screen then,
type your ip addres 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:~$
```

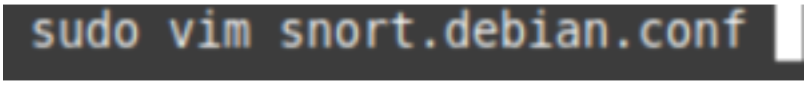
enp0s3 is interface name of my machine,

NOTE: in you it may be diffrent

==

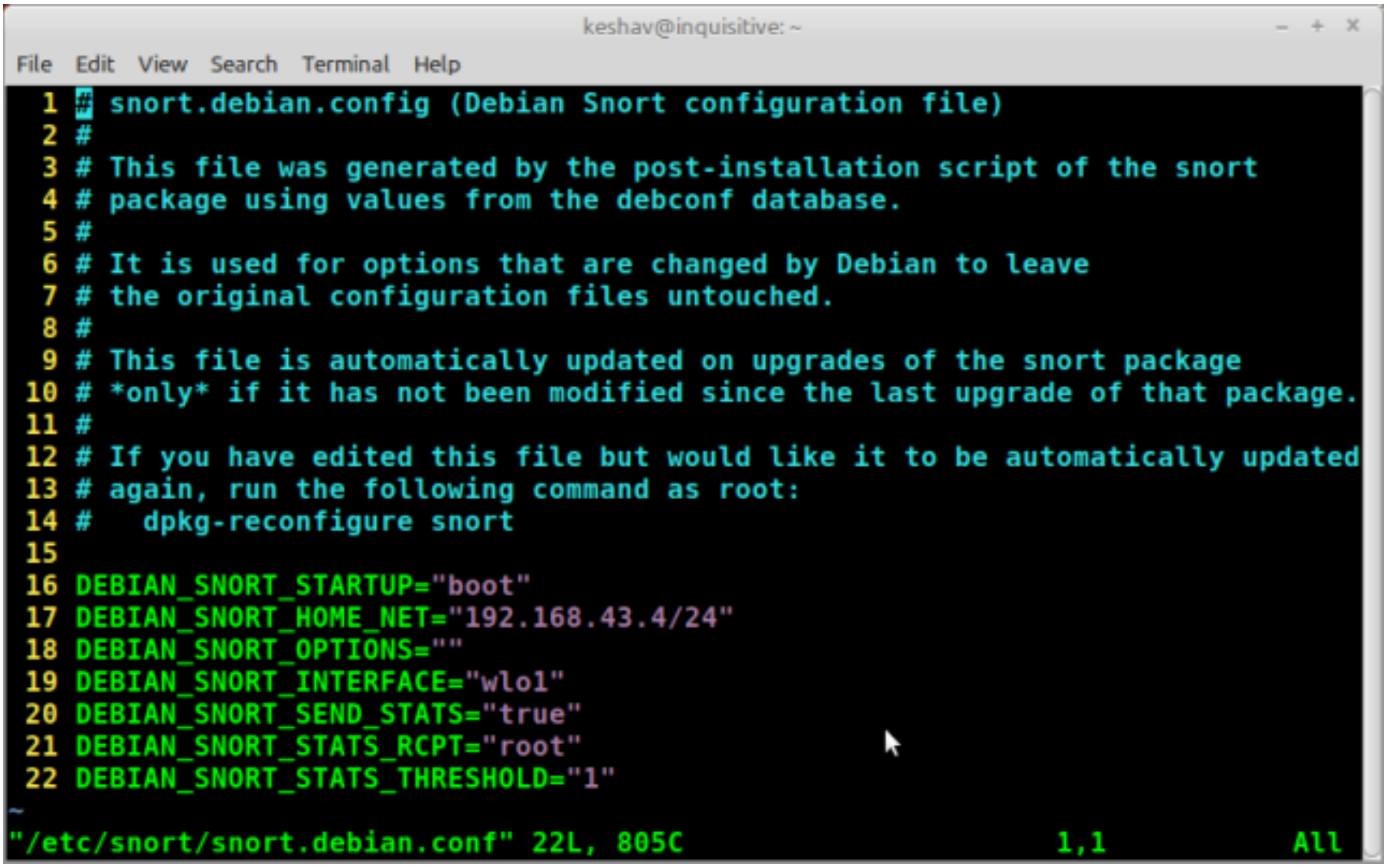
step5

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

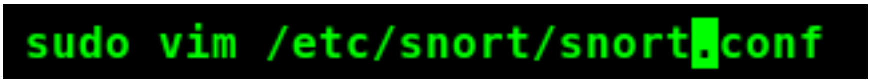


