Cyber Security and Snort IDS/IPS Implementation Report

Internship Title:

Cyber Security and Snort IDS/IPS installation, configuration, detect and validate the rules and alerts

Prepared By: VIJAY S R

Date : 28/11/2025

1. Introduction

This report provides foundational knowledge of cybersecurity and a comprehensive, step-by-step guide to installing, configuring, and operationalizing the Snort Intrusion Detection and Prevention System (IDS/IPS) on an Ubuntu machine. It also includes detailed instructions for custom rules creation and validation of triggered alerts.

2. Cyber Security Basics

Cyber security refers to the practice of protecting systems, networks, data, and applications from digital threats. These threats include malware, unauthorized access, data breaches, phishing attacks, Denial of Service (DoS), and more.

2.1 Key Cyber Security Concepts

- Confidentiality: Ensuring only authorized users have access to data.

- Integrity: Ensuring data is accurate and unchanged.

- Availability: Ensuring systems and data are accessible when required.

- Threat: Any circumstance that can exploit vulnerabilities.

- Vulnerability: A weakness in system security.

- Exploit: A method used by attackers to leverage vulnerabilities.

2.2 Key Security Domains

- Network Security

- Endpoint Security

- Application Security

- Identity and Access Management (IAM)

- Security Operations

3. Snort IDS/IPS Overview

Snort is an open-source, signature-based network intrusion detection and prevention system. It performs real-time packet inspection and traffic analysis.

3.1 Snort Modes

- Sniffer Mode

- Packet Logger Mode

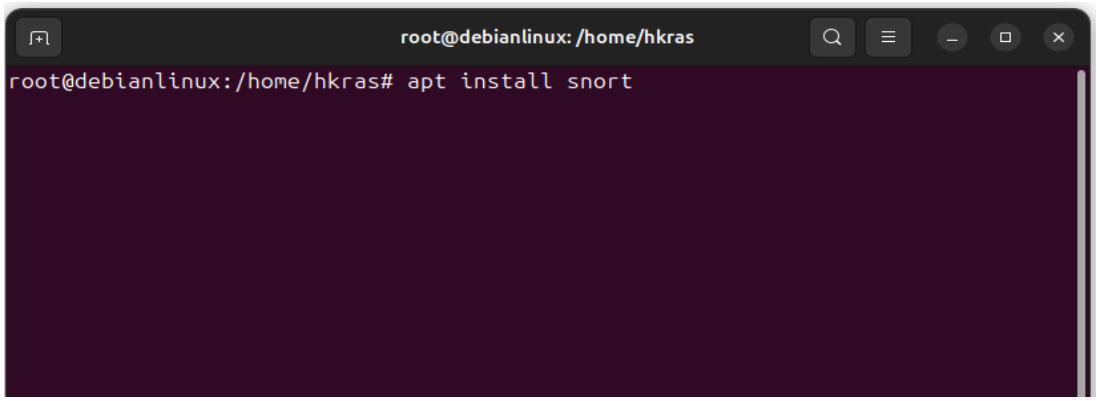
- Network IDS Mode

- IPS Mode

4. Snort Installation on Ubuntu

Installation steps for Snort 2.9.20 . Open the terminal type

sudo apt install snort



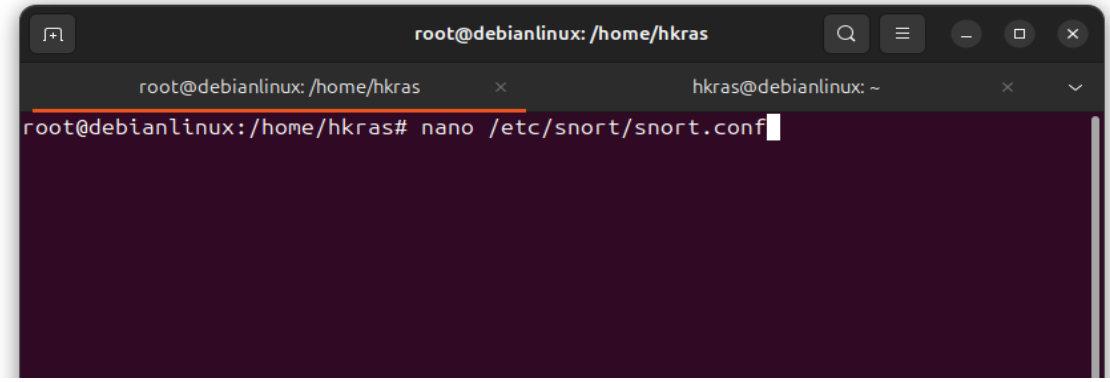
Then check the version:- sudo snort –V or snort —version

