IDS & IPS using Snort

Instructor

Dr. Debasis Das
Associate Professor, CSE
IIT Jodhpur

Co-taught by

Ayanabha Ghosh
PhD candidate, IIT Jodhpur

Introduction

IDS: Intrusion Detection System

- Monitors network or system activity for malicious behavior or policy violations.
- Detects attacks such as port scanning, brute-force attempts, malware communication, etc.

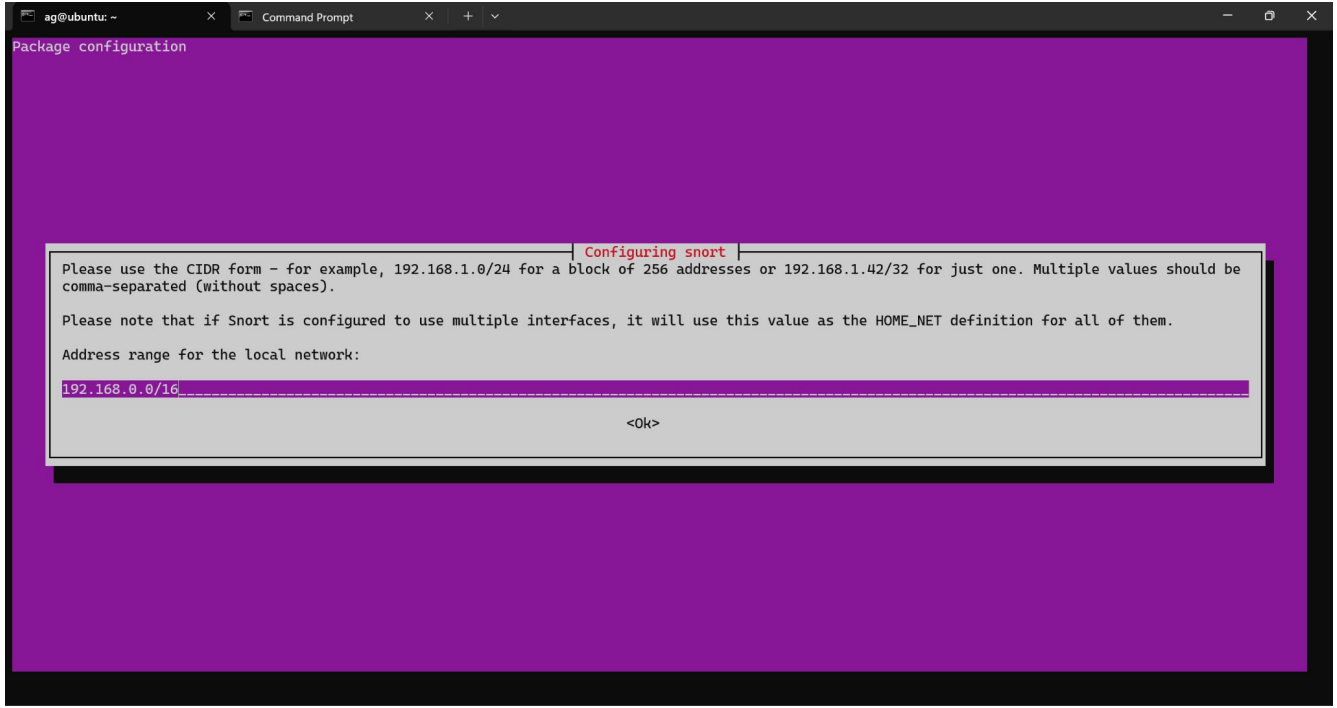
IPS: Intrusion Prevention System

Snort

- An open-source network-based IDS/IPS.
- **IDS Mode** – Detects and alerts on suspicious traffic.
- **IPS Mode** – Detects and actively blocks suspicious traffic (with iptables + NFQUEUE integration).

