Veermata Jijabai Technological Institute, Mumbai 400019

Experiment No.: 05

Aim: Install SNORT, an open-source tool and implement IDS to detect attacks in the network.

Name: Kiran K Patil

Enrolment No.: 211070904

Branch: Computer Engineering

Batch: D

Theory:

The primary objective of this experiment is to establish an Intrusion Detection System (IDS) using SNORT, an open-source and widely-used tool for network security. The experiment involves the creation of a controlled network environment, simulating network attacks, and monitoring these attacks using SNORT. Here are additional details:

1. SNORT:

Purpose: SNORT is an open-source network intrusion detection and prevention system. It's designed to monitor network traffic and detect suspicious or malicious activity.

Features:

- Packet inspection: SNORT inspects network packets for patterns that match predefined rules.
- Alerting: When a rule is triggered, SNORT generates alerts and logs information about the detected activity.
- Rule-based: SNORT uses a rule-based language to specify what to look for and how to respond.
- Customizable: You can create custom rules to tailor SNORT to your network's specific needs.

Installation:

- SNORT can be installed on various Linux distributions. You can use package managers like apt for Debian-based systems or compile it from source.

2. Kali Linux:

Purpose:

- Kali Linux is a popular penetration testing and ethical hacking distribution. In this experiment, it will serve as the attacker machine.

Features:

- Pre-installed hacking tools: Kali Linux comes with a wide range of pre-installed security and hacking tools.
- Customizable: You can add or remove tools as needed for your security assessments.

Installation:

- Kali Linux can be downloaded and installed on a dedicated machine or run from a live USB.

3. **Packet Crafting Tools:**

Purpose:

- To simulate attacks, you may need packet crafting tools to generate malicious packets with specific characteristics.

Examples:

- **Scapy**: A powerful packet manipulation tool that allows you to create, send, and capture network packets.
- **Nmap**: A network scanning tool that can be used to simulate port scans and other network reconnaissance activities.
- **Hping**: A command-line tool for crafting and sending custom packets.

Installation:

- These tools can be installed on Kali Linux using package managers or by compiling from source.

4. **Configuration Files:**

- **SNORT Rules:**

  SNORT uses rules to specify what to look for and how to respond to network activity. These rules are defined in .rules files and typically located in the SNORT configuration directory.

- **SNORT Configuration:**

  The SNORT configuration file (usually snort.conf) specifies various settings, including which network interfaces to monitor and where to log alerts.

5. **Log Files:**

- **SNORT Logs:**

  SNORT generates log files that contain information about detected network activity. Common log locations include /var/log/snort/ or a directory specified in the SNORT configuration.

6. **Documentation and Screenshots:**

- **Purpose:**

  To document the experiment, you'll need to capture and annotate screenshots of key steps and results.

- **Tools:**

  You can use built-in screenshot utilities on your operating system or third-party tools like Greenshot, Shutter, or Flameshot to capture and annotate screenshots.

7. **Network Environment:**

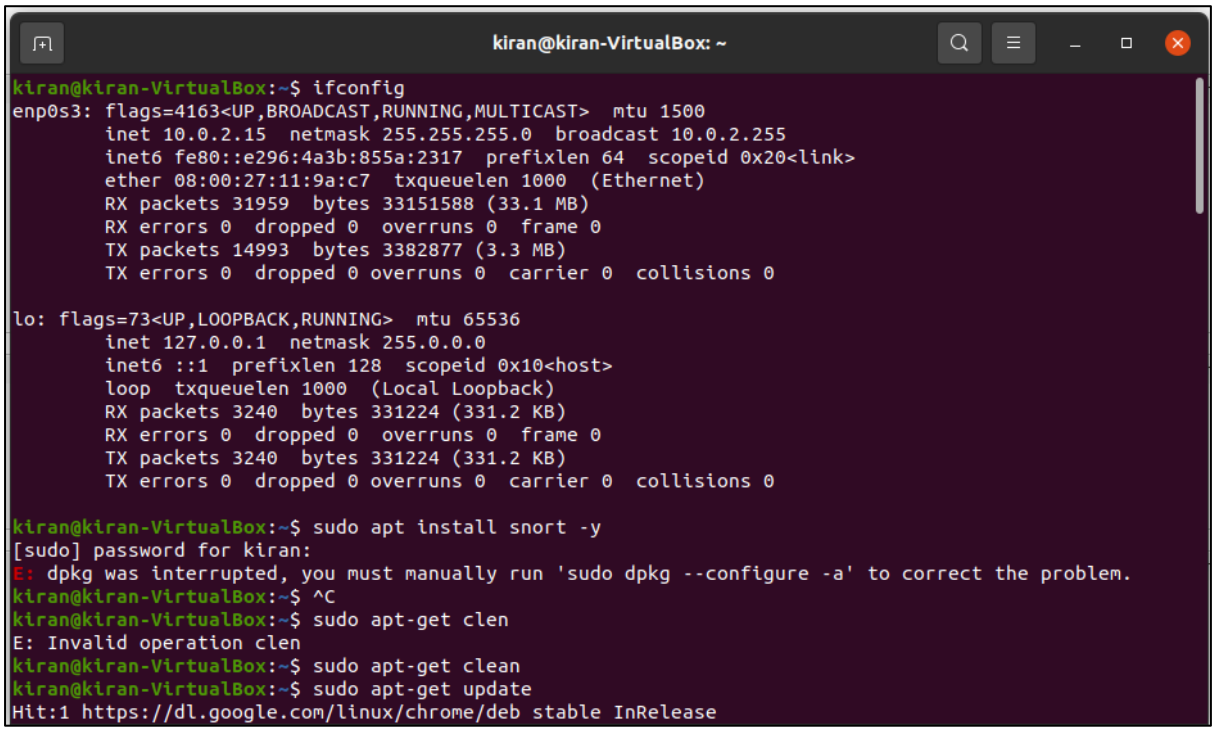
- **Isolation**:

  It's crucial to conduct this experiment in an isolated and controlled network environment to prevent any unintended consequences on a live network.