5. Snort Configuration

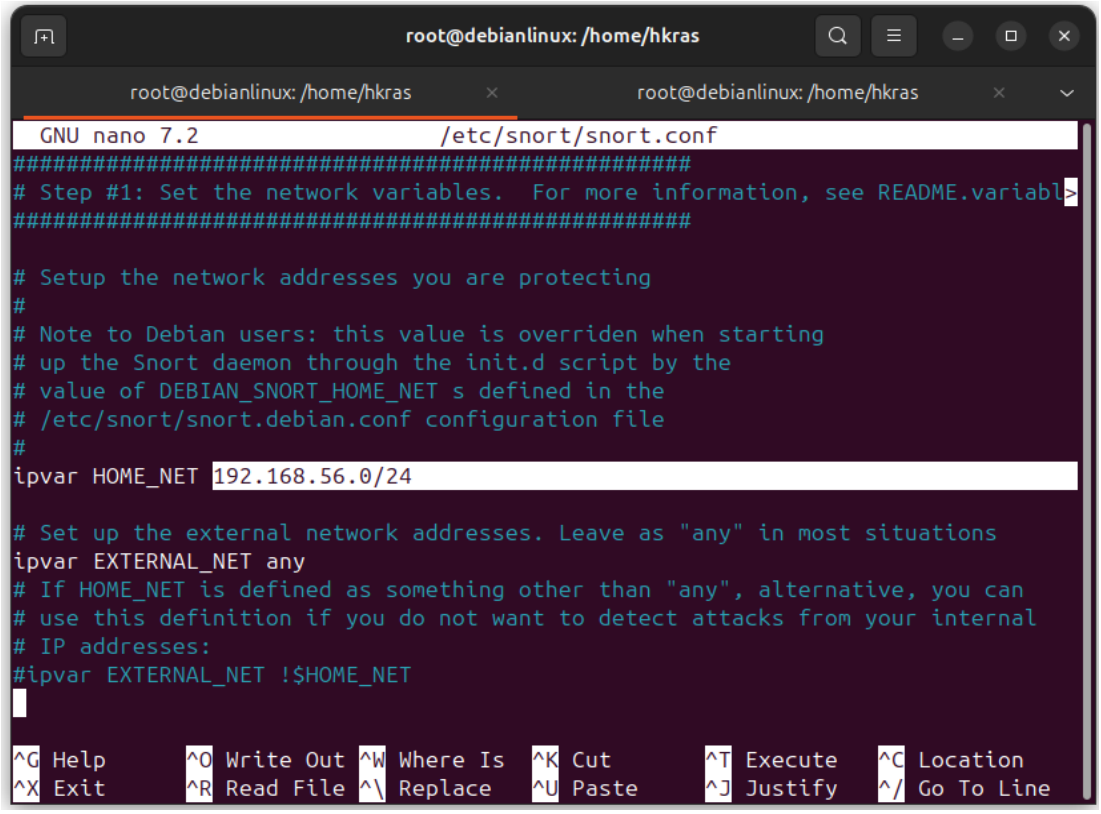
Configuration of directories, rule paths, snort.conf tuning, and enabling local rules.

You should do some changes in snort.conf file.

sudo nano /etc/snort/snort.conf



We should configure our entire network with snort. So you make change your conf file like the below image



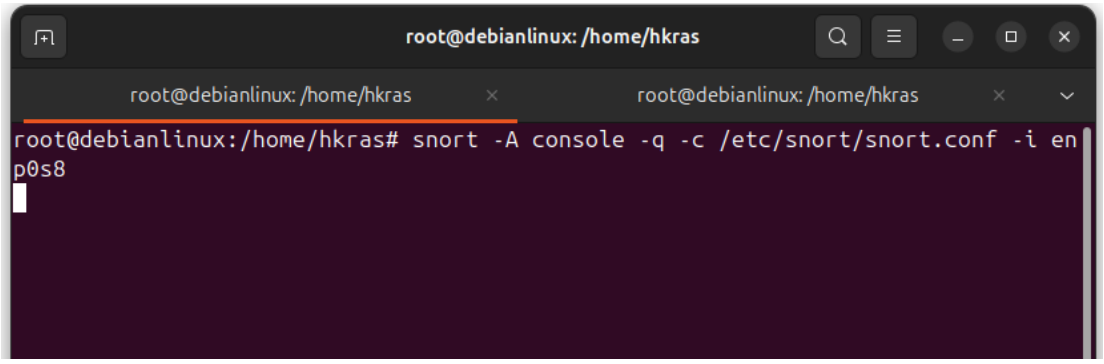
Add your entire network ip range in ipvar HOME_NET . See the above image for your referrence and your ip range may vary depends on your internet service provider. So check your ip address and range using ip –a command on ubuntu.

