**CS Assignment : IDS**

**Name : Sumitra Kamble**

**MIS : 112103066**

**Div: 1**

**Batch: CS-2**

**Objective**

The purpose of this assignment is to gain hands-on experience with an Intrusion Detection System (IDS). This involves installing and configuring an IDS, studying its functionality, and observing how it monitors network activities. The assignment helps in understanding how suspicious traffic is detected, logged, and reported based on defined rules.

**Introduction to Snort**

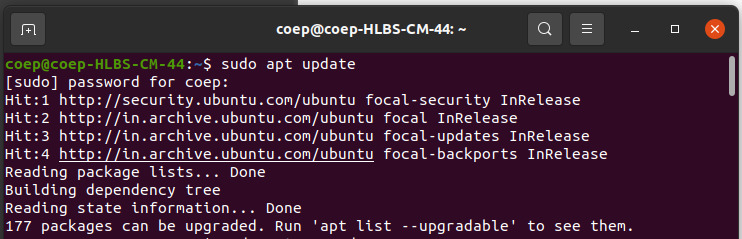
Snort is one of the most popular and widely used open-source IDS/IPS tools. It operates in real-time to analyze packet data, detect suspicious traffic patterns, and log malicious activities. Its flexibility allows users to write custom rules to detect specific attacks or behaviors.

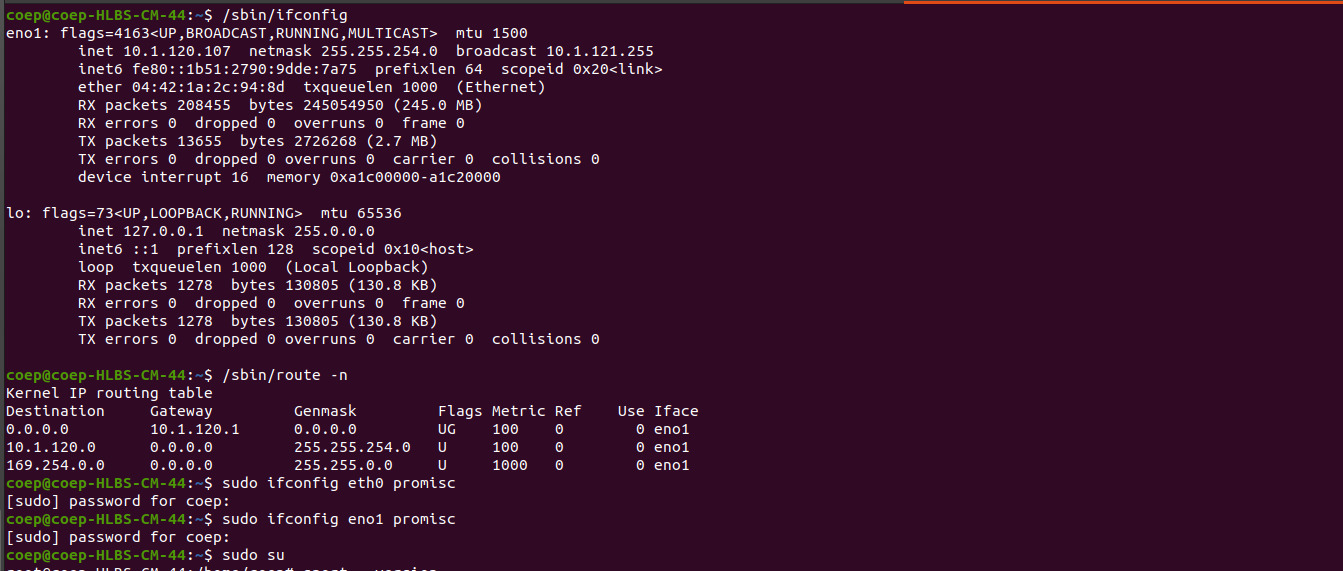
Snort supports three operational modes:

* **Packet Sniffing Mode:** Passively captures and displays traffic.
* **Packet Logging Mode:** Logs packets to disk for further analysis.
* **Intrusion Detection Mode:** Uses rules to detect malicious activities and generates alerts.

**Implementation Steps**

1. **Installing Snort**



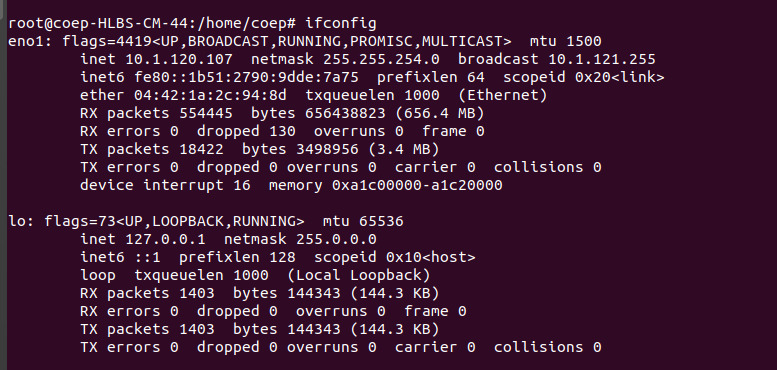


1. **Confirm Installation**



**3. Identifying Network Interfaces**

* ifconfig command to view all active network interfaces:

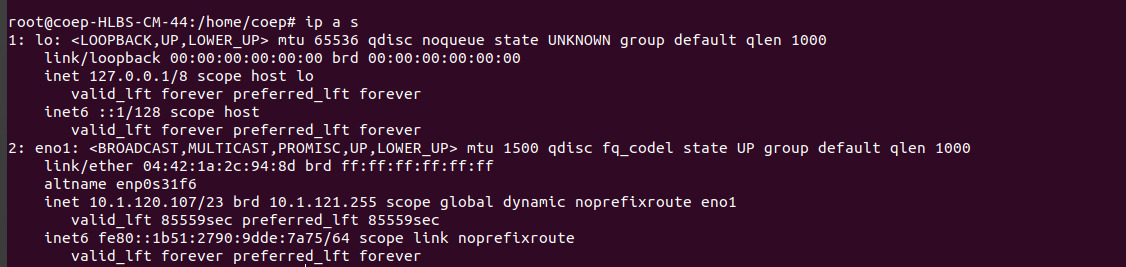


* Identify the interface to be monitored. For this setup, we will use enp0s8.

**4. Determining the Interface IP**

* To get the IP address of the chosen interface, run:

ip a s



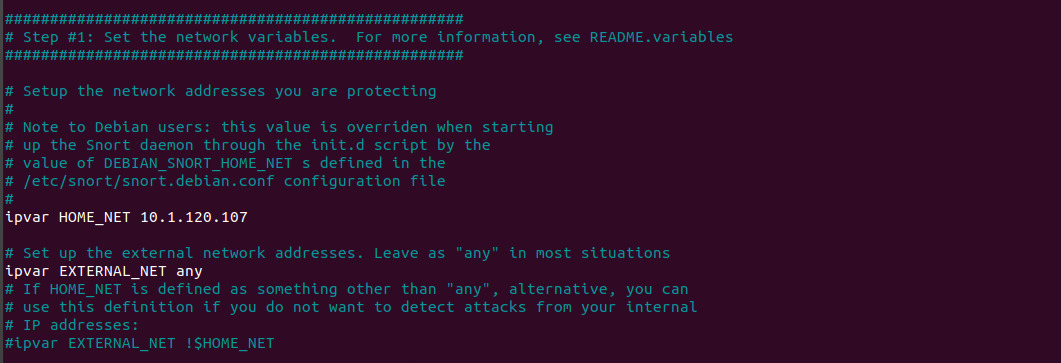
**5. Configuring HOME\_NET**

* Open Snort’s configuration file to set the network IP range:

sudo nano /etc/snort/snort.conf

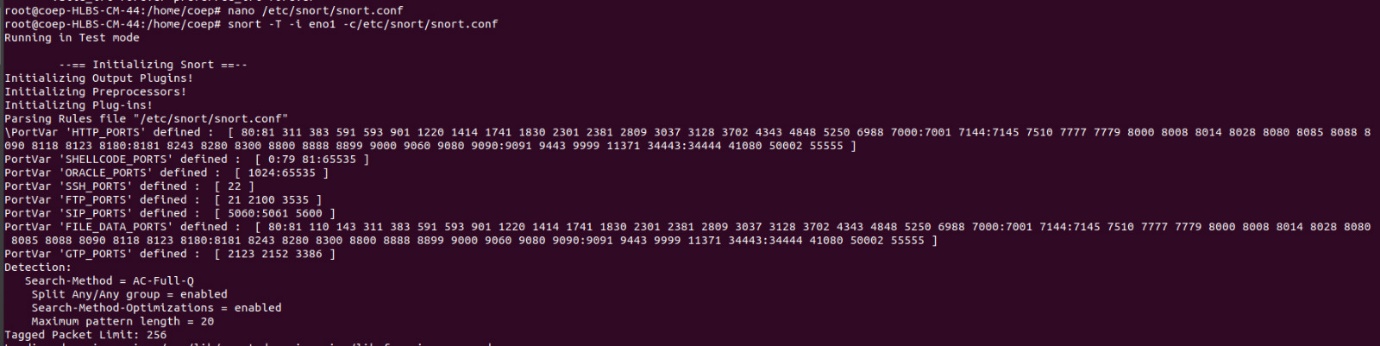
* Locate the line:

ipvar HOME\_NET



**6. Testing Configuration**

sudo snort -T -i eno1 -c /etc/snort/snort.conf



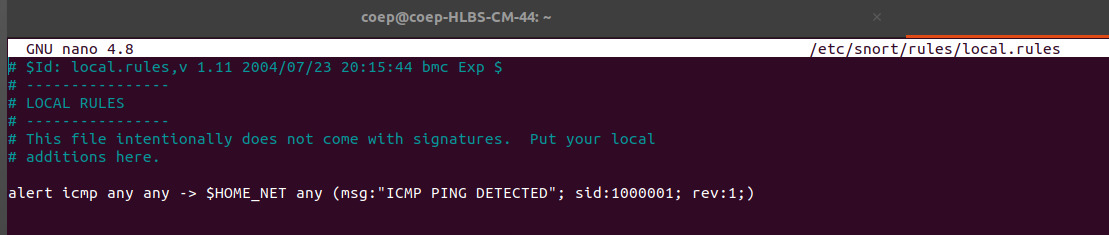
* This command tests the file without running Snort. If the output confirms no errors, the configuration is valid.