```
# snort.debian.config (Debian Snort configuration file)
#
# This file was generated by the post-installation script of the snort
# package using values from the debconf database.
#
# It is used for options that are changed by Debian to leave
# the original configuration files untouched.
#
# This file is automatically updated on upgrades of the snort package
# *only* if it has not been modified since the last upgrade of that package.
#
# If you have edited this file but would like it to be automatically updated
# again, run the following command as root:
#   dpkg-reconfigure snort

DEBIAN_SNORT_STARTUP="boot"
DEBIAN_SNORT_HOME_NET="192.168.43.4/24"
DEBIAN_SNORT_OPTIONS=""
DEBIAN_SNORT_INTERFACE="wlo1"
DEBIAN_SNORT_SEND_STATS="true"
DEBIAN_SNORT_STATS_RCPT="root"
DEBIAN_SNORT_STATS_THRESHOLD="1"
~
"/etc/snort/snort.debian.conf" 22L, 805C                    1,1           All
```

match you ip and interface id name.

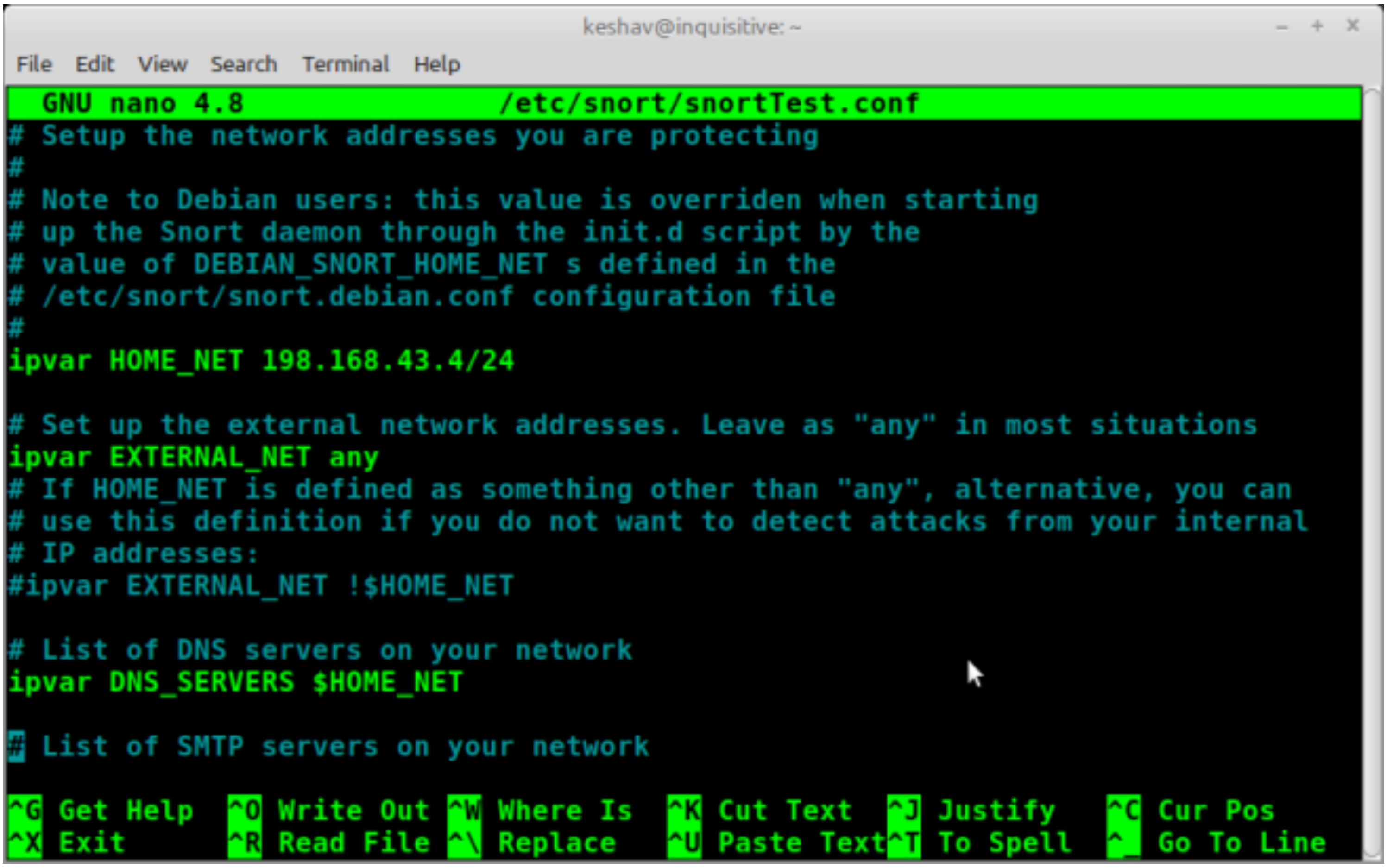
STEP6

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 addres with its range

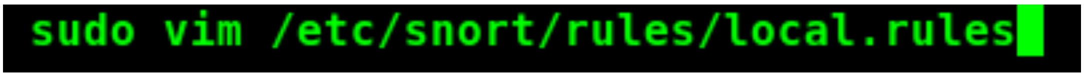


