Name: Shaikh Amaan Shaikh Farooque PRN: 2019BTECS00076
Class: B.Tech CSE Batch: B3
CNS Lab (MKC) Assignment-15

---

Date: 30th Nov 2022 Page No. 1

---

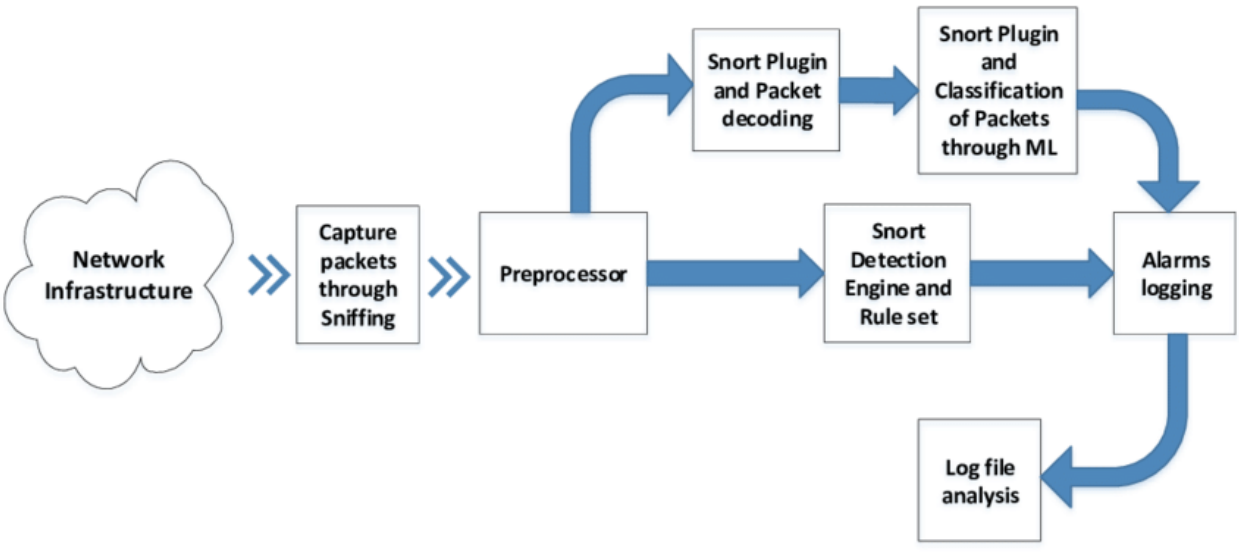
**Title:** Intrusion detection system- Snort

**Aim:** To install and configure snort IDS and check its working again ping attack

**Introduction:**

Snort is a free open source network intrusion detection system and intrusion prevention system created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013.

**Theory:**




If a subscriber configures Snort to operate as a sniffer, it will scan network packets and identify them. Snort can also log those packets to a disk file.

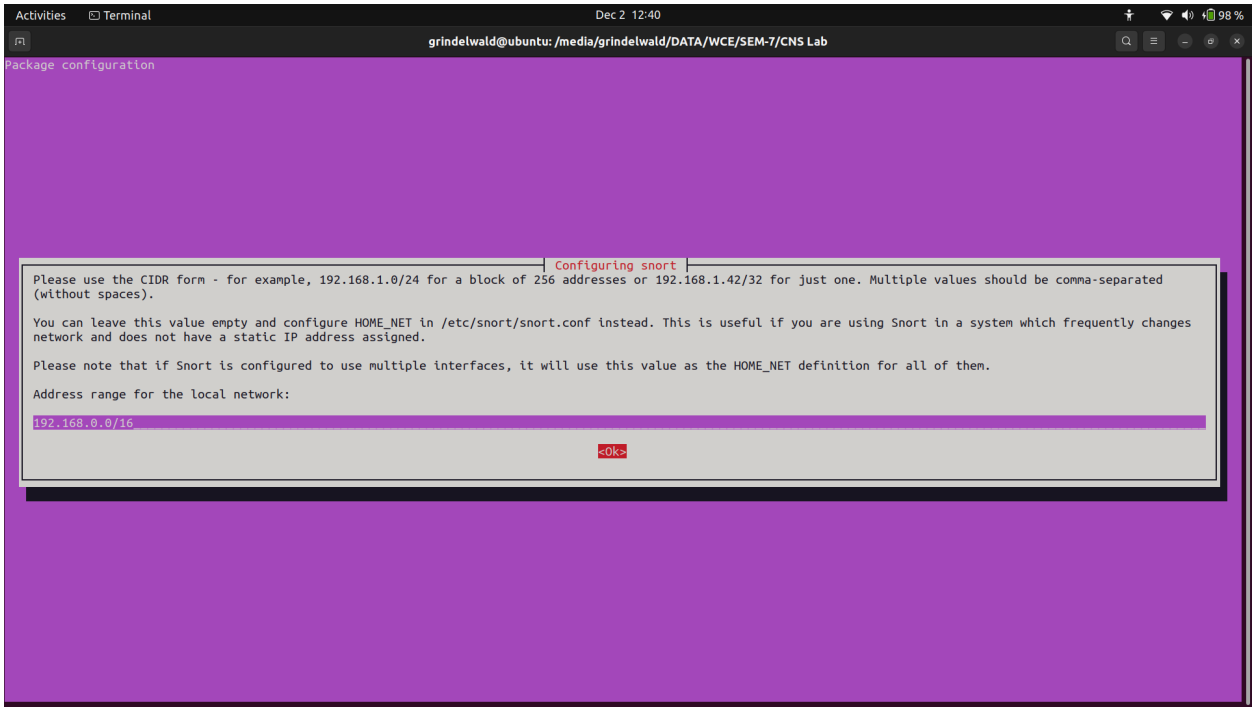
To use Snort as a packet sniffer, users set the host's network interface to promiscuous mode to monitor all network traffic on the local network interface. It then writes the monitored traffic to its console.