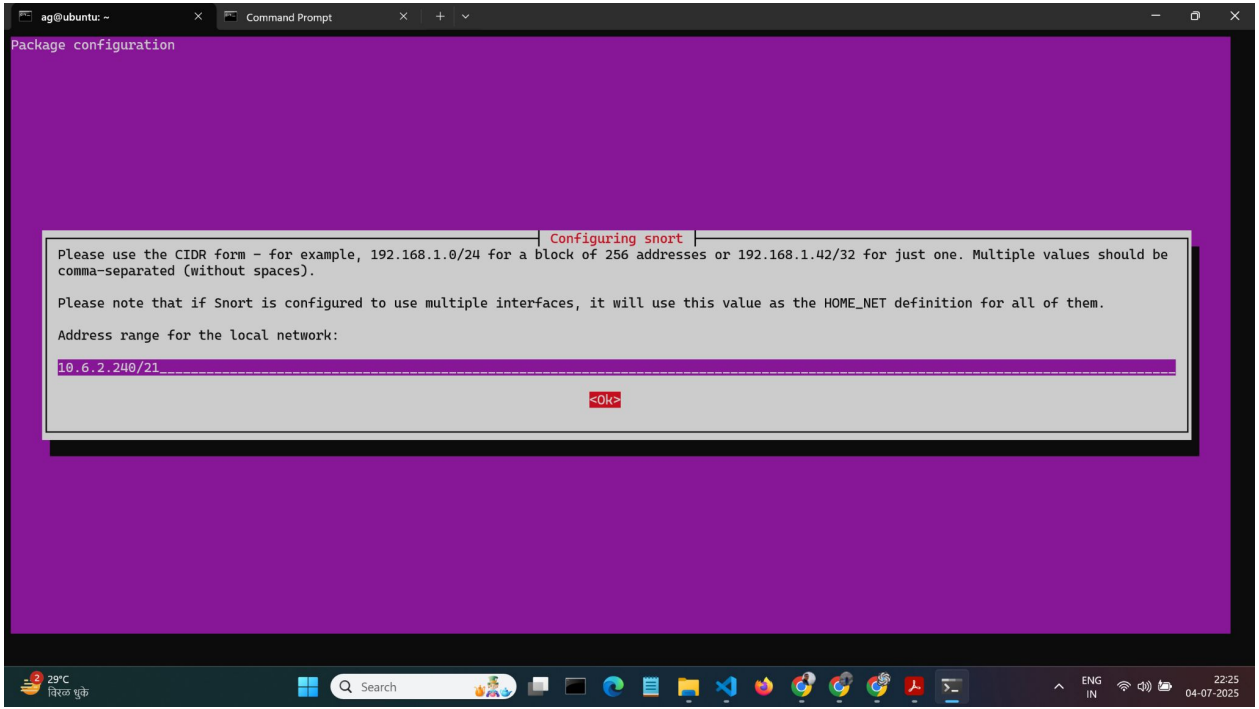
Snort Installation

sudo apt install snort -y



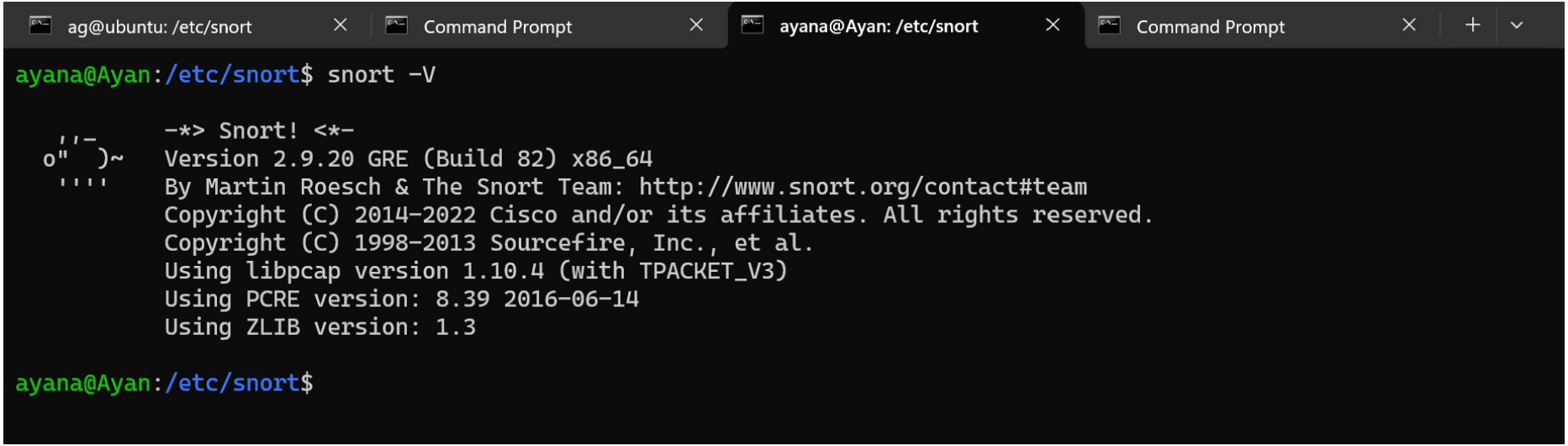
Snort Installation

