Code Alpha Cybersecurity Internship

Submitted by:

Saira Arshad

Internship Period:

August 2025

Institution/Platform:

Code Alpha

Date of Submission:

August 2025

Table of Contents

1. Project Objective

The objective of this task was to develop a basic network sniffer using Python. The program captures and analyzes network traffic in real time, identifies key protocols (TCP, UDP, ICMP), and extracts useful information such as source/destination IP addresses, ports, and payload data. This task aims to build foundational skills in packet analysis, protocol structure, and low-level networking.

2. Tools Used

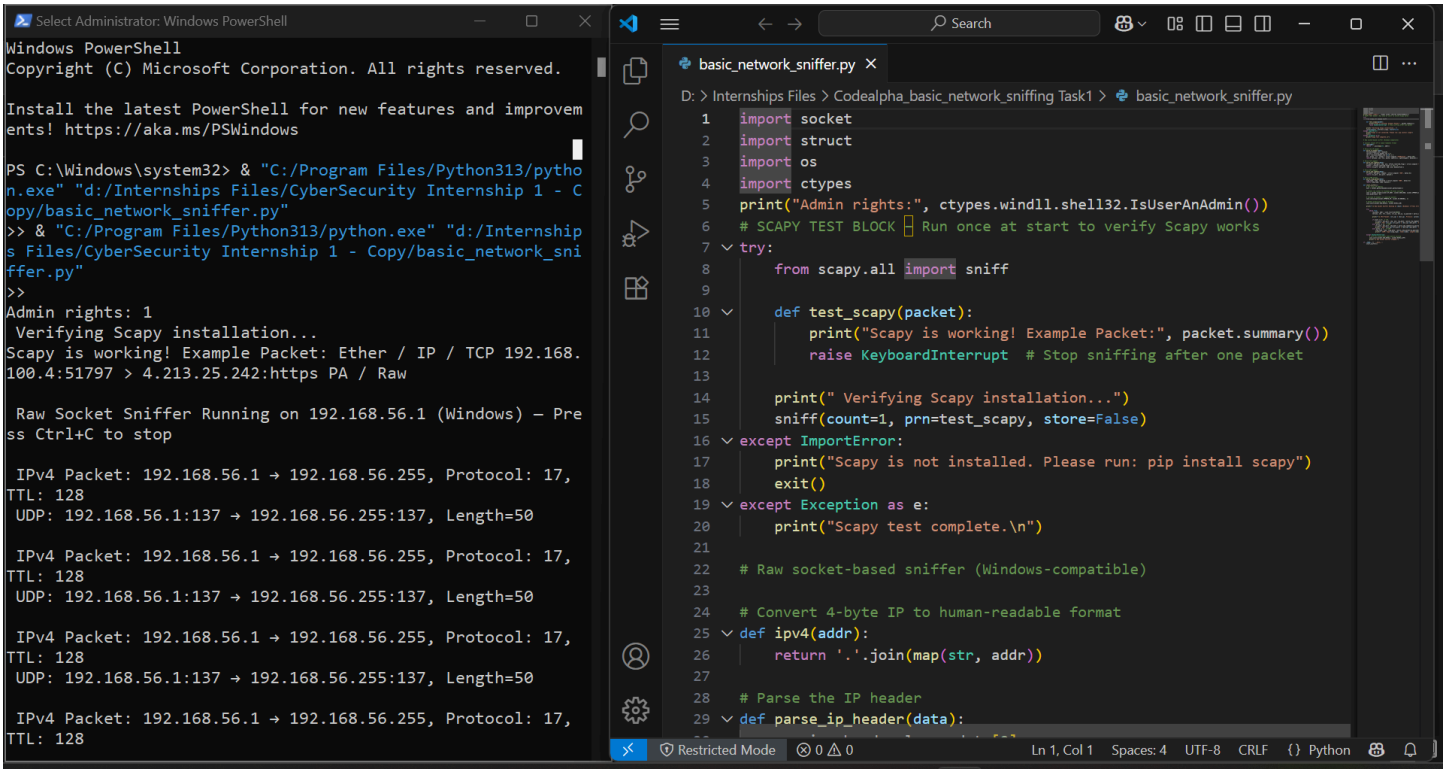
- - Python 3.10+: Core programming language used for development
- - Scapy: For packet manipulation and verification
- - socket: Used to create raw sockets for packet capturing
- - struct: Used to unpack binary data from network packets
- - PowerShell/CMD: Used to run the script with administrator privileges
- - Npcap: Windows packet capture driver required for raw sockets

