IDS_using_SNORT tool

IDS (Intrusion Detection System):

An Intrusion Detection System (IDS) is a security mechanism designed to detect unauthorized access, potential attacks, or suspicious activities within a network or system. The purpose of an IDS is to monitor traffic and identify malicious activities, security breaches, or violations of security policies in real-time, providing alerts for further action**.**

Key Functions of IDS

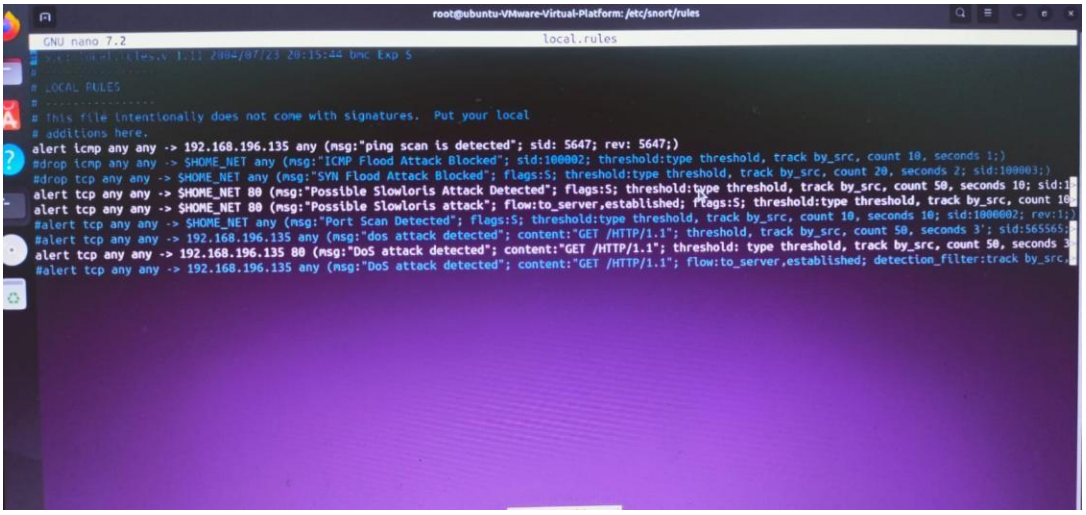
- Monitoring Traffic: IDS continually monitors network or system traffic to detect abnormal patterns that could suggest an attack or security breach.
- Alerting: When an intrusion or potential security threat is detected, the IDS generates alerts or notifications to security personnel, enabling them to take immediate action.
- Recording Events: IDS can log all network activities or system events for future analysis, helping in forensic investigations and improving security policies.

Proof of concept:

Step-1: on the ubuntu terminal

open the rules as cd/etc/snort/rules

In local.rules: alert imp any any -> 192.168.1.109 any (msg:" PING SCAN IS DETECTED"; sid: 569847; rev: 547;)



STEP-2: snort -A console -q -c /etc/snort/snort.conf

1. snort

- This is the Snort command itself, which is used to start the Snort IDS/IPS process.

2. -A console

- The -A option specifies the alert output method.
- console means that Snort will display alerts directly to the console (i.e., standard output).
- This is often used for testing purposes or when you want to monitor alerts in real time directly on the terminal. When Snort detects an intrusion or suspicious activity, it will print an alert to the screen.

3. -q

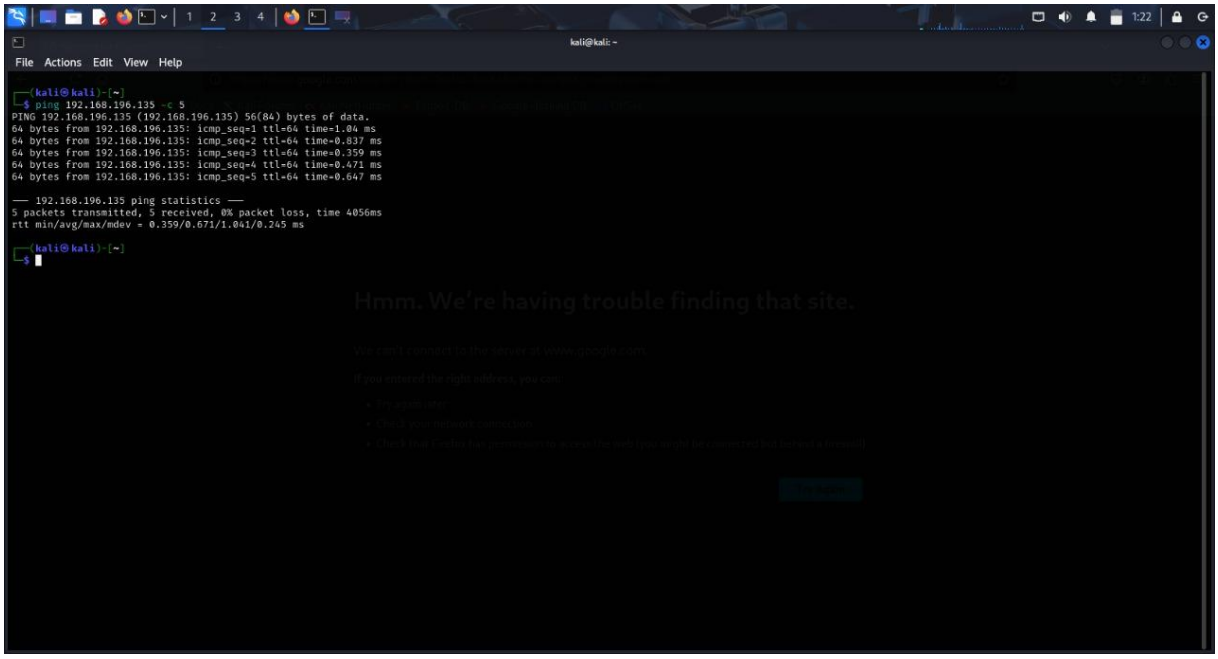
- The -q option stands for "quiet mode".
- When -q is used, Snort reduces the verbosity of its output, showing only alerts and critical information. This means Snort won't output verbose information about the packets it's processing; it will only show the alerts that match your configured rules.
- Without this flag, Snort would typically print more detailed logs and packet information, which might include lots of data that's not always useful for quick monitoring.

4. -c /etc/snort/snort.conf

- The -c option specifies the path to the Snort configuration file.
- /etc/snort/snort.conf is the typical location for the Snort configuration file on many Linux distributions.
- This configuration file contains the rules, settings, and parameters that define how Snort analyzes network traffic. It includes network variables, rule sets, logging options, and other settings.

Step-3:

The target machine is kali Linux ,here we are performing the PING scan



Step-4:finally alert appeard