Setting up with IP (ip a) of device



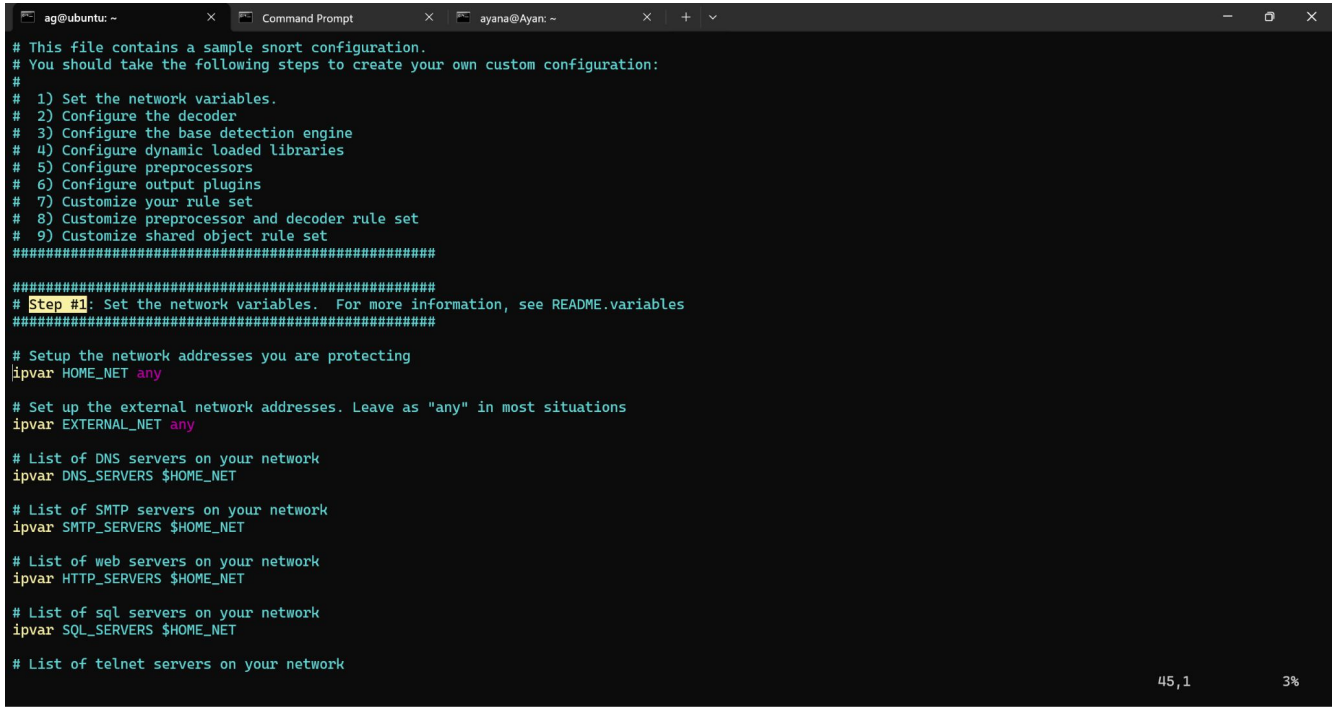
Snort Installation

Verify installation: snort -V



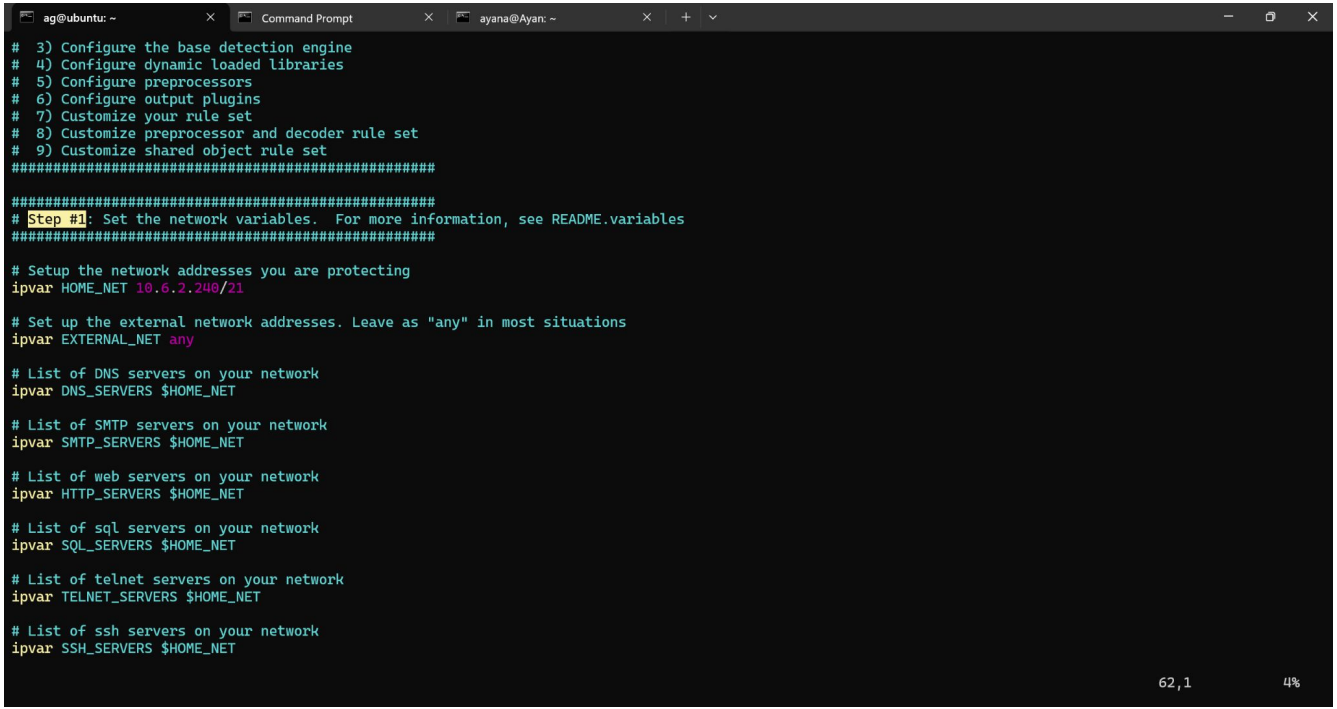
