31/8/23

Wireshark

wireshark, a powerful open-source network protocal analyzer, empowers network proffrionals to explore & understand the intricacies of data transmission across networks. This tool plays a pivotal role in diagnosing network issues, optimizing performance, and ensuring robust security measures. In this write-up, we delve into the core funclities of wireshark and highlight its significance in network analysis.

Functionality overview:

i) Packet capture & Filtering.
wireshark's primary function lies in capturing network packets from various interfaces. Its flexible filtering options enable users to capture specific types of traffic based on protocols, source/destination addresses and even keywords within packet payloades.

ii) Real-time Analysis:
Wireshark's real-time monitoring capability is invaluable for observing ongoing network activities. This feature aids in detecting sudden traffic spikes, unusual protocol behavior, and unauthorized network usage.

iii) Protocol Analysis: It decrypts encrypted protocols offering insights into secure communication method

iv) Packet Reconstruction: Allows reassemble of fragmented packets.

v) Statistical Information: Presents statistical analysis of captured data

vi) color-coded visualization: Employs color-coded packets to indicate various aspects such as error

vii) customizable Display: This tool offers a customiza-ble interface where users can choose which fields to display & how to arrange them.

→ Procedure

i) In the 1st window, select ethernet.

ii) Filter TCP or any require protocol

iii) Click on it, new window opens.

iv) Dropdown : Transmission control Protocol, Src Port : 62148, Dst Port : 443, Seq : 2, Ack : 65, Len : 0

v) This is ~~avalial~~ available in the prev window in the left split of screen

vi) clicking on dropdown of it, clicking on any of them highlights its counterpart in right split side of screen

vii) In cmd, type ~~[illegible]~~ > ipconfig

~~ut~~ RESULT:

```
Windows IP configuration
Ethernet adapter Ethernet:
connection-specific DNS suffix. :
Link-local IPv6 Address . . .   : fe80::be70:f6a9
                                  ed25:c329%1
IPv4 Address . . . : 10.124.2.83
Subnet Mask . . . . : 255.255.0.0
Default gateway . . . : 10.127.0.11
```

31/8/23