Exp No: 5
9/5/24

WIRESHARK

Aim :

To capture and analyse the network packets using Wireshark tool .

Wireshark :

It is a network analysis tool formerly known as Ethereal, captures packets in realtime and display them in human readable format. Wireshark includes filters, color coding and other features that let you dig deep dive into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, troubleshoot network problems .

Capture and Analysing packets :

Procedure :

- Select Local Area Network in Wireshark
- Go to capture -> option
- Select stop capture automatically after 100 packets
- Then click start capture
- Save the packets

1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide flow graph :

Procedure :

- Select Local Area Connection in Wireshark
- Go to capture -> option
- Select stop capture automatically after 100 packets.
- Then click start capture
- Search TCP Packets in search bar
- To see flow graph click statistics -> flow graph
- Save the packets

2. Create a filter to display only ARP packets and inspect the packets.

Procedure :

- Go to capture -> option
- Select stop capture automatically after 100 packets.
- Then click start capture.
- Search ARP packets in search bar.
- Save the packets.

3. Create a filter to display only DNS packets and provide flow graph.

Procedure :

- Go to capture -> option
- Select stop capture automatically after 100 seconds.
- Then click start capture.

- Search DNS packets in search bar.
- To see flowgraph click statistics -> flowgraph.
- Save the packets.

4. Create a Filter to display only HTTP packets and impect the packets.

Procedure :-

- Select Local Area Connection in Wireshark
- Go to capture -> option
- Select stop capture automatically after 100 packets
- Then click start capture
- Search HTTP packets in search bar
- Save the packets

5. Create a filter to display only IP/ICMP packets and inspect the packets procedure.

Procedure :.

- Select a Local Area Connection in Wireshark.
- Go to capture -> option
- Select stop capture automatically after 100 packets.
- Then click start capture
- Search ICMP/IP packets in search bar
- Save the packets

6. Create a Filter to display only DHCP packets and inspect the packets.

Procedure :

- Select Local Area Connection in Wireshark
- Go to capture -> option
- Select stop capture automatically after 100 packets
- Then click start capture
- Search DHCP packets in search bar
- Save the packets

9/11

9/10

Result :

Thus, to filter, capture, view and analyse packets using Wireshark has been implemented successfully.