Snort setup .conf file

sudo vim /etc/snort/snort.conf



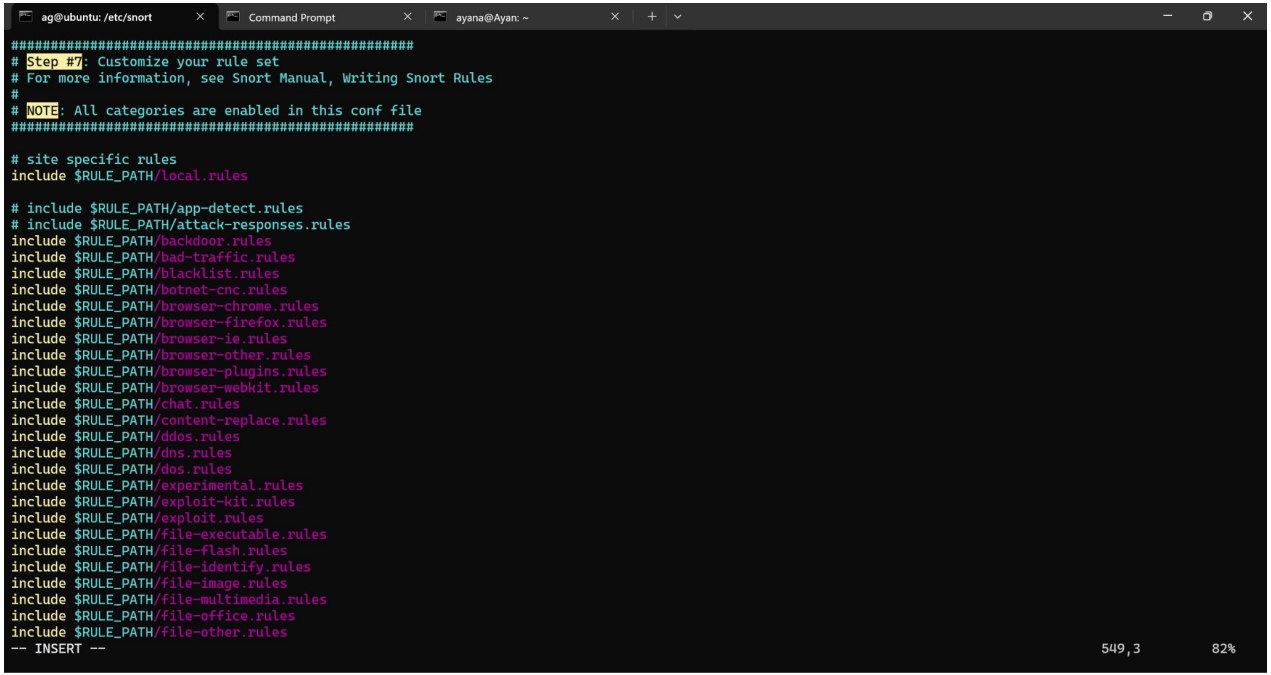
Snort setup .conf file

Change to the HOME_NET IP