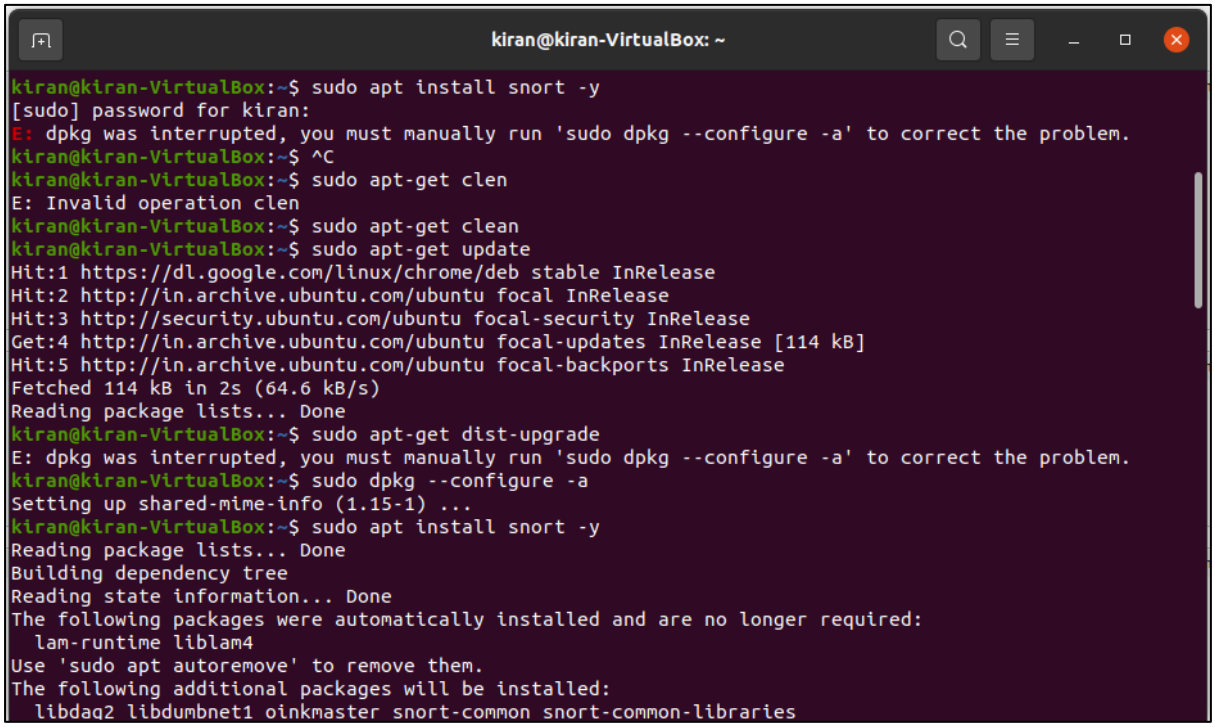
Remember that conducting network attack simulations and using tools like SNORT should be done ethically and legally, with proper authorization and consent. Unauthorized or malicious activities are illegal and unethical. Always use these tools responsibly and for legitimate security testing or research purposes.

Implementation:

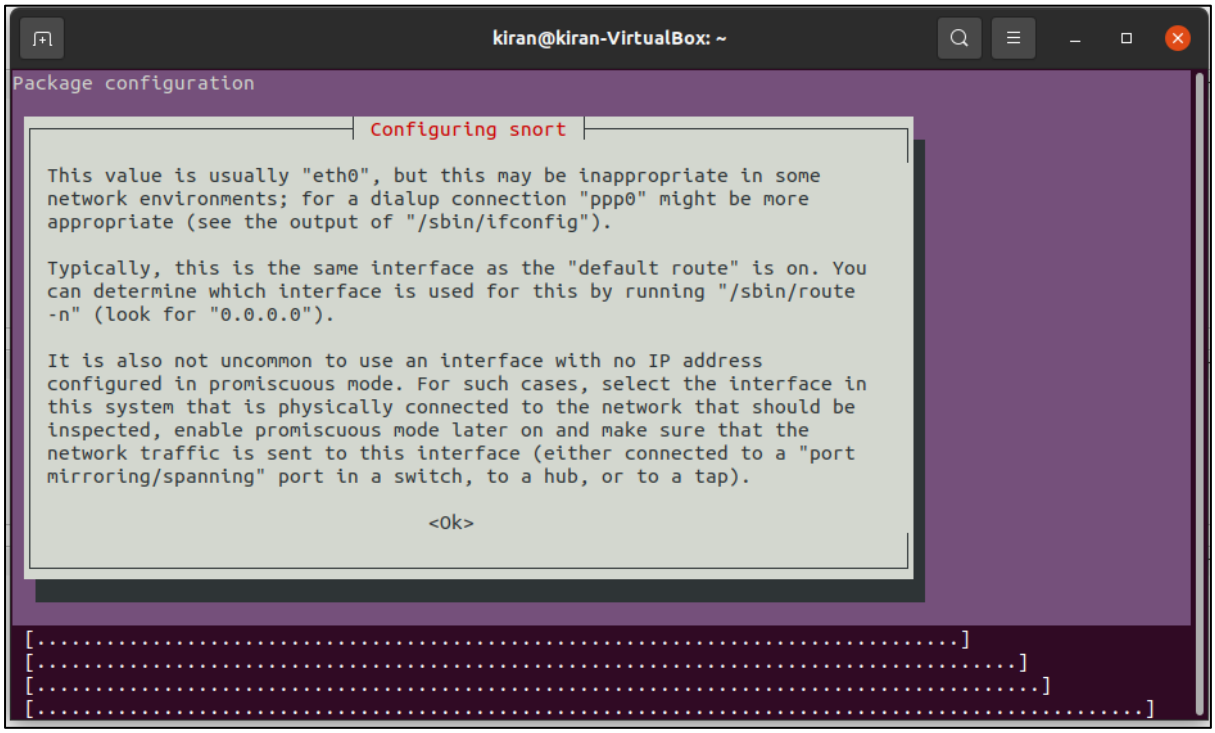
Ifconfig : to know your ip address



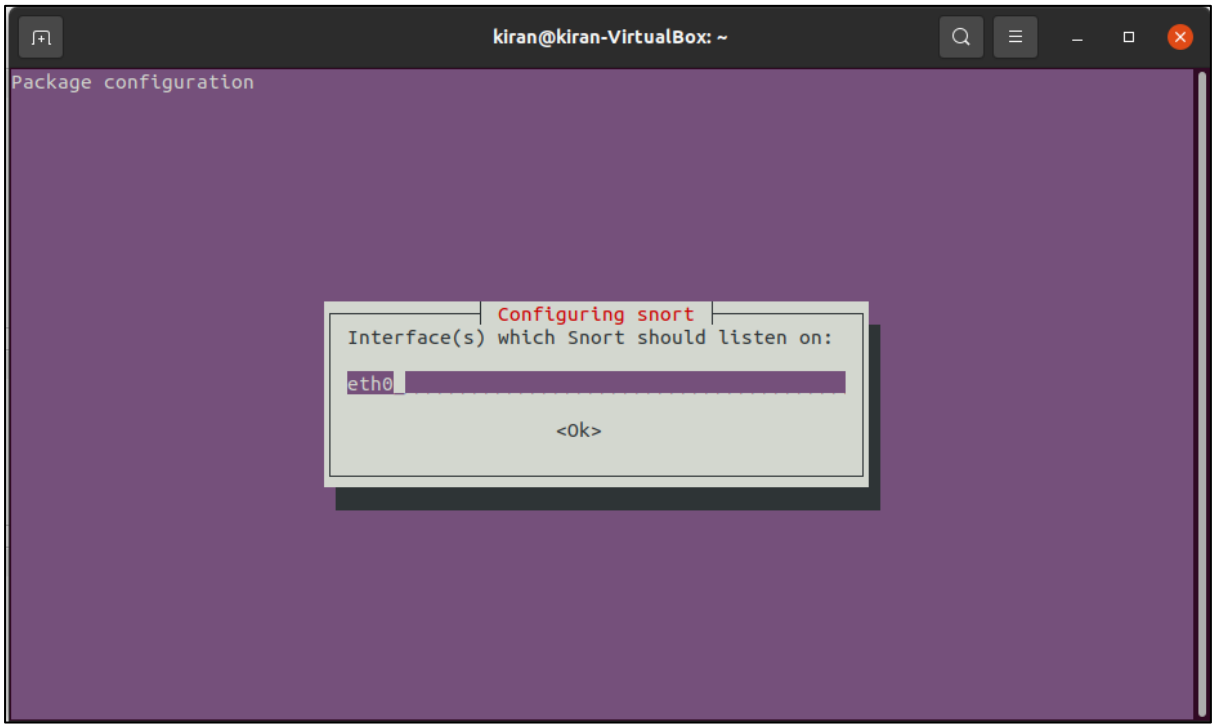
Install snort :
sudo apt install snort -y