6. Running Snort in IDS and IPS Modes

Commands for:

- IDS mode

sudo snort –A console –q –c /etc/snort/snort.conf –i enp0s8



Interface may change depends on your vms like eth0, eth1, eth2 this

- enable and run Inline IPS mode using NFQUEUE and iptables redirection using following commands

Enable NFQUEUE:

sudo apt install –y libnetfilter-queue-dev

Run snort inline:

sudo snort –Q —daq nfq –c /etc/snort/snort.conf –i enp0s8

Add iptables rules to divert packets:

sudo iptables –I INPUT –j NFQUEUE —queue-num 0

sudo iptables –I OUTPUT –j NFQUEUE —queue-num 0

7. Snort Rules Creation

7.1 Rule Structure

Action protocol source_ip source_port -> dest_ip dest_port (options)

7.2 Example Rules

- ICMP Ping Detection Rule

alert icmp any any -> $HOME_NET any (msg:”icmp ping detected”; sid:1000001; rev:1;)

- FTP Anonymous Login Detection

alert tcp any any -> $HOME_NET 21 (msg:”FTP Anonymous Login Attempt”; content:”USER anonymous”; sid:1000002; rev:1;)

- SSH Bruteforce attempt Rule

alert tcp any any -> $HOME_NET 22 (msg:”SSH Bruteforce Attempt”; threshold:type both, track by_src, count 5, seconds 60; sid:1000003; rev:1;)

- SQL Injection Detection Rule

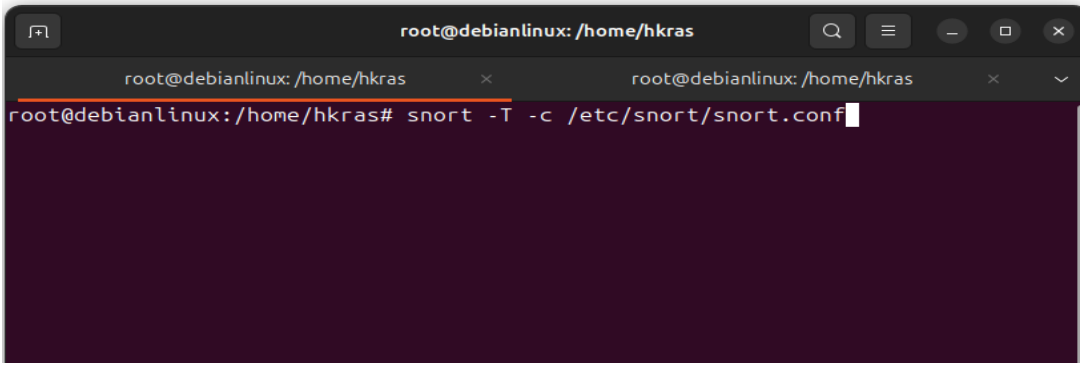
alert tcp any any -> $HOME_NET 80 (msg:”SQL Injection Attempt”; content:”select”; nocase; sid:1000004; rev:1;)

Alert tcp any any -> $HOME_NET 80 (msg:”SQL Injection Attempt”; content:”union”; nocase; sid:1000005; rev:1;)

