

Packet Sniffer with Alert System

Name: Sasi kumar Medabalimi

Date: 24/07/2025

Introduction

This project is a lightweight packet sniffer that monitors live network traffic and alerts on suspicious activity such as ICMP protocol use.

Tools Used

- Python 3
- Scapy
- JSON
- Windows Terminal(cmd)

Steps Involved

1. Capturing live traffic using scapy
2. Parsing each packet
3. Comparing against alert rules in rules.json
4. Logging all traffic
5. Displaying real-time alerts for suspicious packets

Conclusion

This tool provides insight into network activity and helps detect unauthorized or abnormal traffic, serving as a foundation for a custom NIDS.