Lab : CL-VII

Assignment 4

Configure and Snort tool for network intrusion.

AIM

Configure and demonstrate use of Network Intrusion tools 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 :

As stated earlier, R is a programming language and software environment for statistical analysis, graphics representation and reporting. The following are the important features of R −

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

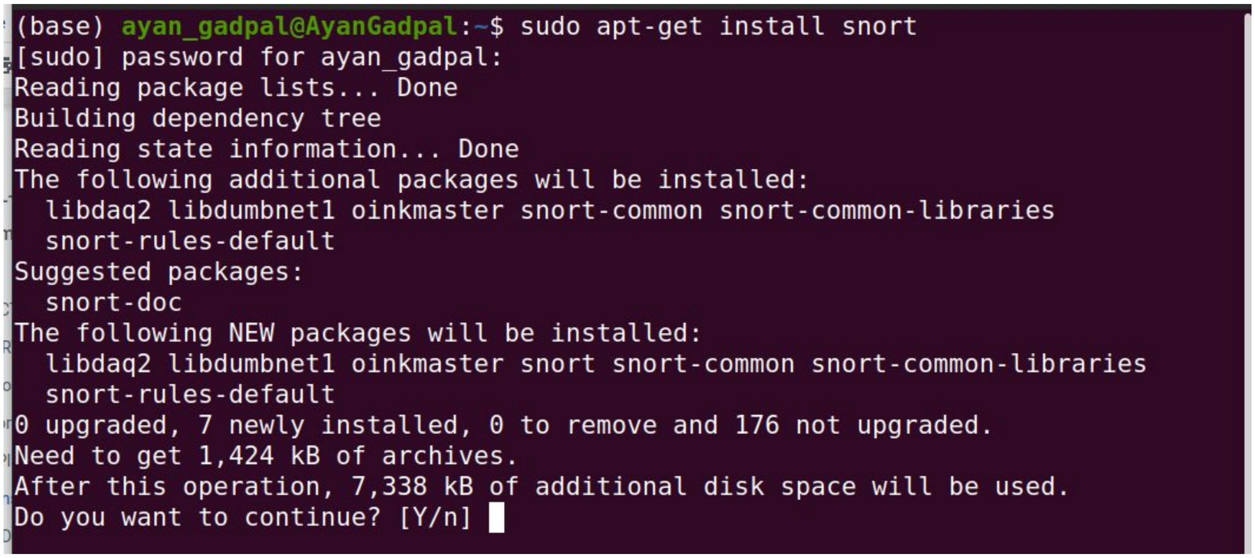
Platforms on which Snort runs

Snort runs on most UNIX and various windows. It requires GTK+, GTK6, libpcap and other libraries in order to run.