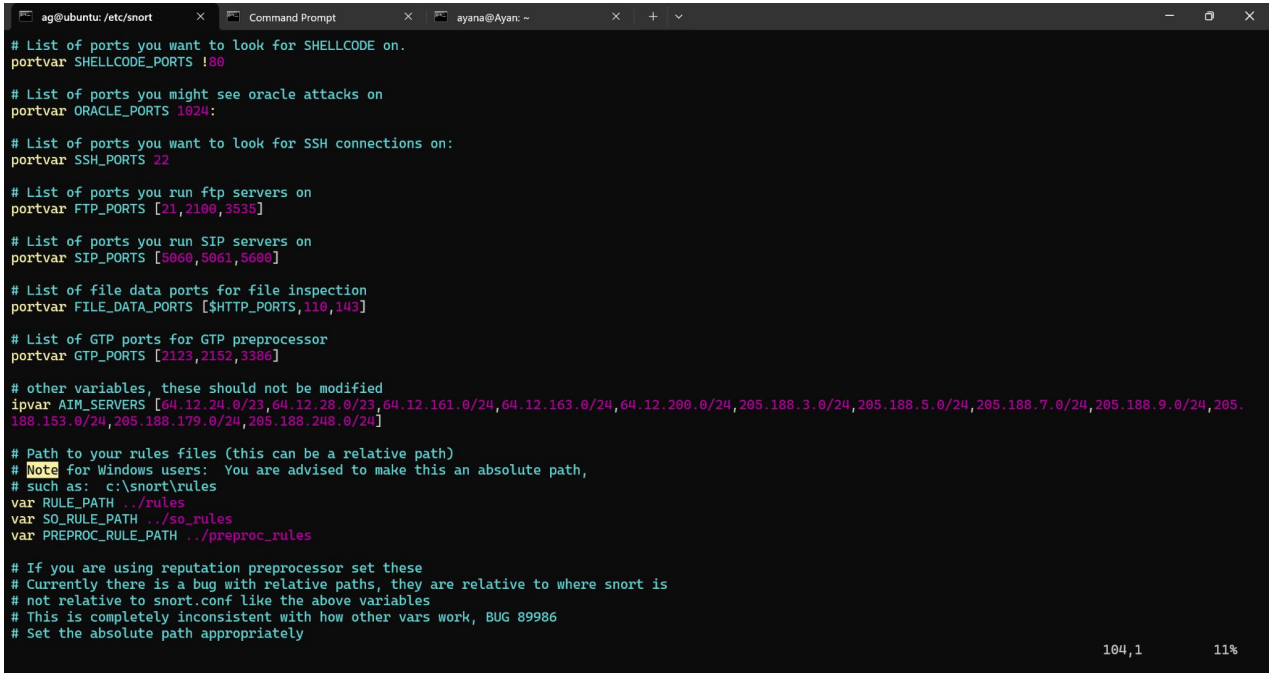
Snort setup .conf file

Comment out all ‘include $RULE_PATH…’ if not done
Keep the ‘include $RULE_PATH/local.rules’