8. Validating Snort Rules (testing Alerts)

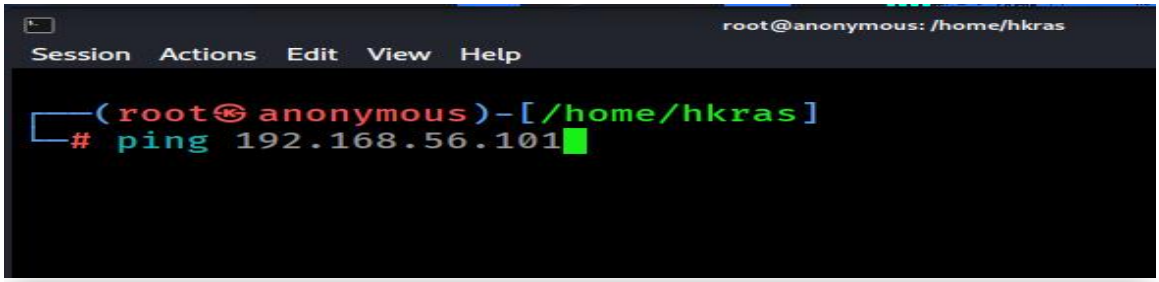
8.1 validate Configuration

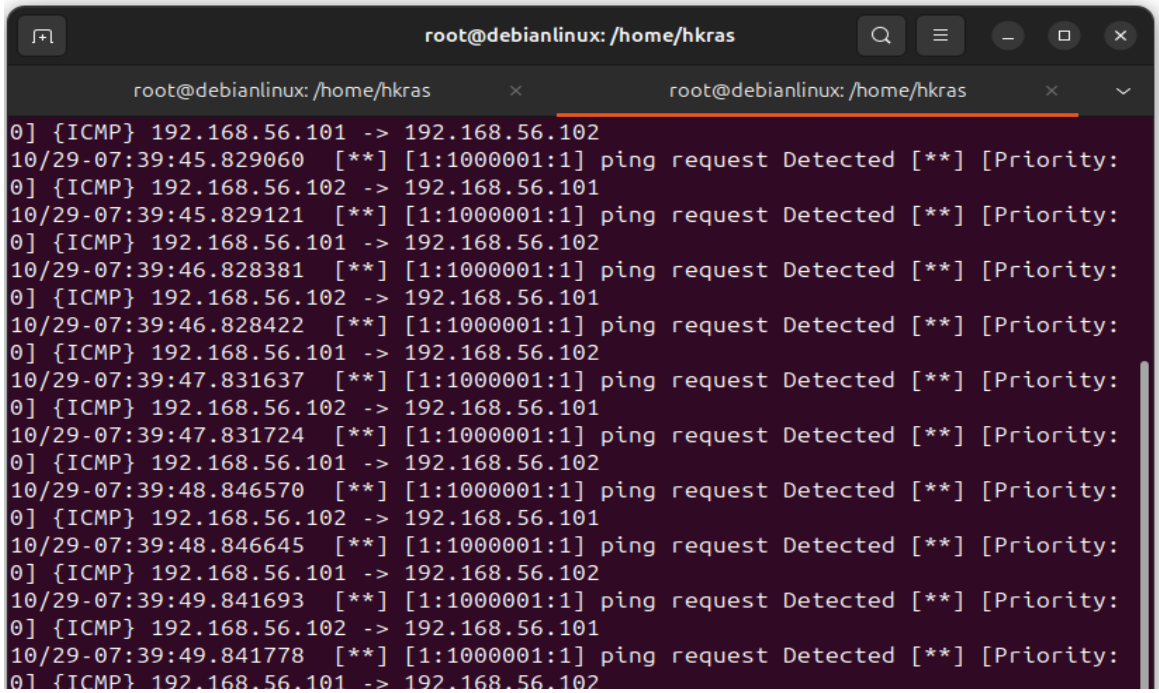
sudo snort –T –c /etc/snort/snort.conf



8.2 Testing ICMP Rule

Ping 192.168.x.x (type the snort installed machine ip address)

