NATIONAL INSTITUTE OF TECHNOLOGY
WARANGAL-506004
DEPARTMENT OF COMPUTER SCIENCE
AND ENGINEERING
CSE IV B.Tech,Section-C

ROLL NO : 197279
REG. NO. : 811913
NAME : SUDIREDDY DINESH REDDY
SECTION : CSE - C

Security Lab Assignment 10

Wireshark:

Wireshark is a network packet analyzer. It presents captures packet data in as much as detail as possible. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as sniffer, network protocol analyzer , and network analyzer.

Features :

- It has various settings such as timers, filters so that we can filter the output.
- It can only capture packets on pcap supported networks.
- Wireshark supports a variety of well-documented capture files formats such as the pcapng, libpcap. These formats are used for storing the packets.

Uses :

- It can also examine packets that have been dropped.
- It enables us to understand how all devices, such as laptops, cell phones, desktop computers, switches, routers, and so on, connect inside a local network or with the rest of the world.
- It allows users to see all of the traffic that passes through the network.

Analysis from the experiment:

- First, we select a network interface.
- Then, started the capturing packets from the network interface.
- Then, wireshark will the show the packets that are continuously being captured from the network interface.
- The data packet contains
    - no. for number of packets
    - Time
    - Source
    - Destination
    - Length
    - Info

- The data captured is shown in the format of bytes.
- The packets are shown according to the protocol.
    - Green - TCP
    - Dark blue - DNS
    - Light blue - UDP

- We can also apply filters to select the specific packets
- And then I have connected to an FTP server online and tried to download a datafile from the server so that we can observe the packet data present.
- Then I have seen that the username and password used to connect to the FTP server has been shown.
- The I have seen the TCP stream that contains the over ftp connection details and requests continuously .
- This TCP stream is received in encoded format so that we can also convert it to other formats such as RAW UTF-8 etc.