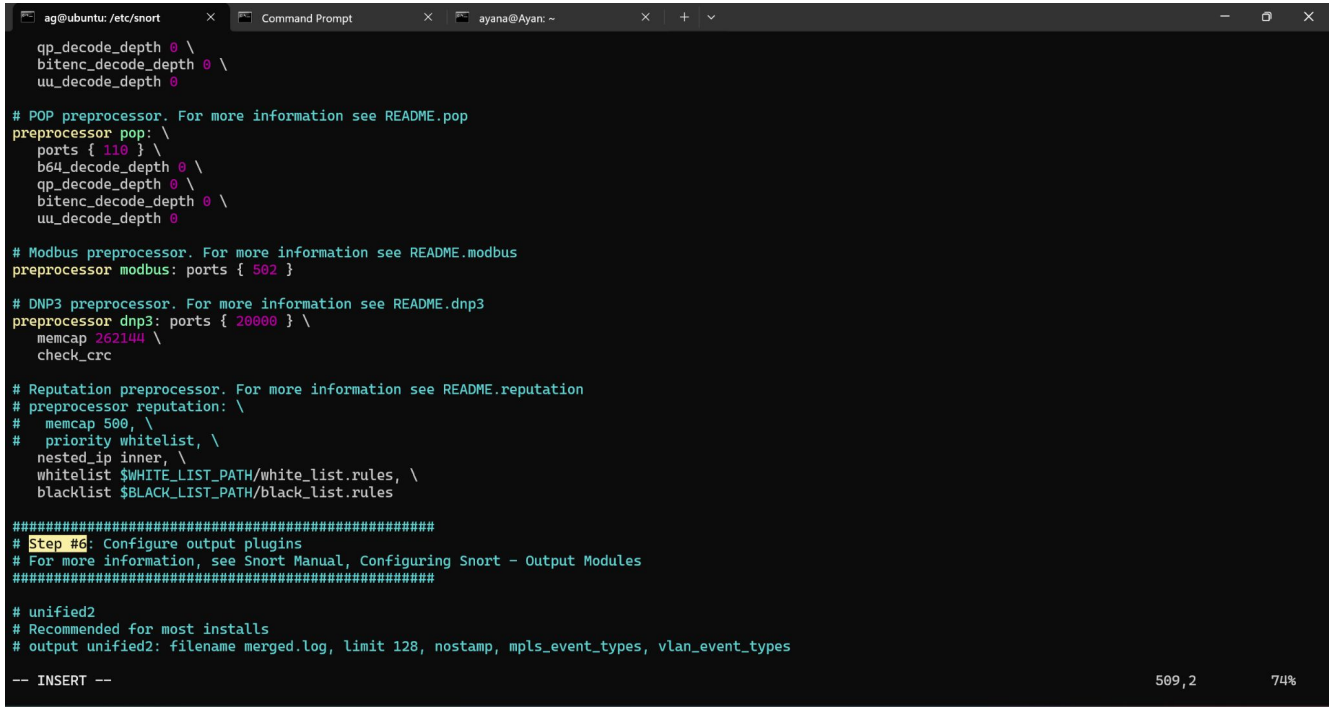
Snort setup .conf file

Change the ‘var RULE_PATH’ to ‘/etc/snort/rules’ if not done



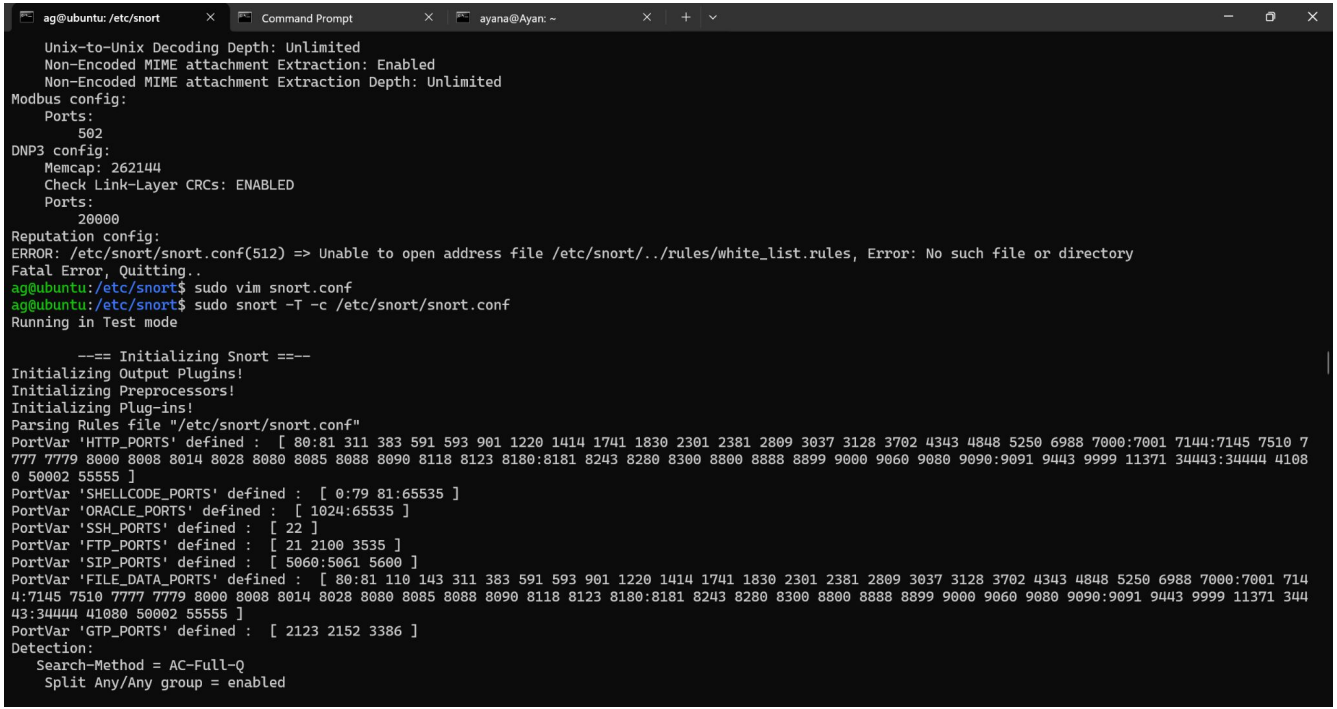
Snort setup .conf file

Comment out the $WHITE_LIST… and $BLACK_LIST… paths block