```
  GNU nano 4.8                /etc/snort/snortTest.conf
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf 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  ^\ Replace    ^U Paste Text^T To Spell    ^_ Go To Line
```

after changing save it.

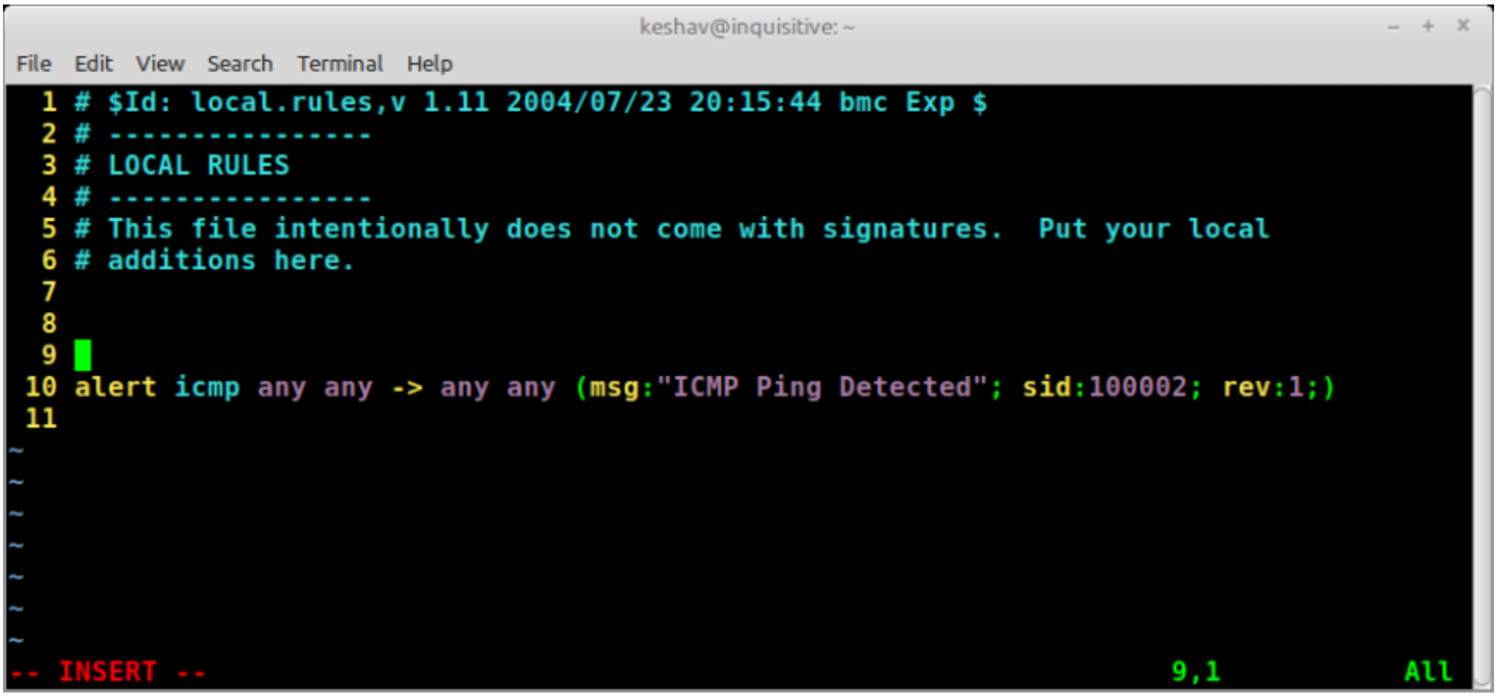
Step7

Open rule file of snort
command



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

write rule for ping and ssh attempt detection

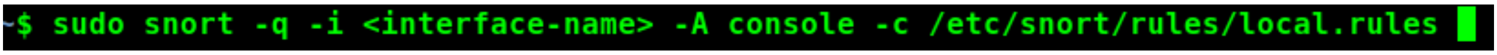


