WEEK 17

Tool Exploration -Wireshark

OBSERVATION:

Week-17

Tool Exploration - Wireshark

Wireshark is an open source packet analyzer which is used for education analysis, software development communication protocol development and network protocol is used to leach packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyser, it is used by network security problems.

Wireshark is a free applications used to capture data back and forth. It is called free packet it to accept all packets which it receives.

Uses :-

-> It is used by network security engineers to access security problems.

-> It is used by network engineers to trouble shoot network issues.

-> It is also used to analyse dropped packets

-> It helps to troubleshoot latency used malicious activities on the network

-> It helps us to know how our laptop mobile phones desktop communicate

Functionality of Wireshark

It is similar to a TCP dump networking. It has a graphic and filtering functions. It also unicast traffic which is not to network port address interface host networking method to network traffic. When it is enabled switch sends copies of all network packet present at port to another port.

Features of Wireshark

It is a multi platform software ie it can run on linux, Windows OSX, Free BSD etc:- It is a standard three pane, packet It performs deep inspection of protocols.

It performs best & filter option which makes easy to user to view. the data

- It can capture raw USB traffic
- It is useful in IP address.
- It also evolves live analysis, ie from different types of network like ethernet loopback etc through which we can read live data.