Assignment No. 4

AIM :

Configure and demonstrate use of traffic monitoring tool such as Snort security perspective.

OBJECTIVE :

Study any network intrusion software and use its implementation features.

THEORY :

Introduction to Snort

Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) created in 1998 by Martin Roesch. Snort is now developed by Cisco, which purchased Sourcefire in 2013.

Snort is an open source intrusion prevention system offered by Cisco. It is capable of real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort can be used as a packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), network file logging device (capturing files in realtime from network traffic), or as a full blown network intrusion prevention system. The mission for Snort is to deliver the most effective and comprehensive real-time network defense solutions on the planet.

Snort consists of the following components :

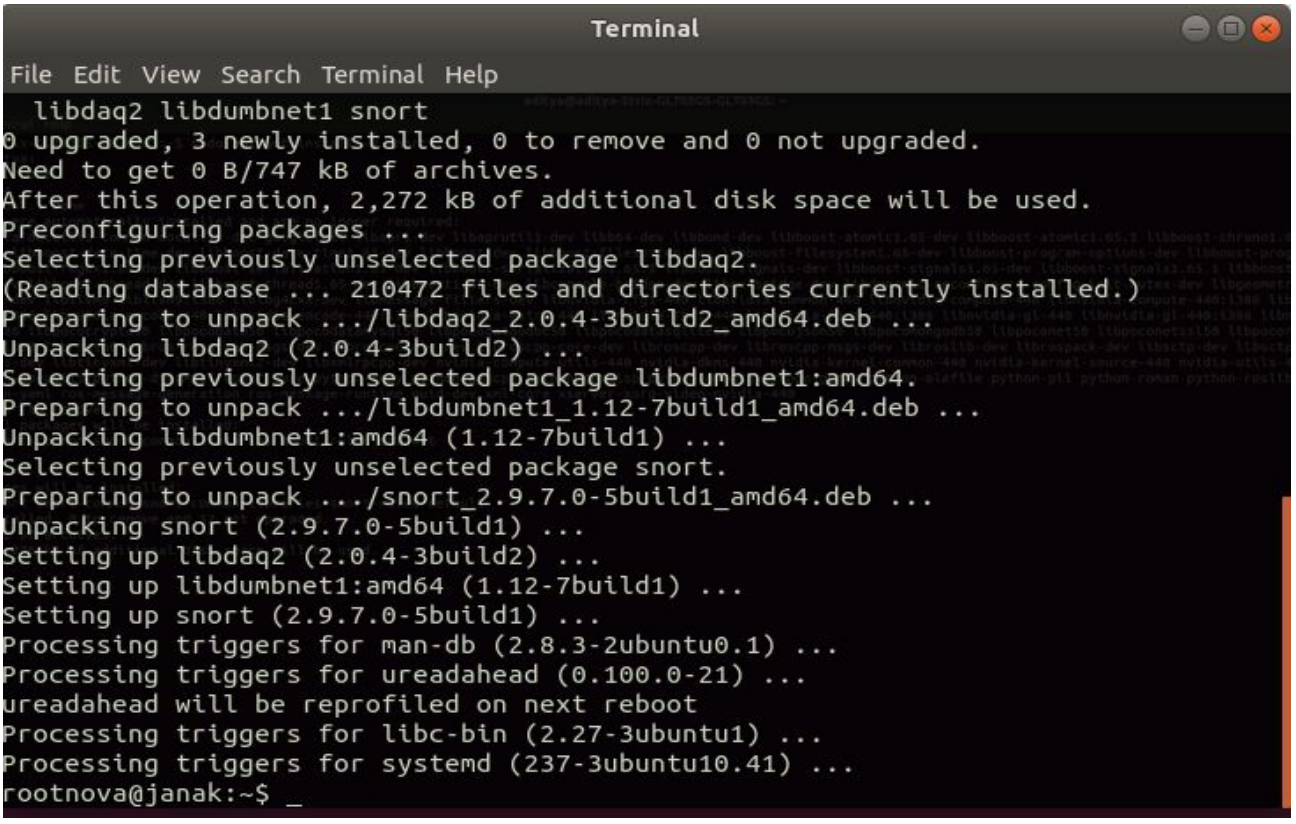
- Packet Decoder
- Pre-processors
- Detection Engine
- Logging and Alerting System
- Output Modules