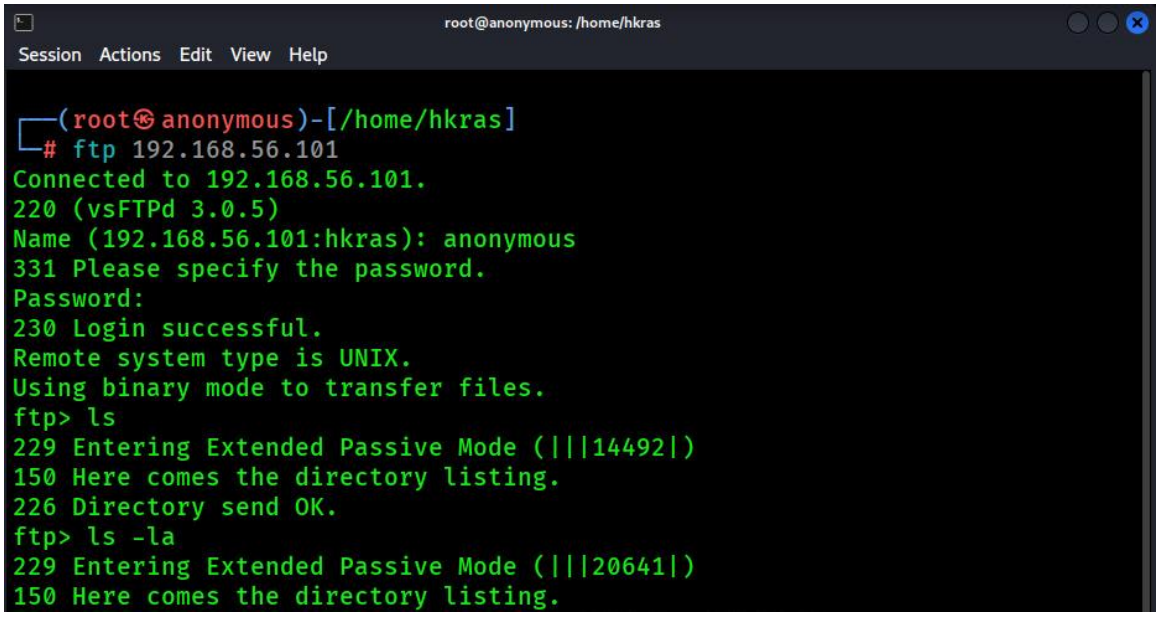


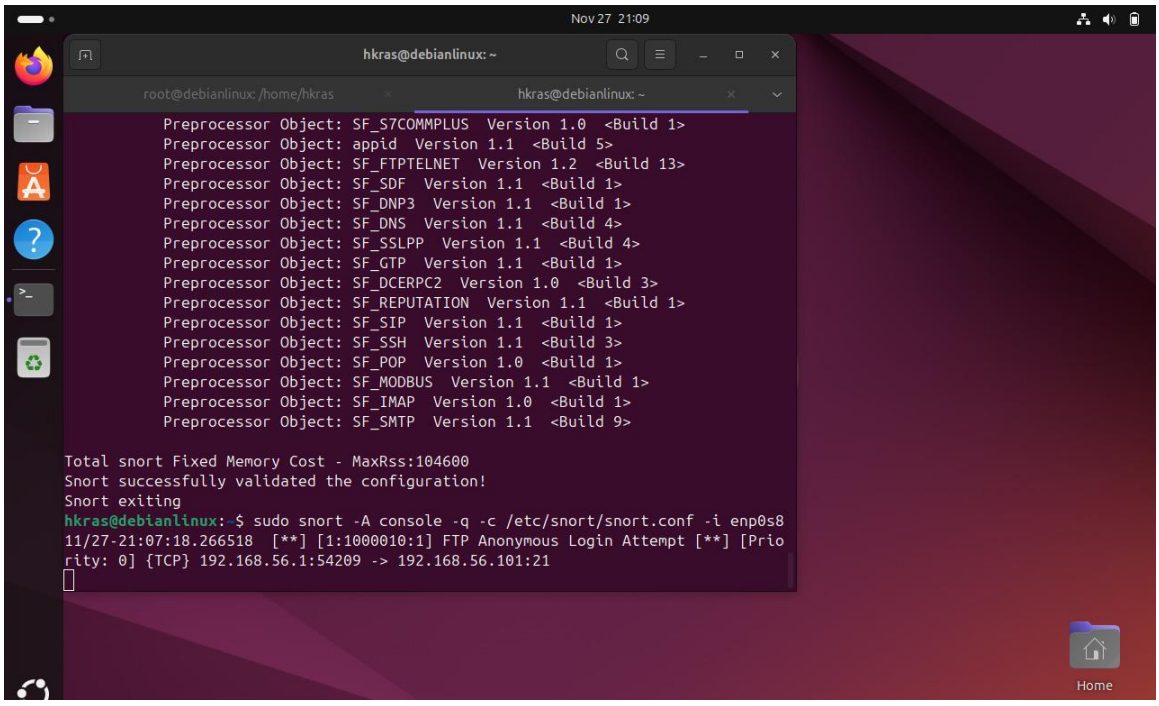


Ping request detected and the alert triggered

8.3 Testing FTP Anonymous Rule

ftp 192.168.x.x (snort installed machine ip)