- 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

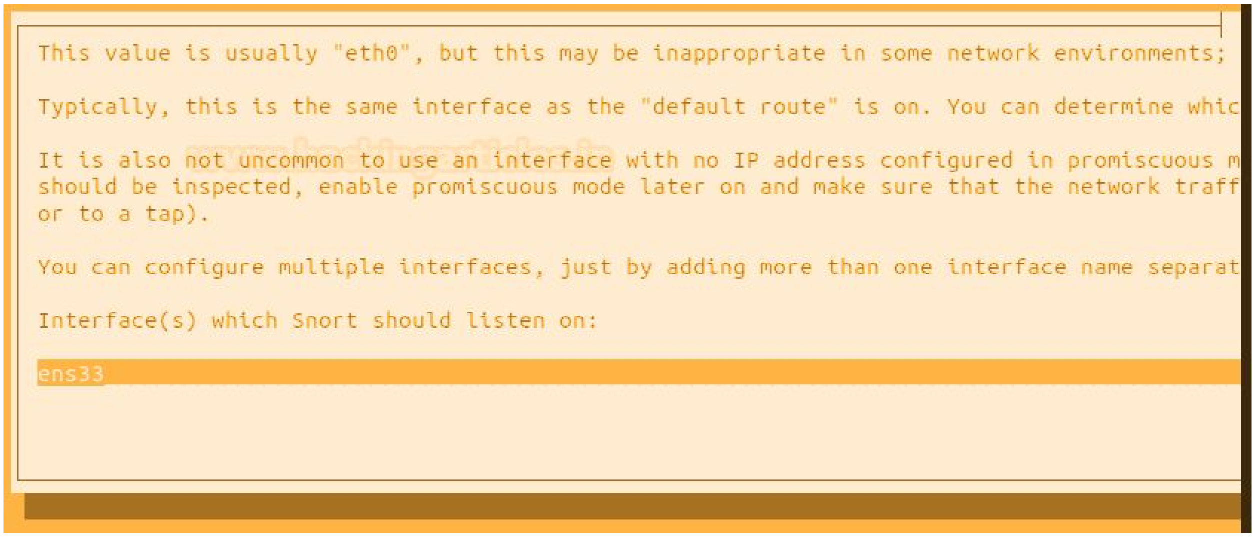
Installing Snort

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



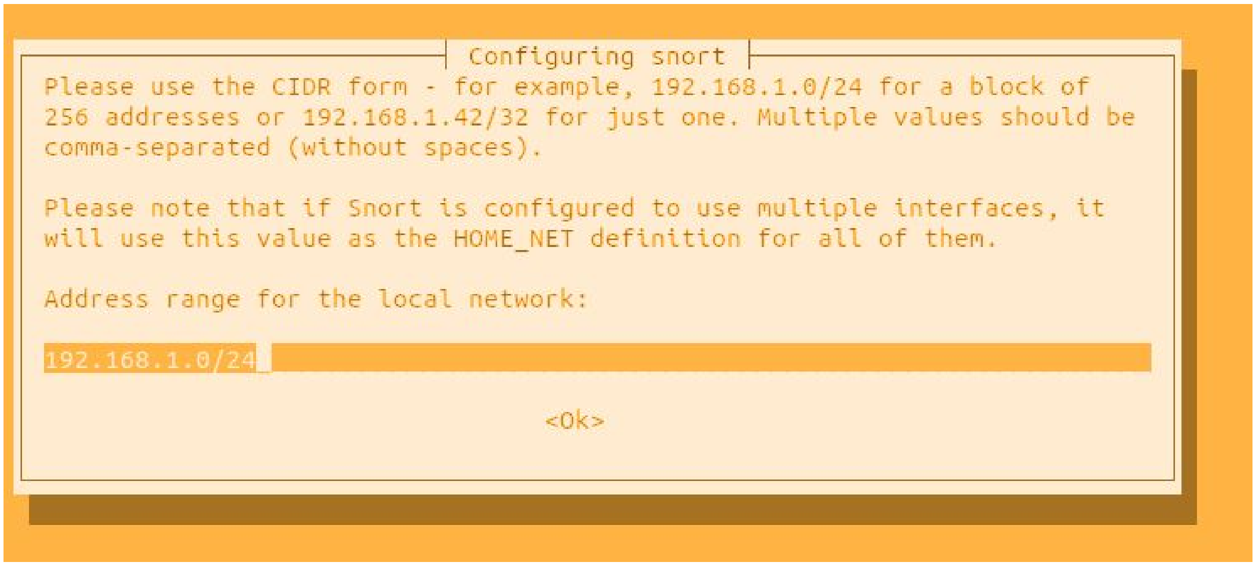
```
(base) ayan_gadpal@AyanGadpal:~$ sudo apt-get install snort
[sudo] password for ayan_gadpal:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries
  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 176 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]
```

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



```
This value is usually "eth0", but this may be inappropriate in some network environments;

Typically, this is the same interface as the "default route" is on. You can determine whic

It is also not uncommon to use an interface with no IP address configured in promiscuous m
should be inspected, enable promiscuous mode later on and make sure that the network traff
or to a tap).

You can configure multiple interfaces, just by adding more than one interface name separat

Interface(s) which Snort should listen on:

ens33
```

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



```
                     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
comma-separated (without spaces).

Please note that if Snort is configured to use multiple interfaces, it
will use this value as the HOME_NET definition for all of them.

Address range for the local network:

192.168.1.0/24_

                          <Ok>
```

- 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

- Now run given below command to enable IDS mode of snort . sudo snort -A console -i ens33 -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

cd /etc/snort/rules ls -la

- 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

- Sample Rule alert icmp any any -> 192.168.1.21 any (msg: "ICMP Packet found"; sid:10000001;)

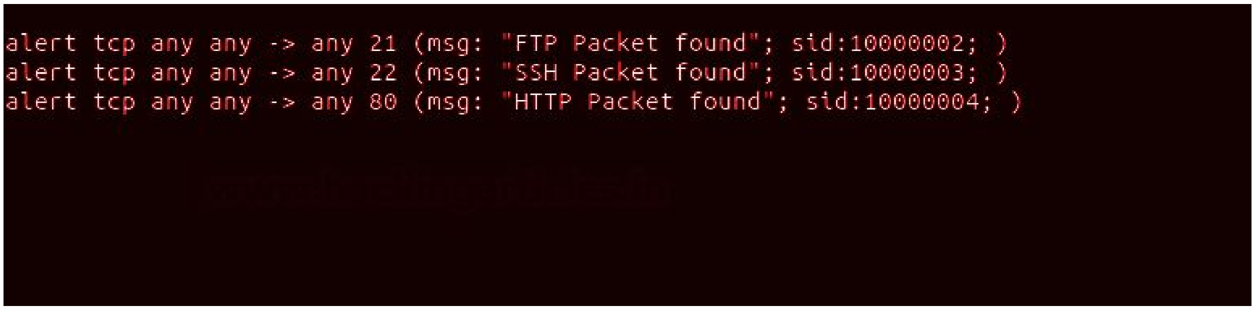
- On Intrusion snort will output

- 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: "SSH Packet found"; sid:10000003;)

alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000004;)



```
alert tcp any any -> any 21 (msg: "FTP Packet found"; sid:10000002; )
alert tcp any any -> any 22 (msg: "SSH Packet found"; sid:10000003; )
alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000004; )
```

Conclusion

Hence we studied the network intrusion detection system known as Snort and showed its demonstration.