Platforms on which Snort runs :

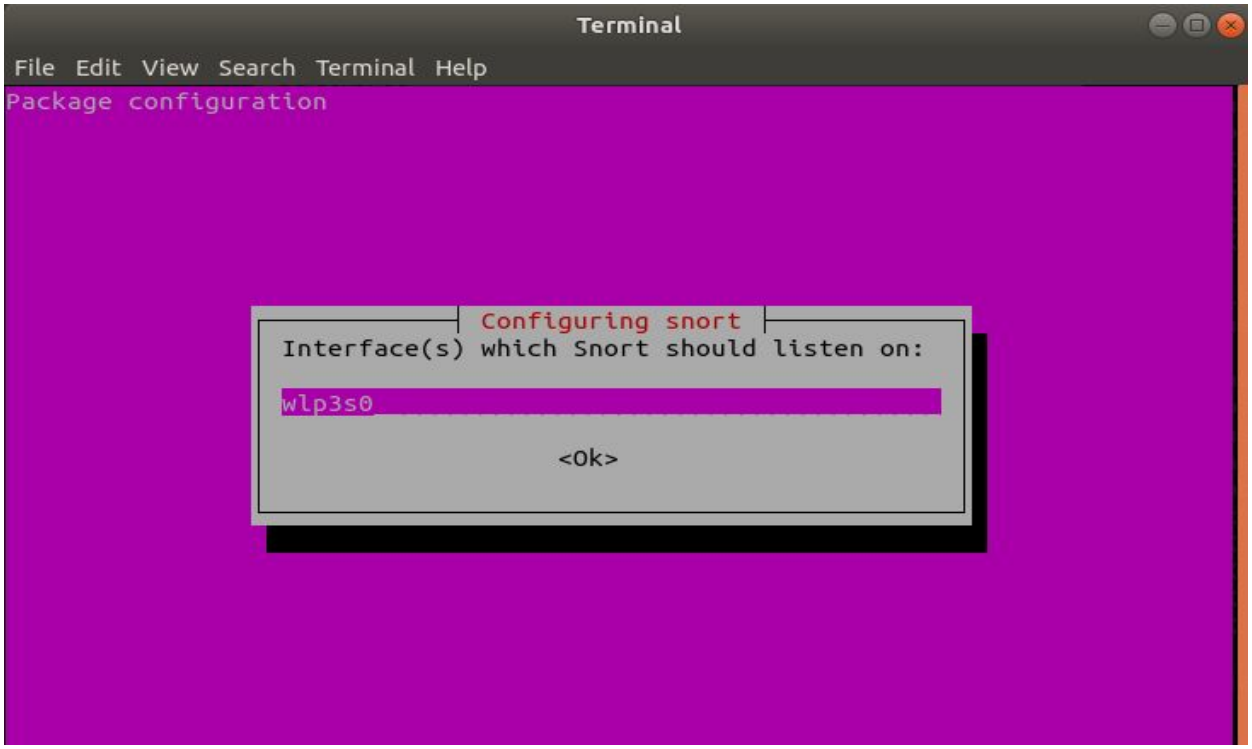
- Unix
  Applet,MAC,BEOS,JBM,AIX,BSD open etc.
- LINUX
  Mandrake LINUX,Red Hat,SUSE Linux etc.
- Windows
  Windows server 2003/XP/2000/NT/7/10

Installation of Snort :