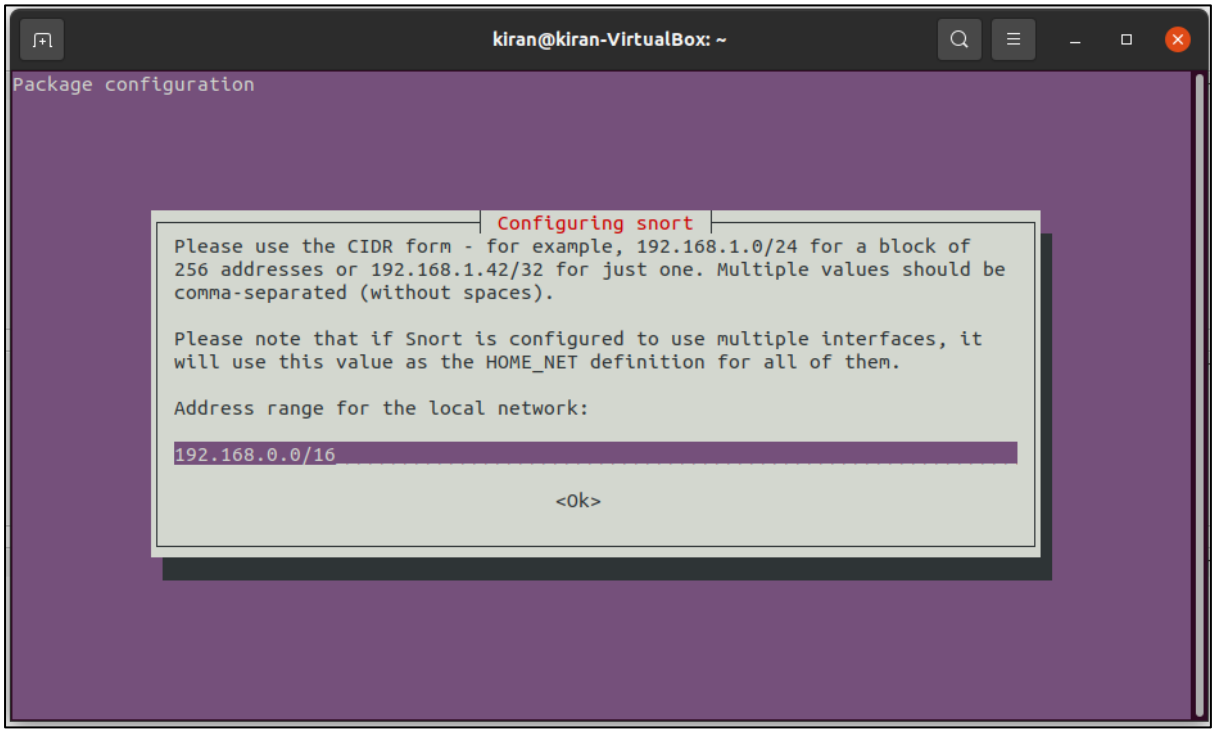


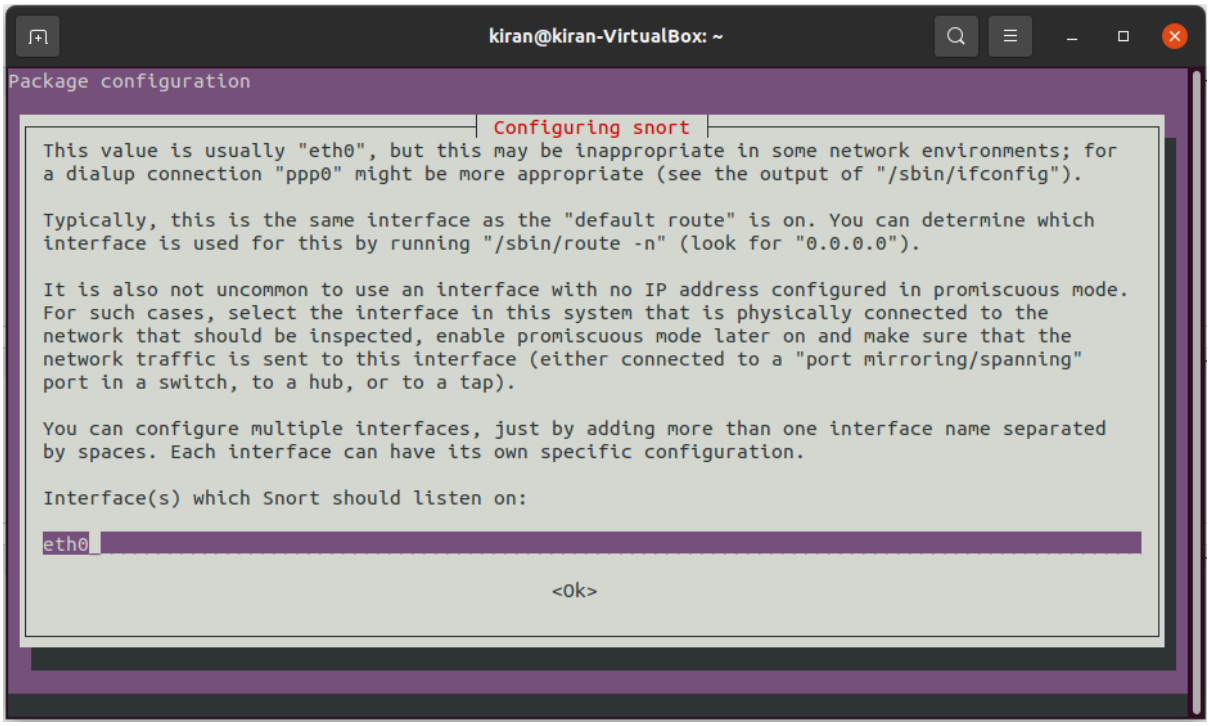
Configure the snort



Set the interface the default interface is set to eth0



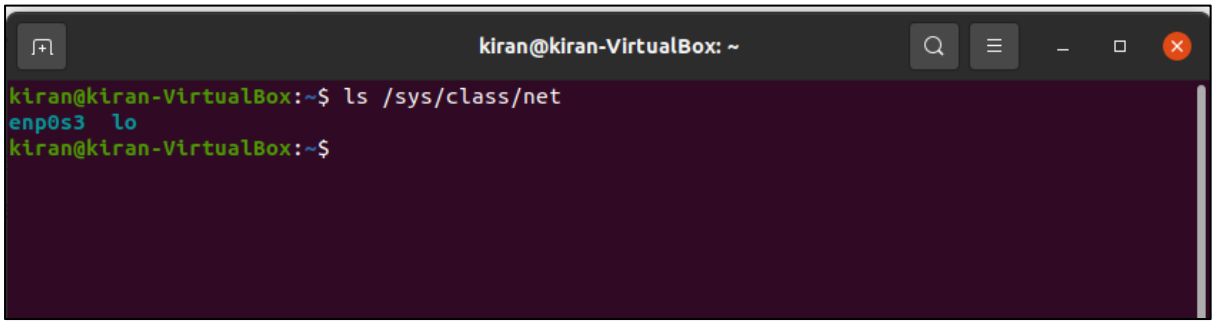




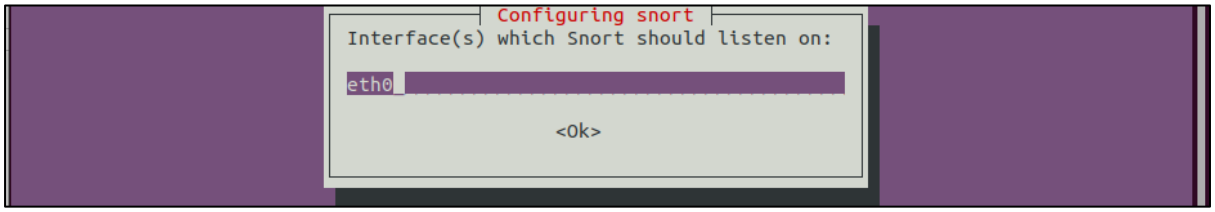
Here the eth0 interface is an invalid interface

Get interface :

ls /sys/class/net

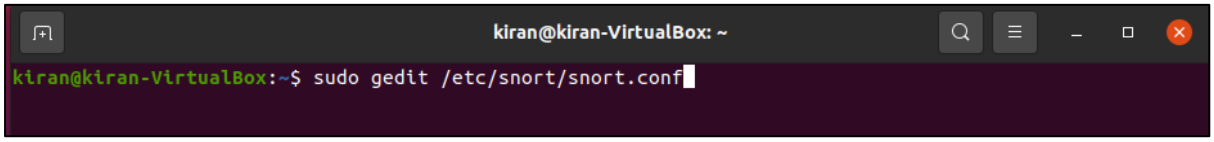


Then configure the snort with enp0s3 interface by changing it from eth0 to enp0s3