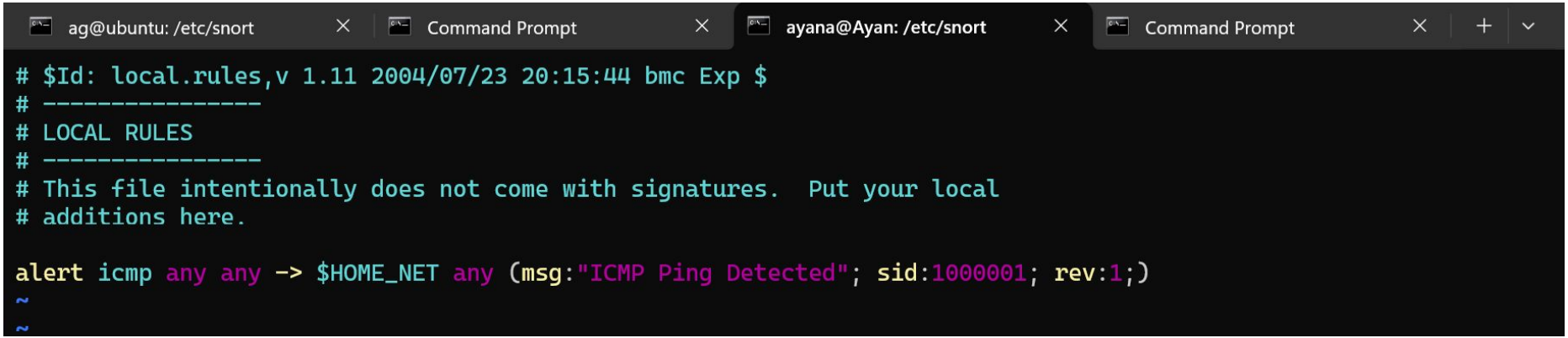
Verify .conf file

sudo snort -T -c /etc/snort/snort.conf



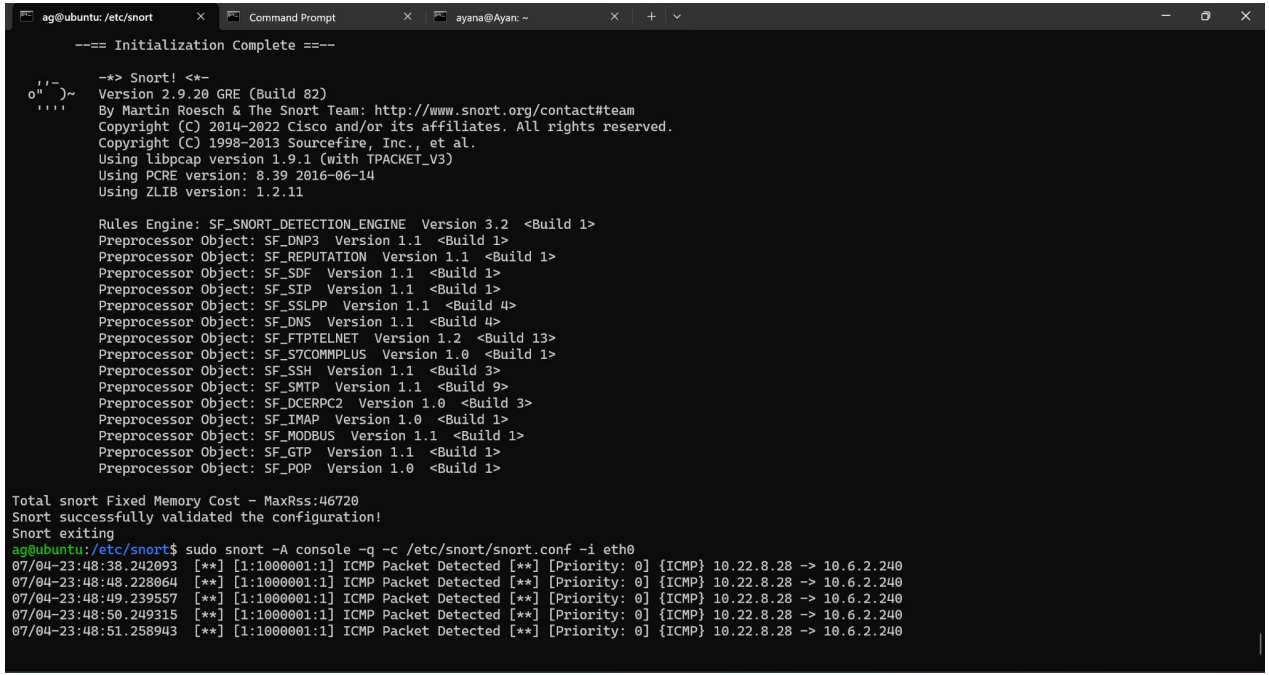
IDS : Custom ICMP rule

sudo vim /etc/snort/rules/local.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;)