```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.



alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:100002; rev:1;)

~
~
~
~
~
~
~
-- INSERT --                                                  9,1           All
```

in above figure i writed one rule,
for PING detection, save this rule file.

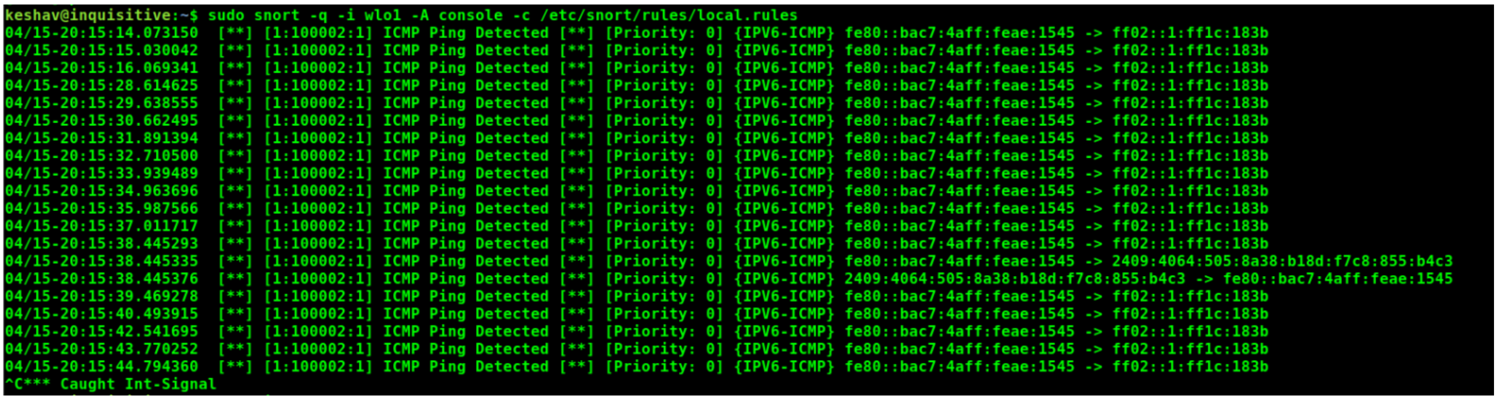
Step8

lets run our snort,
command for runing snort is given below