By writing desired network traffic to a disk file, Snort logs packets.

**Procedure:**

1. Installation:

```
sudo apt install snort
```




2. Service status

```
sudo systemctl status snort.service
```

```
grindelwald@ubuntu:/etc/snort/rules$ sudo systemctl status snort.service
● snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: active (running) since Fri 2022-12-02 14:59:38 IST; 26s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 23143 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
      Tasks: 6 (limit: 6884)
     Memory: 233.2M
        CPU: 1.001s
     CGroup: /system.slice/snort.service
             ├─23163 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -c /etc/snort/snort.conf -S "\"HOME_NET=[192.168.0.0/16]\"" -i
             ├─23178 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -c /etc/snort/snort.conf -S "\"HOME_NET=[192.168.0.0/16]\"" -i
             └─23192 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -c /etc/snort/snort.conf -S "\"HOME_NET=[192.168.0.0/16]\"" -i

Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Dec 02 14:59:38 ubuntu snort[23192]:           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
Dec 02 14:59:38 ubuntu snort[23192]: Commencing packet processing (pid=23192)
lines 1-23/23 (END)
```

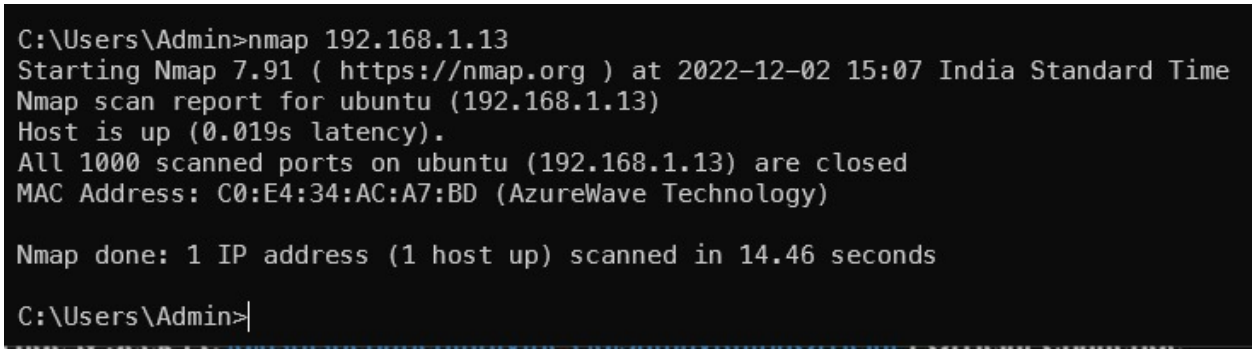
3. Device information

```
ifconfig
```

```
grindelwald@ubuntu:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:d5:5d:81:90  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether e8:d8:d1:57:20:e3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4722  bytes 502086 (502.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4722  bytes 502086 (502.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.13  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::6cd5:b1b7:aaf9:a9a9  prefixlen 64  scopeid 0x20<link>
        ether c0:e4:34:ac:a7:bd  txqueuelen 1000  (Ethernet)
        RX packets 227681  bytes 185392350 (185.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 130449  bytes 36364391 (36.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

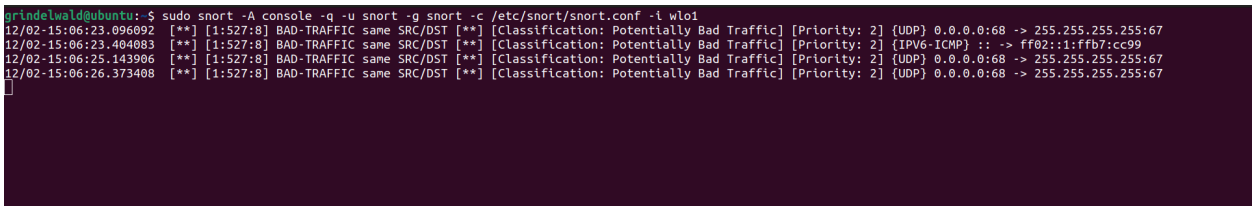
4. Ping from other device

```
ping 192.168.1.13
```




5. Starting snort to detect intrusion

```
sudo snort -A console -q -u snort -g snort -c
/etc/snort/snort.conf -i wlo1
```




**Conclusion:** Installed and configured snort successfully and detected potentially bad traffic.