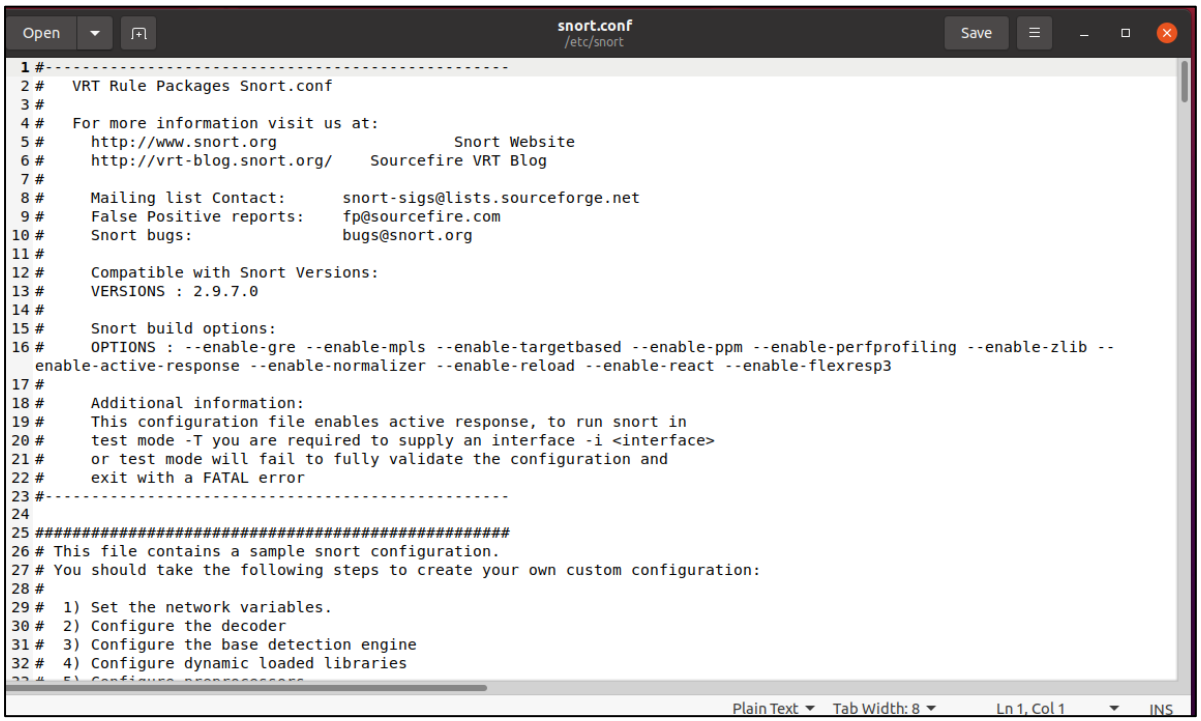


Now check the snot configuration file

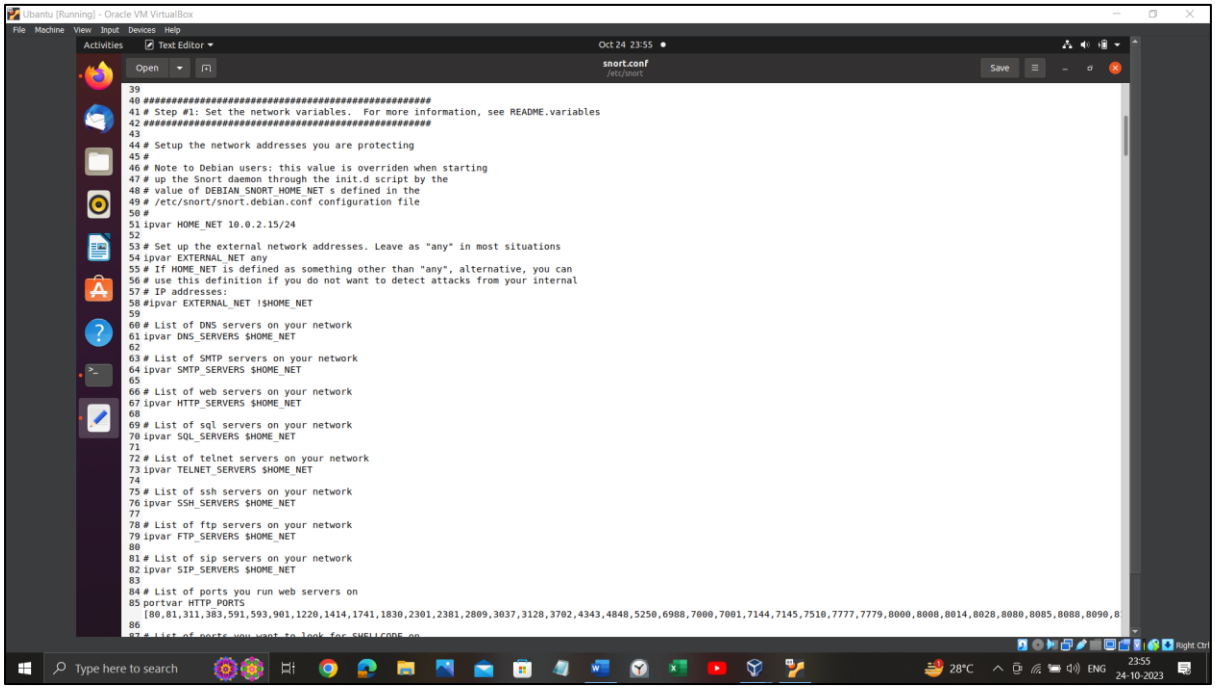
Sudo gedit /etc/snort/snort.conf



Snort.conf file

