Experiment :

Date

Page No.

Experiment - 4

Objective: Introduction to network protocol analyzer Wireshark.

Theory: Wireshark is a network protocol analyzer tool. It is a powerful tool used for capturing, analyzing and interpreting network traffic in real-time. Wireshark allows users to inspect the data packets flowing through a network interface, providing detailed information about the protocols & communication happening on the network. It's commonly used for network troubleshooting, security analysis, and protocol development.

Features of Wireshark.

1. Live Packet Capture: Wireshark allows user to capture live network traffic from various network interface in real time
2. Offline Packet Analysis: Users can also analyse pre-captured packet capture files (PCAP or other formats) offline.
3. Graphical Packet Analysis: It provides graphical representations of packet data, including packet timing, packet size distribution, protocol hierarchy etc.
4. Cross - Platform Compatibility: It is available for multiple operating systems, including Windows,

CLASSTIME

Experiment : Date

Page No.

macOS & various Linux distributions, making it accessible to a wide range of users.

5. Packet Reconstruction : User can reconstruct & reassemble fragmented or segmented packets to analyse complete data streams, such as TCP streams or HTTP sessions.

Learning Outcome: Understood the function and features of network protocol analyzer that is Wireshark.

14/2/24

CLASSTIME

Experiment :

Date

Page No.

Experiment - 5

Aim: Running and using services/commands related to Networking.

Tool used: Command Prompt

Theory:

1. IPconfig: This command is used in windows operating system to display the current TCP/IP network configuration values. It shows details such as IP address, subnetmask, default gateway, and DNS servers of the network interface on the local machine.

2. nslookup: This command is used to query DNS server to obtain domain name or IP address mapping, or to perform other DNS lookups. It's commonly used to troubleshoot DNS-related issues, as it can help you diagnose problems with domain name resolution.

3. IPconfig/all: This is an extension of ipconfig. It displays more detailed information about all network interfaces on system including MAC address and additional configuration details.

CLASSTIME

Experiment :

Date

Page No.

4. Ping : It is a command line utility used to test the reachability of a host on an IP network. It works by sending ICMP (Internet Control Message Protocol) echo request packets to the target host and waiting for ICMP echo reply packets to come back.

5. tracert : This command is used to trace the route that packets take from your computer to a destination IP address or domain name. It shows the IP address of routers that the packets traverse as they travel to destination.

Result : Successfully run all the commands (IPconfig, IPconfig/all, nslookup, tracert and ping) on command prompt.

CLASSTIME