```
~$ sudo snort -q -i <interface-name> -A console -c /etc/snort/rules/local.rules
```

OUTPUT Look like this

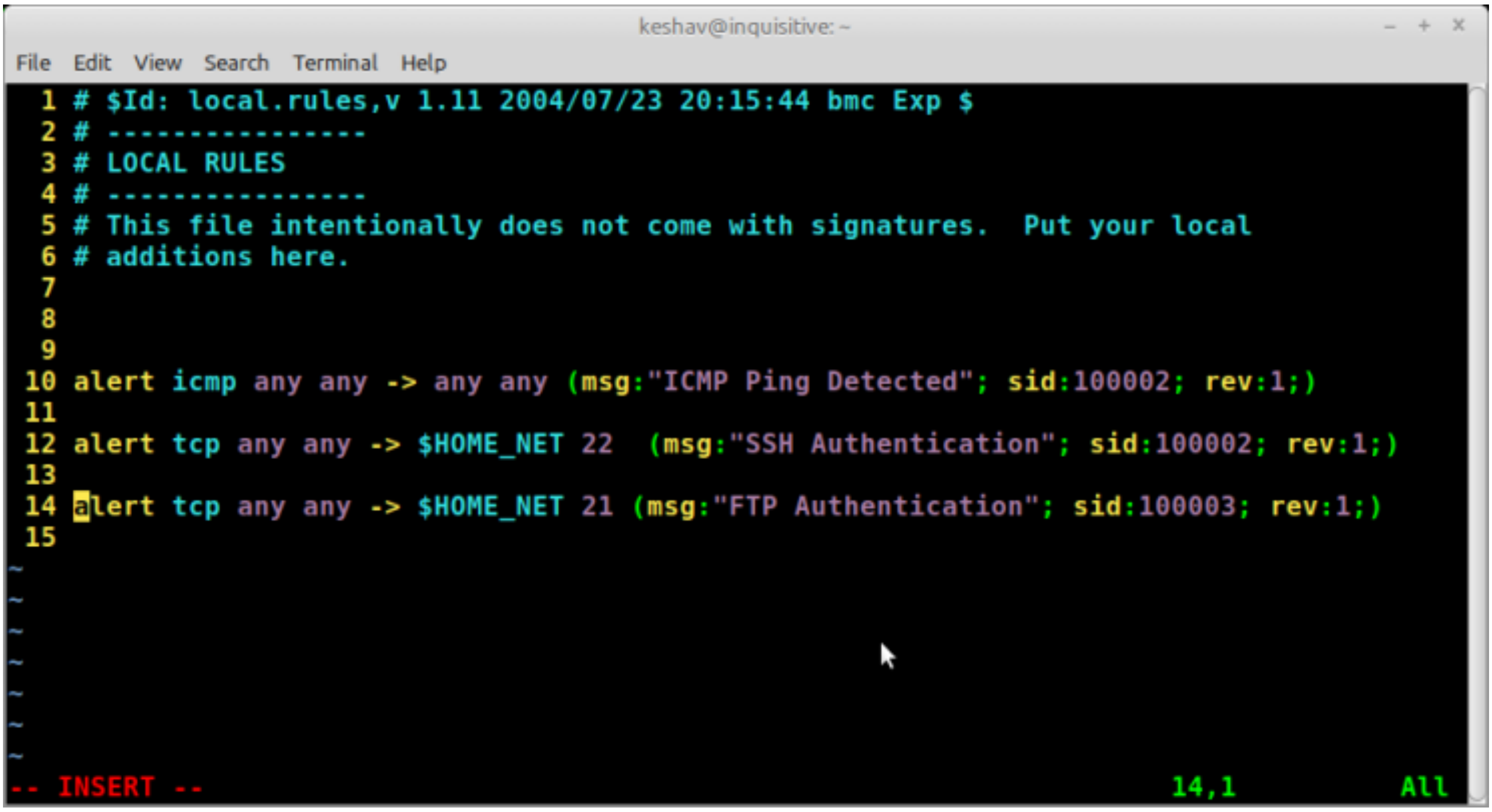