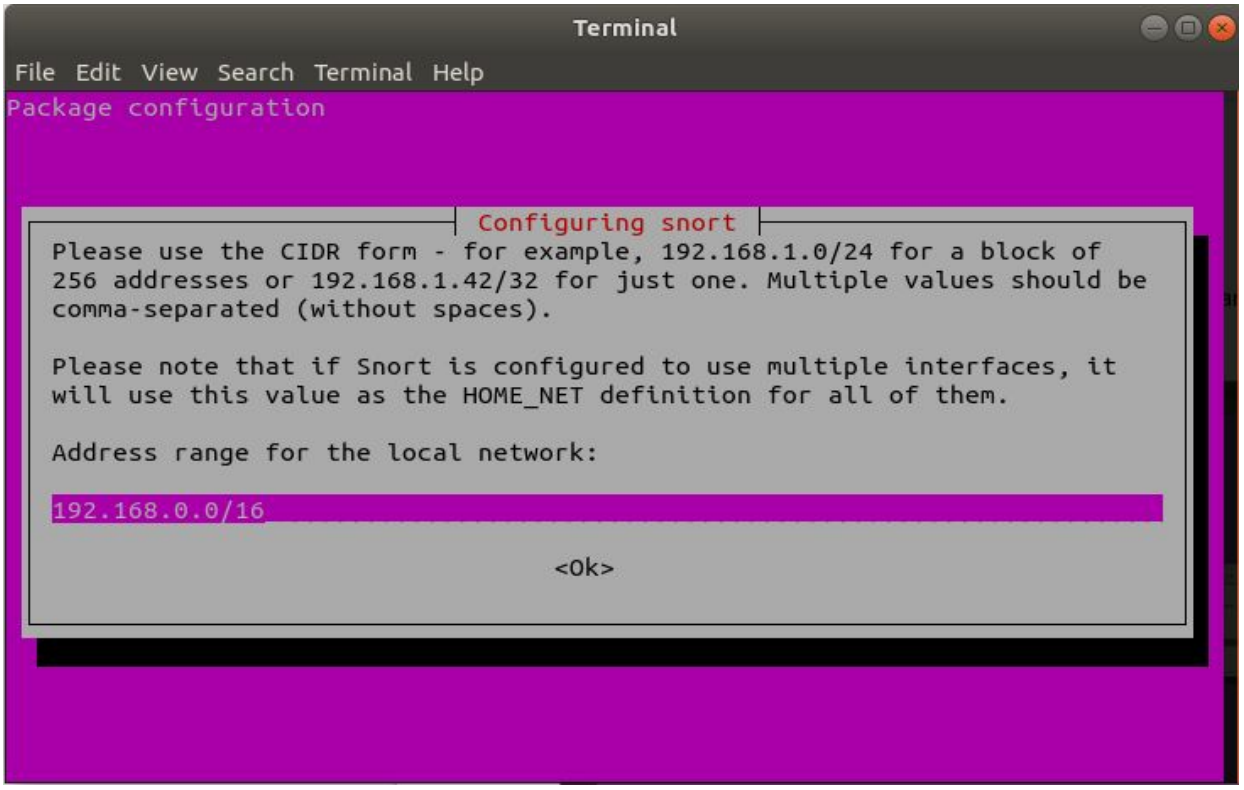
- Snort is installed using the following command
  sudo apt-get install snort



- Once the installation starts,it will ask you the interface that we previously checked. Give its name here and press enter