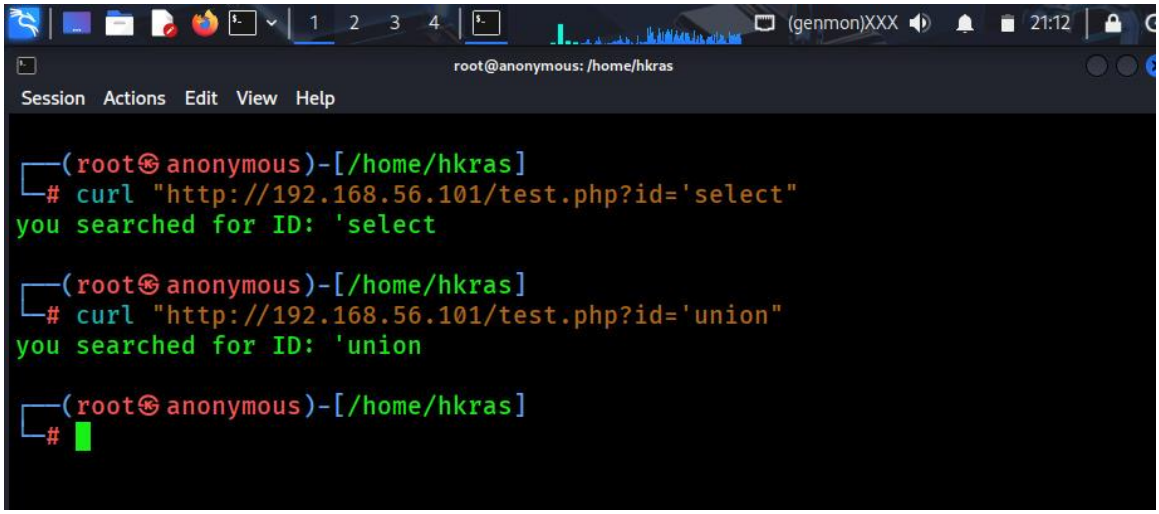


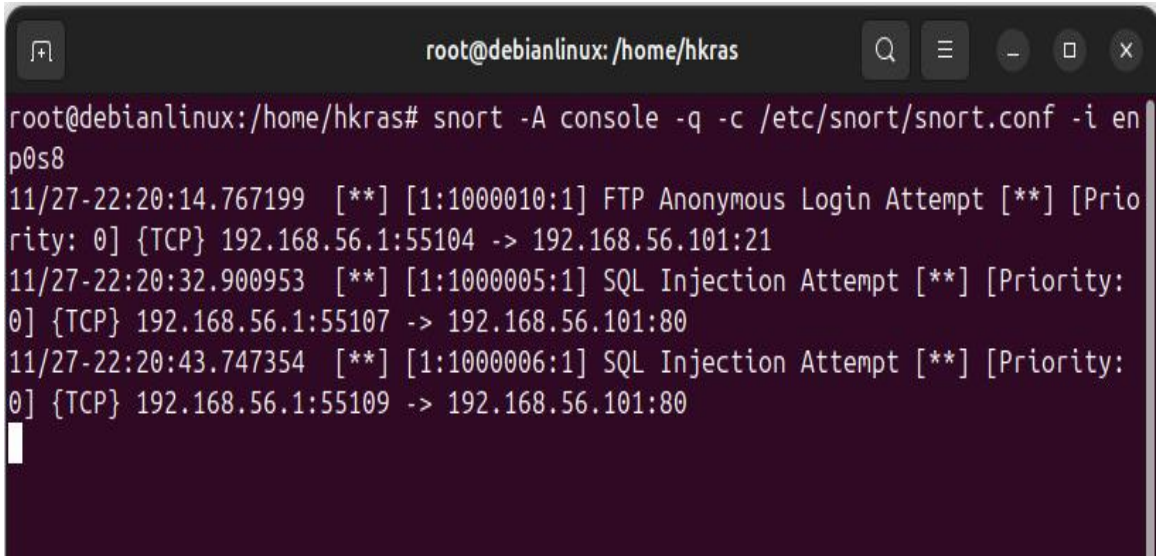
FTP anonymous login attempt detected and the alert triggered.

8.4 Testing SQL Injection Rule

Curl “http://192.168.56.101/test.php?id=’union”

Curl “http://192.168.56.101/test.php?id=’select”





SQL Injection attempt detected and alert triggered in Snort IDS Mode.

9. Viewing Alerts

Snort logs alerts to:

/var/log/snort/alert

To view:

sudo tail –f /var/log/snort/alert

10. Conclusion

This report covered the cybersecurity fundamentals and provided a complete guide to deploying Snort IDS/IPS on Ubuntu, including installation, configuration, rule authoring, and alert validation. By following these instructions, you can use snort as an effective network monitoring and intrusion detection tool on your environment.