```
keshav@inquisitive:~$ sudo snort -q -i wlo1 -A console -c /etc/snort/rules/local.rules
04/15-20:15:14.073150  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:15.030042  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:16.069341  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:28.614625  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:29.638555  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:30.662495  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:31.891394  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:32.710500  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:33.939489  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:34.963696  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:35.987566  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:37.011717  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:38.445293  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:38.445335  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> 2409:4064:505:8a38:b18d:f7c8:855:b4c3
04/15-20:15:38.445376  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} 2409:4064:505:8a38:b18d:f7c8:855:b4c3 -> fe80::bac7:4aff:feae:1545
04/15-20:15:39.469278  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:40.493915  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:42.541695  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:43.770252  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
04/15-20:15:44.794360  [**] [1:100002:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> ff02::1:ff1c:183b
^C*** Caught Int-Signal
```

===
==========================

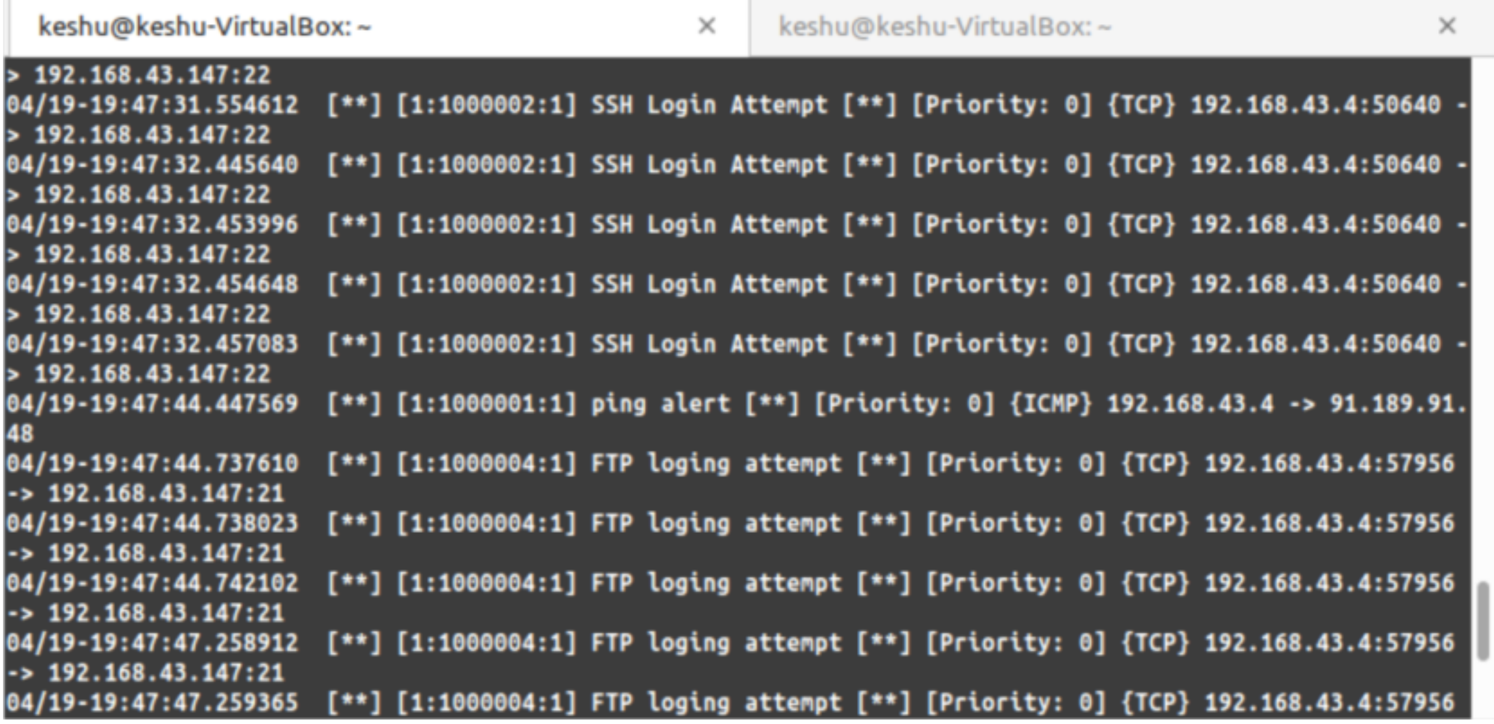
Now lets add two more rules,

1st for PING and Second for SSH and Third for FTP ,



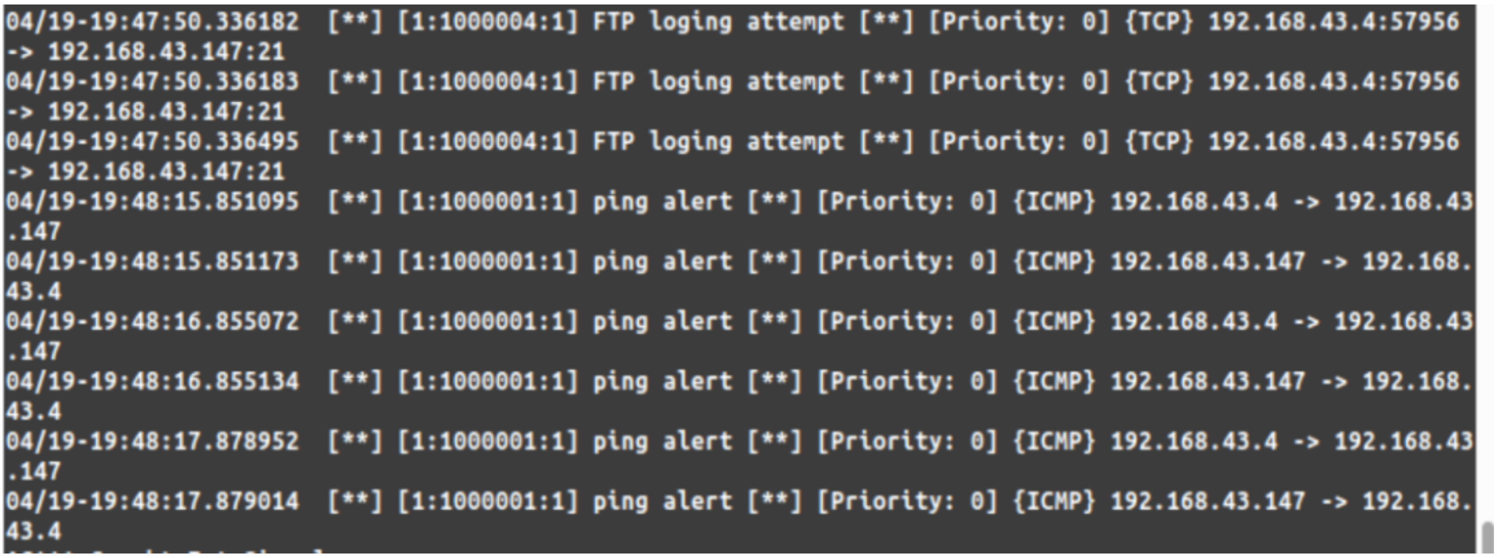
```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.



alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:100002; rev:1;)

alert tcp any any -> $HOME_NET 22  (msg:"SSH Authentication"; sid:100002; rev:1;)

alert tcp any any -> $HOME_NET 21 (msg:"FTP Authentication"; sid:100003; rev:1;)

~
~
~
~
~
~
~
-- INSERT --                                                  14,1          All
```

Now run again snort,
lets see how ssh and ftp loging attempts look like,
In Fig1 and Fig2 we can see SSH ,FTP and PING attempt on our network



```
> 192.168.43.147:22
04/19-19:47:31.554612  [**] [1:1000002:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.43.4:50640 -
> 192.168.43.147:22
04/19-19:47:32.445640  [**] [1:1000002:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.43.4:50640 -
> 192.168.43.147:22
04/19-19:47:32.453996  [**] [1:1000002:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.43.4:50640 -
> 192.168.43.147:22
04/19-19:47:32.454648  [**] [1:1000002:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.43.4:50640 -
> 192.168.43.147:22
04/19-19:47:32.457083  [**] [1:1000002:1] SSH Login Attempt [**] [Priority: 0] {TCP} 192.168.43.4:50640 -
> 192.168.43.147:22
04/19-19:47:44.447569  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.4 -> 91.189.91.
48
04/19-19:47:44.737610  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:44.738023  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:44.742102  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:47.258912  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:47.259365  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
```

Fig2



```
04/19-19:47:50.336182  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:50.336183  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:47:50.336495  [**] [1:1000004:1] FTP loging attempt [**] [Priority: 0] {TCP} 192.168.43.4:57956
-> 192.168.43.147:21
04/19-19:48:15.851095  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.4 -> 192.168.43
.147
04/19-19:48:15.851173  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.147 -> 192.168.
43.4
04/19-19:48:16.855072  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.4 -> 192.168.43
.147
04/19-19:48:16.855134  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.147 -> 192.168.
43.4
04/19-19:48:17.878952  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.4 -> 192.168.43
.147
04/19-19:48:17.879014  [**] [1:1000001:1] ping alert [**] [Priority: 0] {ICMP} 192.168.43.147 -> 192.168.
43.4
```

NOTE

if you want, snort drop down ssh login attempt, after 3 attempt then go and learn deep about writing snort rules,

It will help to write advanced rules