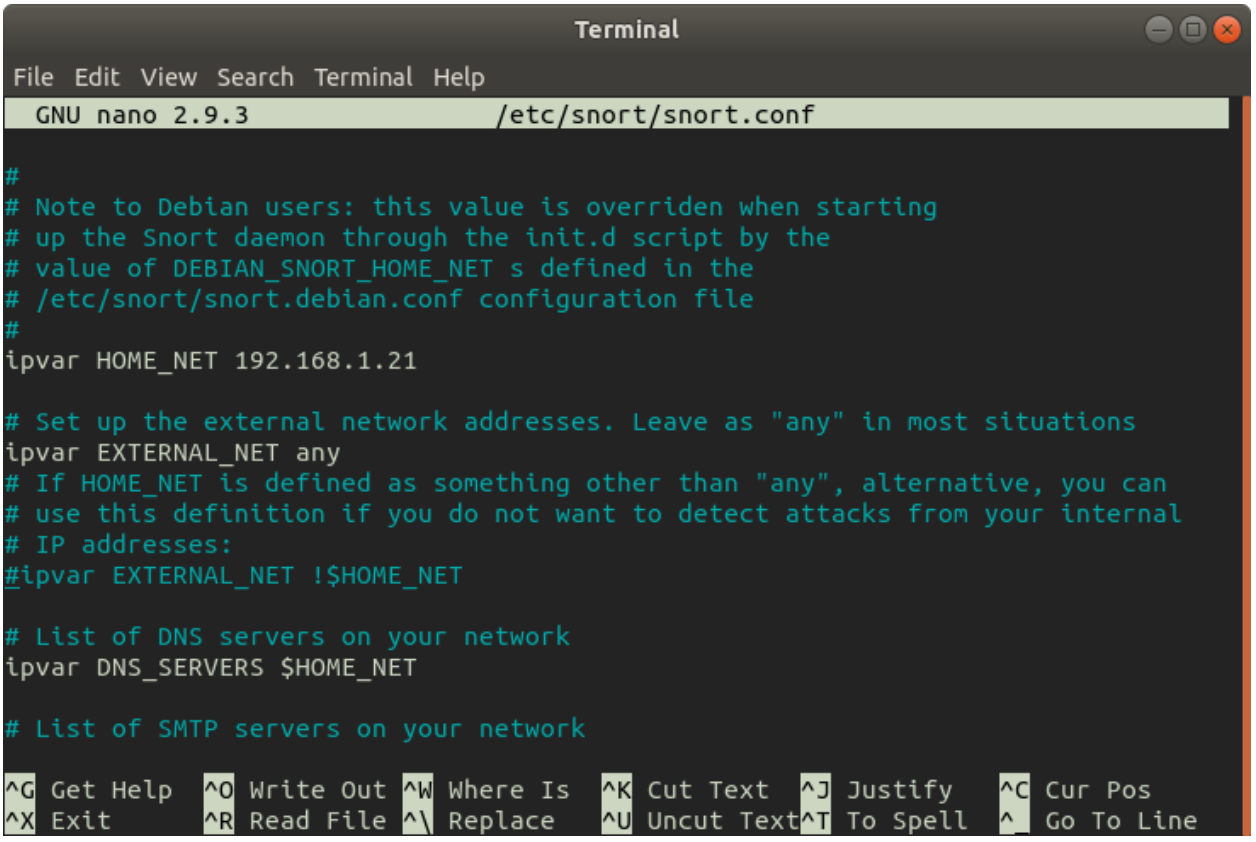


- Then it will ask you about your network IP.Here, you can either provide a single IP or the range of IPs.



- As the snort is installed,open the configuration file using nano or any text editor to make some changes inside.

sudo nano/etc/snort/snort.conf



- Scroll down the text file near line number 45 to specify your network for protection as shown in the given image.

- Now run the below command to enable IDS mode of snort. sudo snort -A console eno2 -c /etc/snort/snort.conf

- Once the snort is installed and configured, we can start making changes to its rules as per our own requirement and desire.

```
Terminal
File  Edit  View  Search  Terminal  Help
|     2 byte states : 13.83
|     4 byte states : 0.00
+-----------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1036 ]
pcap DAQ configured to passive.
Acquiring network traffic from "wlp3s0".
Reload thread starting...
Reload thread started, thread 0x7fe1e2019700 (8197)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> 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 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
Commencing packet processing (pid=8192)
_
```

