Aim: Set up, configuration and use of SNORT for Intrusion Detection

Theory:
Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.
Snort can be configured to run in three modes:
1. Sniffer mode : It simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen)
2. Packet Logger mode : logs the packets to disk
3. Network Intrusion Detection System (NIDS) mode: it performs detection and analysis on network traffic. This is the most complex and configurable mode

Steps:
1. Get root access
$ sudo su root

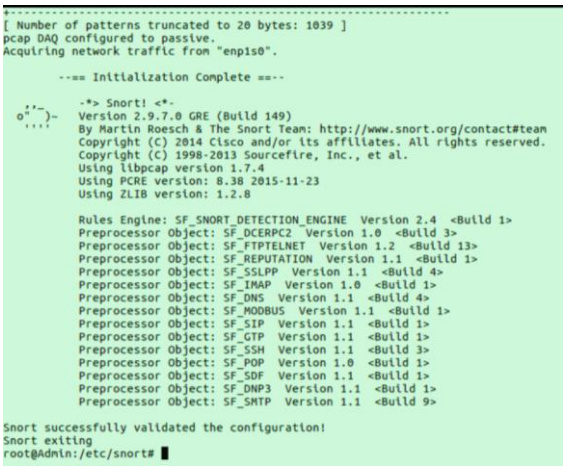
2. Do updation
apt-get update

3. Installation
apt-get install snort
During installation:

- Put the name of network interface (by default it is eth0, change it to the interface name of your machine)
- Put the IP address of the machine followed by /24 (by default it is the network address. Replace it with your IP addr/24)

4. Configuration
cd /etc
ls
cd /snort
ls
gedit snort.conf
Go to line no. 51
ipvar HOME_NET any
Replace “any” with your ip address i.e. ipvar HOME_NET 192.168.208.22
Save and close the file

5. Monitoring
snort –q –A console –i enp2s0
enp2s0 is the name of the interface



6. Perform the following nmap command on neighbour's machine and observe the output in your machine
$ nmap ip addr of your machine (This command is to be performed on neignbour's machine)
Output to be observed in SNORT terminal: IP address of the neighbour who is performing Intrusion i.e. Port Scanning