Experiment 17

AIM: Tool Exploration -Wireshark

31/08/23

Experiment - 17

AIM: Tool Exploration - Wireshark.

Introduction:

Wireshark is a widely used open source network protocol analyzer that provides insights into the operations of Computer Networks.

- It is used to track packets so that each one is filtered to meet our specific needs.
- It is also used by network engineers to examine security problems.

Features Explored

(1) Packet Capture:

Wireshark can capture packets from various network interfaces.

(2) Protocol Analysis:

Wireshark supports a wide range of network protocols like HTTP, ARP, TCP, UDP, etc..

(3) Filtering of data

Wireshark allows users to apply filters to captured packets, helping focus on specific details.

(4) Packet Decoding

The captured packets are decoded and presented in a human-readable format.

(5) Colorization

In WireShark, packet colors can indicate various attributes, such as packet types or errors, thereby enhancing the visual analysis.

Filter by Protocol

- Once we start capturing packets, we can click on the "Current filter" box and type the protocol that we want to sort our packets by.

Filter by IP Address

- Right click on the IP address, we want to sort with "Apply as Filter → "Selected":
and only the packets that involve our selected protocol as source or destination are filtered.

- By using these filtering techniques, users can isolate & relevant data from the captured packet systems.
- Thus, WireShark helps in Real-time monitoring, Enhanced Security analysis, In-depth insights and Efficient Trouble-shooting.

31/8/23