- cd /etc/snort/rules ls -la

```
Terminal
File  Edit  View  Search  Terminal  Help

rootnova@janak:~$ cd /etc/snort/rules
rootnova@janak:/etc/snort/rules$ ls -la
total 1592
drwxr-xr-x 2 root root   4096 Sep 19 11:41 .
drwxr-xr-x 3 root root   4096 Sep 22 11:03 ..
-rw-r--r-- 1 root root      0 Sep 19 10:59 any
-rw-r--r-- 1 root root   5520 Apr  3  2018 attack-responses.rules
-rw-r--r-- 1 root root  17898 Apr  3  2018 backdoor.rules
-rw-r--r-- 1 root root   3862 Apr  3  2018 bad-traffic.rules
-rw-r--r-- 1 root root   7994 Apr  3  2018 chat.rules
-rw-r--r-- 1 root root  12759 Apr  3  2018 community-bot.rules
-rw-r--r-- 1 root root   1223 Apr  3  2018 community-deleted.rules
-rw-r--r-- 1 root root   2042 Apr  3  2018 community-dos.rules
-rw-r--r-- 1 root root   2176 Apr  3  2018 community-exploit.rules
-rw-r--r-- 1 root root    249 Apr  3  2018 community-ftp.rules
-rw-r--r-- 1 root root   1376 Apr  3  2018 community-game.rules
-rw-r--r-- 1 root root    689 Apr  3  2018 community-icmp.rules
-rw-r--r-- 1 root root   2777 Apr  3  2018 community-imap.rules
-rw-r--r-- 1 root root    948 Apr  3  2018 community-inappropriate.rules
-rw-r--r-- 1 root root    257 Apr  3  2018 community-mail-client.rules
-rw-r--r-- 1 root root   7837 Apr  3  2018 community-misc.rules
-rw-r--r-- 1 root root    621 Apr  3  2018 community-nntp.rules
-rw-r--r-- 1 root root    775 Apr  3  2018 community-oracle.rules
-rw-r--r-- 1 root root   1621 Apr  3  2018 community-policy.rules
-rw-r--r-- 1 root root   3551 Apr  3  2018 community-sip.rules
-rw-r--r-- 1 root root   2722 Apr  3  2018 community-smtp.rules
-rw-r--r-- 1 root root   4063 Apr  3  2018 community-sql-injection.rules
-rw-r--r-- 1 root root   3742 Apr  3  2018 community-virus.rules
-rw-r--r-- 1 root root   2406 Apr  3  2018 community-web-attacks.rules
-rw-r--r-- 1 root root   5128 Apr  3  2018 community-web-cgi.rules
-rw-r--r-- 1 root root   4589 Apr  3  2018 community-web-client.rules
-rw-r--r-- 1 root root    254 Apr  3  2018 community-web-dos.rules
-rw-r--r-- 1 root root   1473 Apr  3  2018 community-web-iis.rules
-rw-r--r-- 1 root root  68917 Apr  3  2018 community-web-misc.rules
-rw-r--r-- 1 root root 163259 Apr  3  2018 community-web-php.rules
-rw-r--r-- 1 root root   7646 Apr  3  2018 ddos.rules
-rw-r--r-- 1 root root  64313 Apr  3  2018 deleted.rules
```

- To check whether the Snort is logging any alerts as proposed,add a detection
- rule alert on IP packets in the “local.rules file”
  -> echo “”>icmp-info.rules
  -> cat icmp-info.rules

```
root@janak:/etc/snort/rules# echo "" >icmp-info.rules
root@janak:/etc/snort/rules# cat icmp-info.rules

root@janak:/etc/snort/rules# cat icmp.rules
```

- Sample Rule alert icmp any any
  -> 192.168.1.21 any (msg: “ICMP Packet found”; sid:10000001;)
- On intrusion snort will output

```
alert icmp any any -> 192.168.1.21 any (msg: “ICMP Packet found”; sid:10000001;)_
```

- Now we will apply rules on port 21,22 and 80.This way, whenever a suspicious packet is sent to these ports, we will be notified.Following are the rules to apply to achieve the said
  -> alert tcp any any-> any 21 (msg: “FTP Packet found”;sid:10000002;)
  -> alert tcp any any-> any 22 (msg: “FTP Packet found”;sid:10000003;)
  -> alert tcp any any-> any 80 (msg: “FTP Packet found”;sid:10000003;)

```
alert tcp any any-> any 21 (msg: “FTP Packet found”;sid:10000002; )
alert tcp any any-> any 22 (msg: “FTP Packet found”;sid:10000003; )
alert tcp any any-> any 80 (msg: “FTP Packet found”;sid:10000003; )
```

Conclusion :

In this assignment we studied about a network intrusion detection system called Snort, its installation process and showed its demonstration.