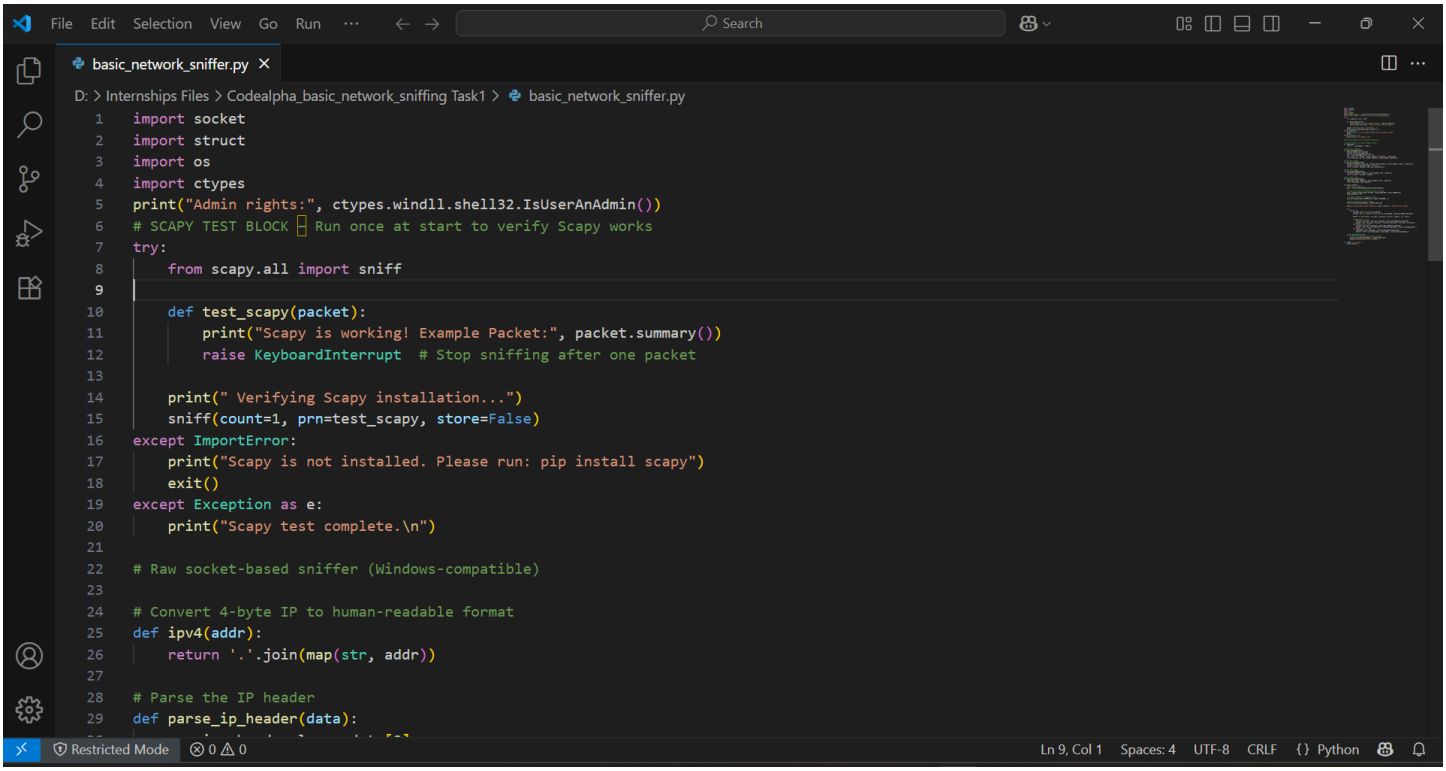
3. Code Explanation

The script begins by checking if it is being run as an Administrator. It uses the socket module to create a raw socket that listens to all network traffic on the host machine. The IP header is parsed using struct.unpack to extract details such as TTL, protocol type, and IP addresses.

Depending on the protocol (TCP, UDP, ICMP), further functions are used to parse and display relevant information such as port numbers, sequence numbers, and data lengths. A Scapy block is also included at the beginning to verify that packet analysis tools are working correctly.

4. Screenshots





5. Output Samples

Admin rights: 1
Sniffing on 192.168.100.82 (Windows) — Press Ctrl + C to stop

IPv4 Packet: 192.168.100.82 → 239.255.255.250, Protocol: 17, TTL: 2
UDP: 192.168.100.82:55033 → 239.255.255.250:1900, Length=201

IPv4 Packet: 192.168.100.82 → 8.8.8.8, Protocol: 6, TTL: 64
TCP: 192.168.100.82:50321 → 8.8.8.8:443, Seq=123456789, Ack=987654321

6. Learnings and Challenges

Learned how raw sockets work and how to access low-level network data.
Understood how to parse IP, TCP, UDP, and ICMP headers using struct.
Faced issues with Windows permissions (WinError 10013) which required running the script as Administrator.
Gained hands-on experience with the Scapy library and its role in cybersecurity tools.

7. Conclusion

This project successfully met the requirements of Task 1 in the Code Alpha Cybersecurity Internship. It provided practical experience with raw sockets, packet parsing, and network protocol structures. The ability to interpret and analyze network packets is a valuable skill in the field of cybersecurity

8. Submission Info

Name: Saira Malik

Internship: Code Alpha Cybersecurity Internship

Task: Task 1 - Basic Network Sniffer

Date of Submission: August 2025