Cycle II

LAB 17:

Aim : Tool Exploration -Wireshark.

Wireshark

- Wireshark, a powerful open-source network protocol analyzer, or packet analyzer.
- It is used for network troubleshooting, analysis, Software and communication protocol development and education.
- It is used to track packets so that each one is filtered to meet our specific needs. It is also used by network security engineers to examine security problems.

Functionality of Wireshark :-

- It lets the users put network interface controllers that support promiscous mode into that mode, so they can see all the traffic visible on that interface.
- Packet capture and filtering:
  Primary function of wireshark lies in capturing network packets from various interfaces. Its flexible filtering options enable users to capture specific types of traffic based on protocol, source/destination addresses and even keywords within packet payloads.
- Real time Analysis:
  Wireshark's real time monitoring capability is invaluable for observing ongoing network activities

- This feature helps in detecting sudden traffic spikes, unusual protocol behaviour, and unauthorized network usage.
- Protocol Analysis:
  It decrypts encrypted protocols offering insights into secure communication method.
- Packet Reconstruction: Allows reassembling of fragmented packets.
- Statistical Information: Presents statistical analysis of captured data.
- Color-coded visualization: Employs color-coded packets to indicate various aspects such as error.
- Customizable Display: This tool offers a customizable interface where users can choose which fields to display & how to arrange them.

Procedure:

1) In the 1st window, select ethernet.
2) Fitles TCP or any required protocol.
3) Click on it, new window opens.
4) Dropdown: Transmission Control Protocol.

Scr Port: 62148, Dst Port: 443, Seq: 2,
Ack: 65, Len: 6

5) This is available in the previous window in the left split of screen.

6) Clicking on dropdown of it, clicking on any of them highlights its counterport in right split side of screen.

7) In cmd, type > ipconfig
~~RES~~
Result:-
Windows IP configuration
Ethernet adapter Ethernet:
Connection-specific DNS suffix:
Link-local IPv6 Address . . . : fe80::he78:ffa9:
ed25:e329:b3
IPv4 Address . . . : 10.129.2.83
Subnet Mask . . . : 255.255.0.0
Default-Gateway . . : 10.127.0.11