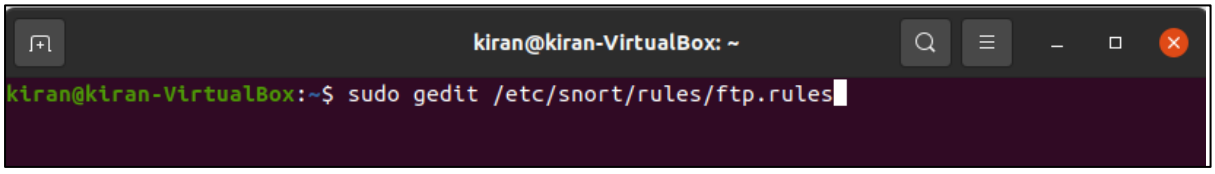


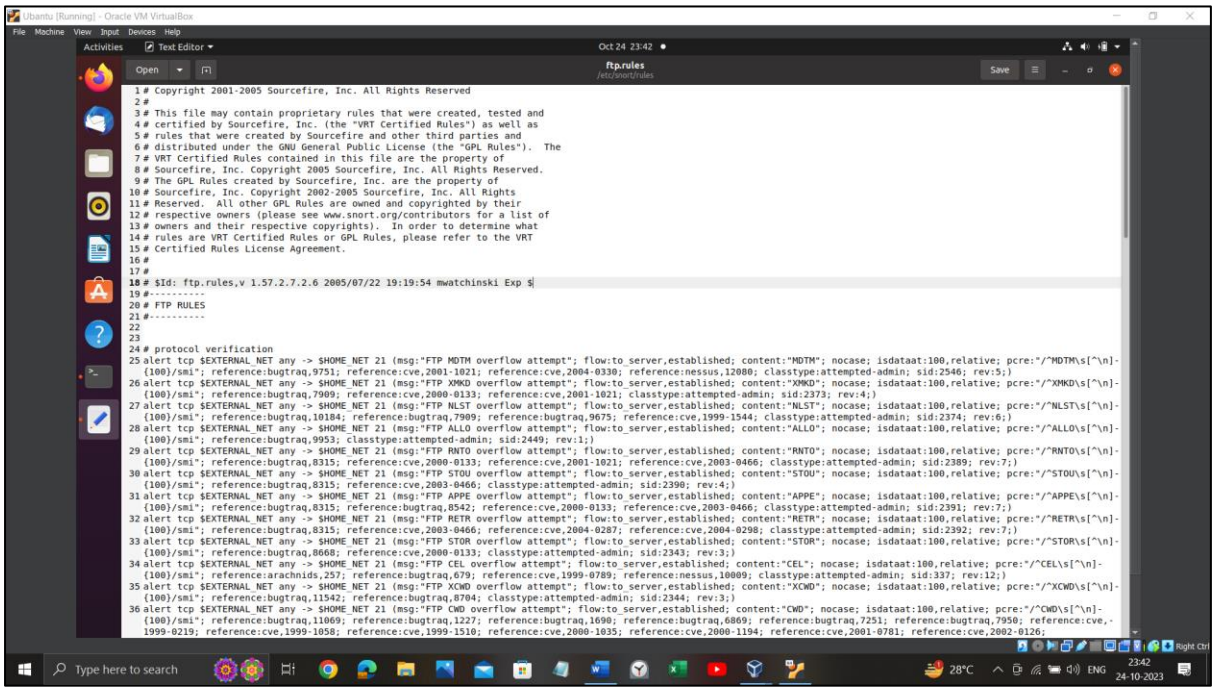
Chamge the ip address



Rules files

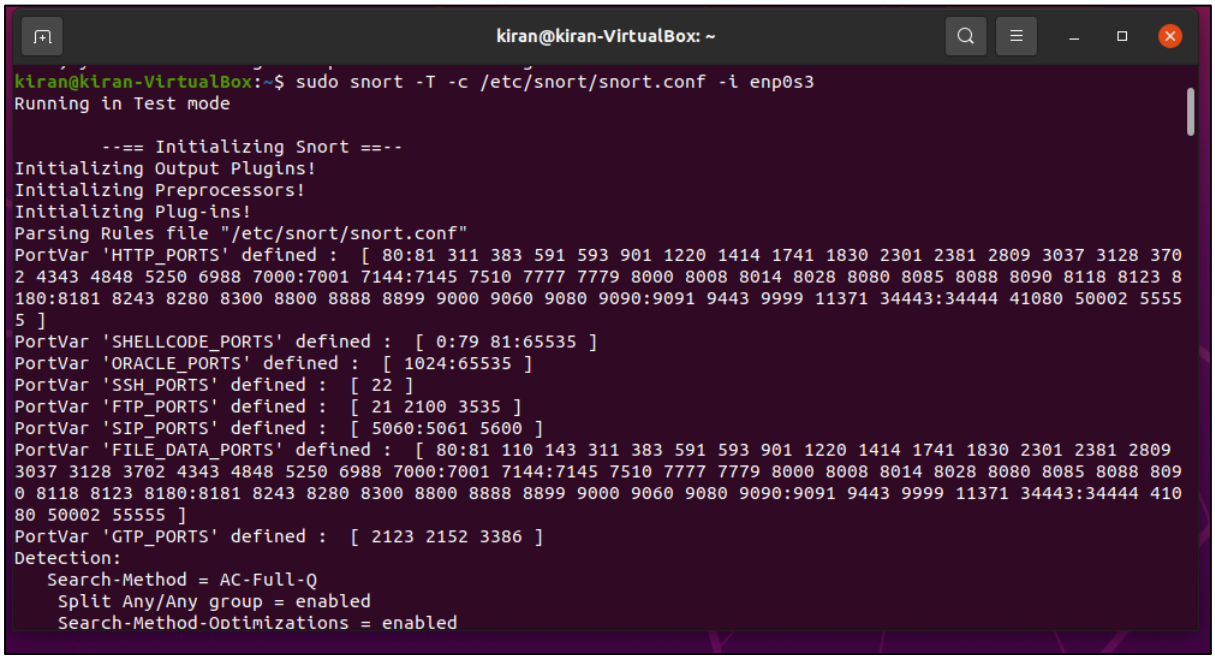
Sudo gedit /etc/snort/rules/ftp.rules file

