CYBER SECURITY INTERNSHIP

Task 5: Capture and Analyze Network Traffic Using Wireshark

Name: Muhammed Shan Yoosuf

Tool Used: Wireshark

Objective: Capture live network traffic and analyze protocols.

Introduction

Wireshark is a network protocol analyzer used to capture and inspect network packets in real-time. It helps in troubleshooting, monitoring, and analyzing network communication by displaying packet-level details.

Procedure

- Installed Wireshark and selected the active network interface.
- Started capturing live network traffic.
- Generated traffic by browsing websites and using ping command.
- Stopped the capture after one minute.
- Applied filters such as tcp, udp, dns, and http.
- Exported the capture file as a .pcap file.

Protocols Identified

- TCP – Observed TCP 3-way handshake (SYN, SYN-ACK, ACK).
- UDP – Used for fast communication without connection establishment.
- DNS – Captured DNS query and response packets while browsing websites.
- HTTP – Observed HTTP GET request and server response packets.

Key Observations

- Source and destination IP addresses.

- Packet length and protocol type.
- Port numbers and communication flow.
- Packet timestamps and sequence numbers.

Conclusion

This task provided practical exposure to packet capture and protocol analysis using Wireshark. It improved understanding of TCP/IP communication, protocol behavior, and network troubleshooting techniques.