Tool Exploration

Wire - Shark

Wire - Shark is an open (tool) source packet analyzer, which is used for education, analysis, software development, communication protocol development and network troubleshooting. It is used to track packets so that each one is filtered to meet our specific needs. It is commonly called as sniffer, network protocol analyzer and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses:

Wireshark can be used in the following ways:

1) It is used by network security engineers to examine the security problems.
2) It allows the users to watch all the traffic being passed over the network.
3) It is used by network engineers to troubleshoot network issues.
4) It also helps to troubleshoot latency issues and malicious activities on your network.

5) It can also analyze dropped packets.

6) It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers etc. communicate in a local network or the rest of the world.

Functionality of WireShark:

WireShark is similar to tcpdump in networking.

Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to computer. It has a graphic end and some sorting and filtering functions.

Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to network's MAC address interface. But the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic.

Port mirroring is a method to monitor the network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

There are a few features of wireshark which are significant. They are listed below.

Features of Wireshark:

1) It is a multi-platform software, i.e., it can run on Linux, Windows, Free BSD, Net BSD etc.

2) It is a standard three pane packet browser.

3) It performs deep inspection of hundreds of protocols.

4) It often involves, live analysis, i.e., from different types of network like Ethernet, loopback, etc., we can read live data.

5) It has sort and filter options which makes ease to user to view the data.

6) It is also useful in VoIP analysis.

7) It can also capture raw USB traffic.