**7. Creating a Custom Rule**

sudo nano /etc/snort/rules/local.rules

* Add the following rule to detect ICMP ping requests:

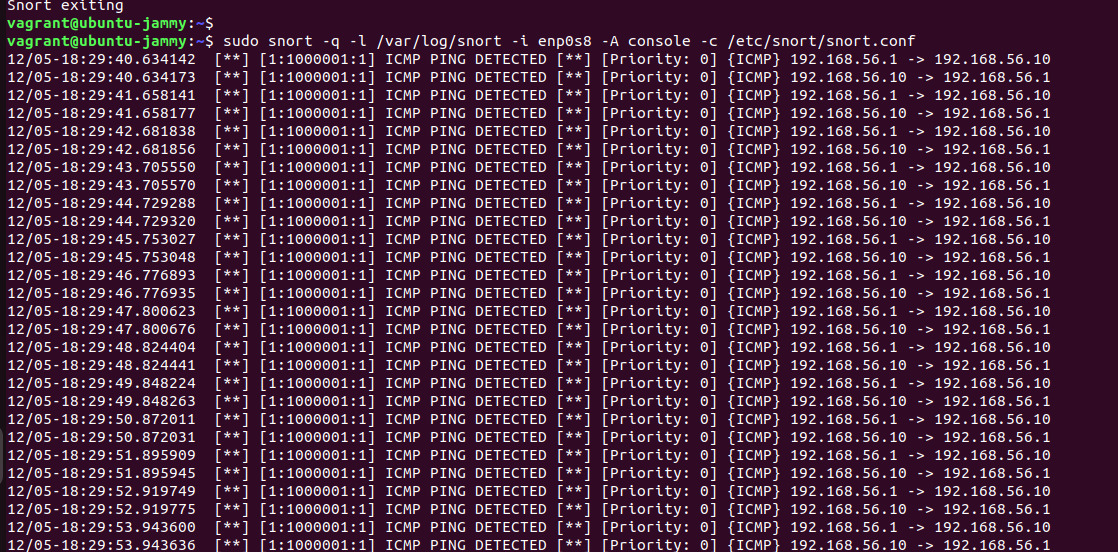
alert icmp any any -> $HOME\_NET any (msg:"Ping Detected"; sid:1000001; rev:1;)



1. alert: Specifies the action to take when the rule is triggered.
2. icmp: Monitors ICMP traffic (commonly used for ping).
3. any any -> $HOME\_NET any: Captures traffic from any source to the defined network.
4. msg: Displays a custom message in the alert.
5. sid: Unique identifier for the rule.
6. rev: Rule version number.

**8. Running Snort in Monitoring Mode**

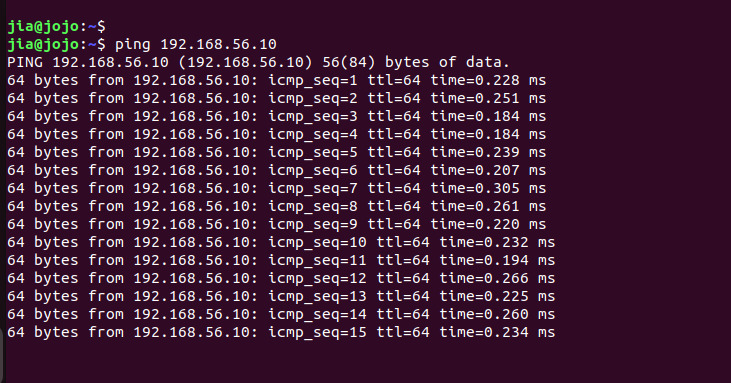
sudo snort -q -i eno1 -A console -l /var/log/snort -c /etc/snort/snort.conf



* Key options:
  + -q: Suppresses startup messages.
  + -i enpo1: Specifies the network interface.
  + -A console: Outputs alerts directly to the terminal.
  + -l /var/log/snort: Specifies the directory for log files.

**9. Testing the Rule**

ping 192.168.56.10



* The alert will also be logged in the directory /var/log/snort.

**Conclusion**

This assignment provided practical insights into installing and configuring Snort as an IDS. By creating a custom rule and monitoring ICMP traffic, we observed how Snort detects and logs network activity. With its extensive capabilities, Snort is a valuable tool for safeguarding networks against malicious activities.