Basic Network Sniffer Project Summary

This project is part of the CodeAlpha Cyber Security Internship. The objective of this task was to build a Basic Network Sniffer using Python.

Objective:

To capture and analyze real-time network traffic using Python and understand the structure of packets flowing through the network.

Tools & Technologies Used:

- Python 3

- Scapy library for network sniffing and packet analysis

Key Features:

- Captures live network packets using Scapy

- Extracts and displays packet information like source IP, destination IP, protocol type, and port numbers

- Supports common protocols like TCP, UDP, and ICMP

How It Works:

- The script uses Scapy's sniffing function to monitor traffic on the default network interface.

- It processes each captured packet and prints structured output to the console for analysis.

Usage Instructions:

1. Install Scapy: pip install scapy

2. Run the script with admin privileges: sudo python sniffer.py

3. Observe the terminal output to see captured packets in real time

Conclusion:

This project demonstrates how basic network sniffing works and how Python can be used to understand and analyze packet-level traffic. It provides a foundation for more advanced network monitoring and intrusion detection systems.