IDS : Ping

sudo snort -A console -q -c /etc/snort/snort.conf -i <interface>
In my case: <interface> = eth0 (obtained from ‘ip a’)



IDS : Ping

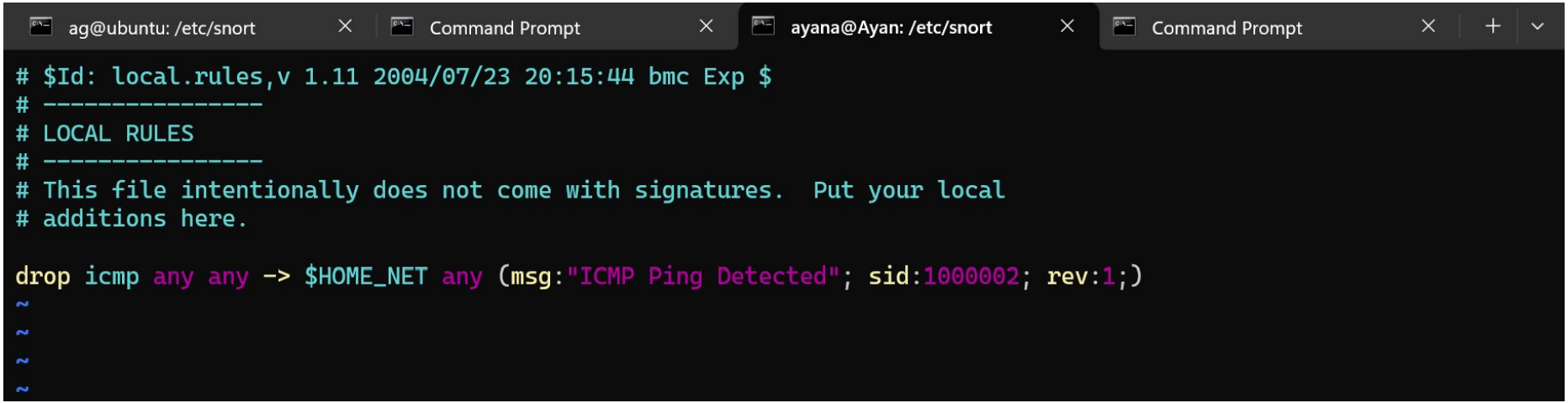
Log file
sudo snort -A **fast** -q -c /etc/snort/snort.conf -i eth0

sudo cat /var/log/snort/alert

```
ayana@Ayan:/etc/snort$ sudo vim ./rules/local.rules
ayana@Ayan:/etc/snort$ sudo snort -A fast -q -c /etc/snort/snort.conf -i eth0
^Z
[2]+  Stopped                 sudo snort -A fast -q -c /etc/snort/snort.conf -i eth0
ayana@Ayan:/etc/snort$ sudo cat /var/log/snort/alert
07/04-19:14:51.353792  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:14:56.176277  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:15:01.183762  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
07/04-19:15:06.186023  [**] [1:1000001:1] ICMP Ping Detected [**] [Priority: 0] {ICMP} 172.30.48.1 -> 172.30.62.123
ayana@Ayan:/etc/snort$
```

IPS : rule

drop icmp any any -> $HOME_NET any (msg:"ICMP Ping Dropped"; sid:1000002; rev:1;)



IPS : Traffic through Snort

sudo apt install libnetfilter-queue-dev -y (dependency)
sudo snort -Q --daq nfq -c /etc/snort/snort.conf

sudo iptables -I INPUT -j NFQUEUE
sudo iptables -I FORWARD -j NFQUEUE
This sends all incoming and forwarded traffic through Snort.

IPS : Ping blocked

Pings are blocked

```
C:\Users\ayana>ping 172.30.62.123 -n 4

Pinging 172.30.62.123 with 32 bytes of data:
Reply from 172.30.62.123: bytes=32 time<1ms TTL=64
Reply from 172.30.62.123: bytes=32 time<1ms TTL=64
Reply from 172.30.62.123: bytes=32 time<1ms TTL=64
Reply from 172.30.62.123: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.62.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ayana>ping 172.30.62.123 -n 4

Pinging 172.30.62.123 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.30.62.123:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Thank you


भारतीय प्रौद्योगिकी संस्थान जोधपुर
Indian Institute of Technology Jodhpur