Exp No:5 9/5/24

WIBESHARK

To capture and analyse the network parkets using wiseshark tool.

Wireshark:

It is a network analysis tool formerly known as Ethereal, captures parkets in realting and display them in human readable format Wireshark includes gilters, color coding and other gentures that let you dig deep dise into network traffic and inspect individual parkets. You can use Wireshark to inspect a suspicions peogram's network traffic, analyze the truffic flow on your network, troubleshoot network

Capture and Snalying packets:

Procedure.

problems

- · Select Lord Area Network in Wireshark
- · Go to capture -> option
- " Select stop capture automatically after 100 parhets
 - . Then lik start capture
- . Some the parkets

Create a Filter to display only TCP(UDP packets, inspect the packets and provide flow geoph: Proudure: · S deet Local Area Connection in Wireshoods · Go to capture -> option Silect stop capture automatically exter 100 parkets. Then dick start capture · Search TCP Packets in search lose · To see flow geaph click statistics -> flow graph · Save the purhets Create a filter to display only ARP packets and imput the parkets Procedure: Go to capture -> option Silut stop capture automatically after (00 parkets. . Then dieh start capture · Search ARP packets in search loar. - Save the pathets. Create a gitter to dipplay only DNS parkets and provide flow graph. Procedure: Go to apture - option Select stop coplaire automatically after 100 seconds. Then click start capture

.

2.

- · Search DNS pathets in search lose.
- To see plangraph dish statistics -> flowgraph.
- · Save the parkets.
- 4. Create a Filter to display only HTTP puliets and impert the parkets.

Procedure:

- · Solut Local Area Connection in Wireshark
- · Go to capture -> option
- · Select step capture automatically yter 100 pachets
- · Then click start capture
- · Search HTTP puchets in search boar
- · Save the parkets

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

Procedure.

- · Select a Local Acca Connection in Wireshark.
- · ho to capture -> option
- · Silent stop capture automatically after 100 parkets.
 - Then dick start capture
- Search ICMP/IP parkets in nearthbar
- · Save the parkets

Cuate a Filter to display only DHCP parkets and inspect the grahets.

Procedure:

6.

- · Select Local Area Connection in Wieshack
- 600 to capture -> option
- · Select stop capture automatically after 100 parkets
- Then dick start capture
- · Search DHET parkets in search bar
- · Save the packets

Result:

Thus, to giltu, aptive, view and analyse parkets using Wireshark has been implemented successfully.