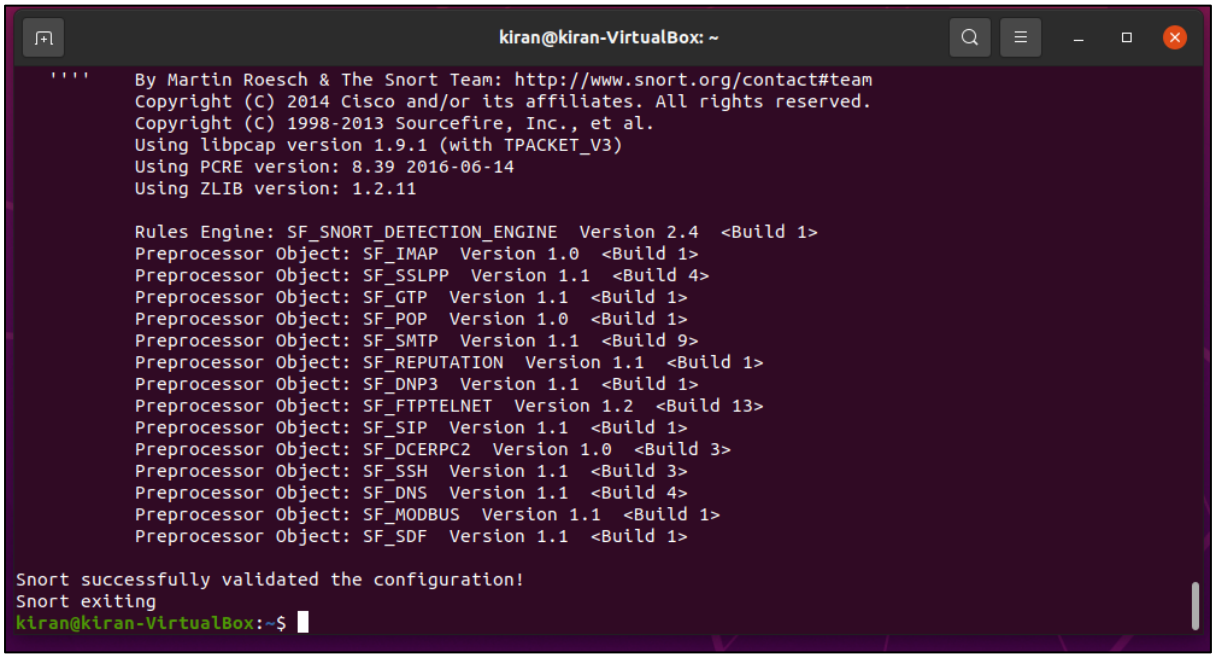




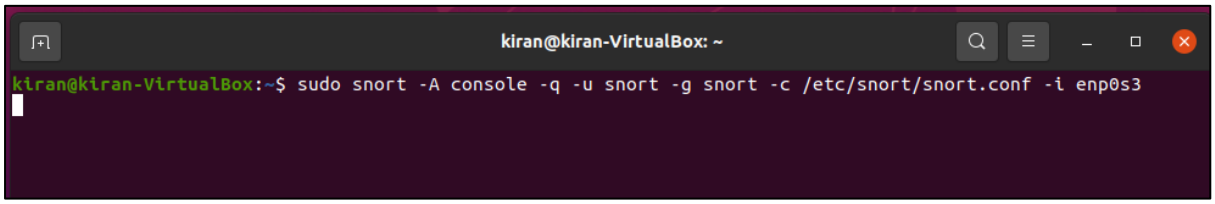
Check the snort is configured successfully and check for validation

Sudo snort -T -c /etc/snort/snort.conf -I enp0s3

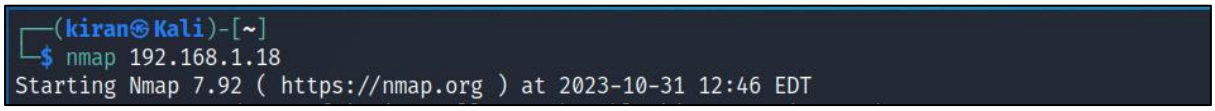




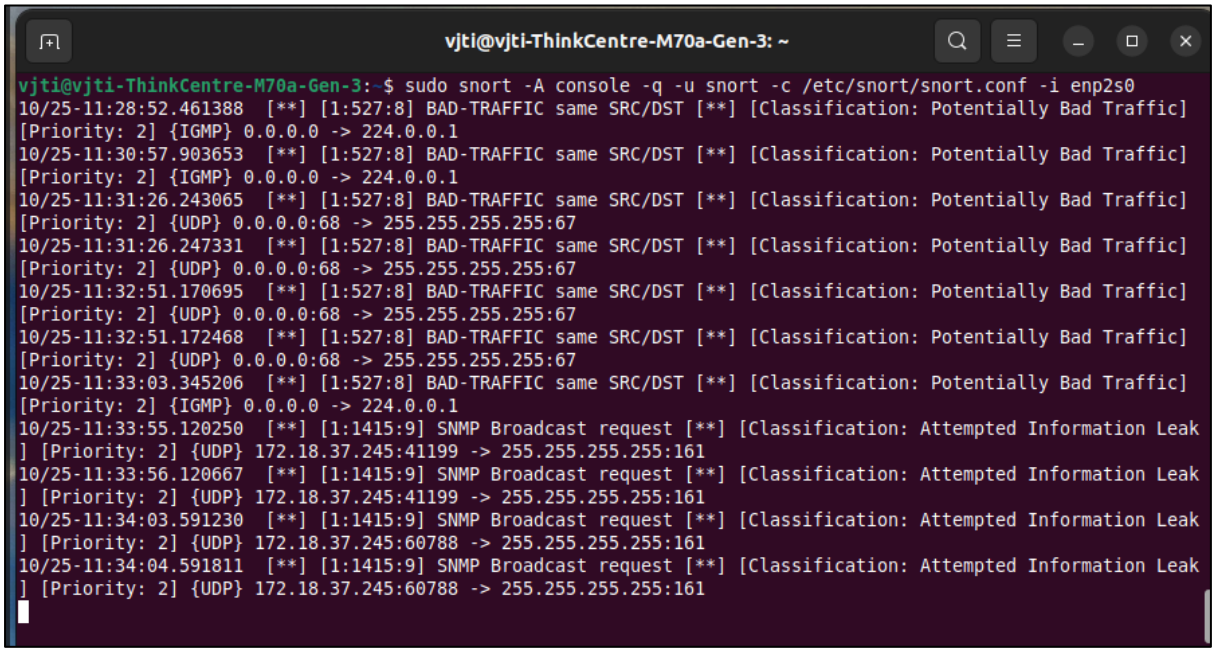
Enable the snort and check for the traffic



Open the kali linux and then perform attacks to this machine



Network traffic and attacks reported



Conclusion:

In conclusion, this experiment involved the setup of SNORT as an Intrusion Detection System (IDS) in a controlled network environment. The experiment included configuring SNORT, creating custom rules, and simulating network attacks using a Kali Linux machine. SNORT effectively monitored the network traffic, detected malicious activity, and generated alerts and logs. Documentation and screenshots were used to capture the experiment's progress and findings. This experiment provided valuable insights into the capabilities of SNORT as an IDS for detecting network threats and enhancing network security.