Day 101

Topic: Wireshark Packet Analysis

Objective: To analyze network traffic in real-time using Wireshark for troubleshooting and security monitoring.

Theoretical Concepts:
Packet sniffing is a core skill for cybersecurity. We introduced Wireshark as the industry-standard network protocol analyzer. We discussed "Promiscuous Mode," which allows a network card to see all traffic on the wire, not just traffic destined for it. We learned about capture filters (to limit file size) and display filters (to find specific packets).

Practical Work:
We captured live traffic while browsing the web. We filtered for *http* traffic and located plain-text credentials in a login form on a test website (demonstrating the risk of non-SSL sites). We analyzed the TCP 3-Way Handshake (SYN, SYN-ACK, ACK) by following a TCP stream. We also looked at ICMP packets generated by a ping command.

Tools Used: Wireshark.

Outcome: Competence in capturing packets, filtering traffic, and inspecting packet headers for security analysis.