Date 24/08/23
Page 44

Write on Wireshark.

Tool Exploration - Wireshark

Wireshark is an open source packet analyzer which is used for education analysis, software development communication protocol development and network troubleshooting. It is used to track packets to that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, network analyzer. It is also used by network security engineers to examine security problem.

Wireshark is a free application used to apprehend data back and forth. It is also called as a free packet sniffer computer application, puts network cared into a unselective mode i.e to accept all packets which it recives.

Uses

1. It is used by network security engineers to examine security problems.
2. It is used by network engineers to trouble shoot network uses.
3. It is also used to analyze dropped packets.
4. It helps to trouble shoot latency malicious activities on the network.
5. It helps us to know how all demo like laptop, mobile phones, desktop switch routers communicate in a local network or the reset of the world.

Functionality of wireshark.

It is similare to a TCP dump in networking. It has a graphic, end, sort and filtering functions. It

Date / /
Page 15

also monitors the unicast traffic which is not sent to network's MAC address interface. The port mirroring is a method to monitor the network traffic. When it is enabled switch sends copies of all network packets present at one port to another port.

Features of wireshark:

- It is a multiplatform software i.e it can run on the Linux, windows, OS X, True BSD, Net BSD, etc.
- It is a standard three pane packet browser.
- It performs deep inspection of hunk of protocols.
- It even has sort and filter option which makes ease to user to view the data.
- It can capture raw USB traffic.
- It is useful in IP analysis.
- It also involves live analysis i.e from different types of network like ethernet, loopback etc through which we can read live data.