17)Tool Exploration -Wireshark (Documentation)

Wireshark Documentation

Wireshark is a widely used open-source network protocol or packet analyzer. It allows network troubleshooting, analysis etc.

It is used for software development communication, protocol development, education filtering etc.

Wireshark is a network packet analyser which presents captured packet data in as much detail as possible.

Some purposes of wireshark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

Features of wireshark:

- Available for UNIX and Windows
- Capture live data from a network interface
- Display packets with very detailed protocol information.
- Save packet data captured
- Filter packets on criteria.
- Export some or all filter packets in a number of capture file formats.
- Colorise packet display based filters
- The information of the packets include ID number, time, Source IP address, destination IP address, protocol name, length

and other important information.

- The IP address of the device can be used in the filter to capture only packets sent out to that particular IP address.
- various settings, timers and filters can be set that ensure only triggered traffic appears.

Functionality of wireshark

- Wire shark is a remote machine that captures packets and sends captured packets to a machine running wireshark. it directs the packets so it can analyzire packets captured on a remote machine at the time they are captured.
- It is similar to TCP dump in networking It has a graphic and filtering functions. It also monitors the unicast traffic.
- Port moving is a method to monitor network traffic. When it is enabled switch sends copies of of all network packets present at one port to another port.
- It also supports capture formats from several other commercial and open source network shitters.
- It lets user put network interface controllers that support promiscus mode in that mode so that they can see all traffic in the interface.

9/2023