PACKET CAPTURE TOOL : WIRESHARK

AIM :
Experiments on Packet capture tool : Wireshark

PACKET SNIFFER :

- Sniffs messages being sent/received from/by your computer.
- Passive program
  → never sends packet itself
  → no packets address to it

PACKET SNIFFER STRUCTURE DIAGNOSTIC TOOLS :

- TCPdump
  → tcpdump -enx host 10.129.41.2 -w exe3.out
- Wireshark
  → wireshark -r exe3.out

DESCRIPTION :

WIRESHARK :

A network analysis tool know as Ethereal, captures packets in real time & display them in human readable format. You can use it to inspect a suspicious program's network traffic

USED FOR :

→ Network administrators : troubleshoot network problems
→ Network security engineers : examine security problems.

→ Developers: debug protocol implementations.

CAPTURING PACKETS

After installing wireshark, launch it & double-click the name of a network interface under capture to start capturing packets on that interface. wireshark captures each packet sent to or from your system.

THE "PACKET LIST" PANE:

Displays all the packets in the current capture file. The "packet list" pane. Each line in the packet list corresponds to one packet in the capture file.

THE "PACKET BYTES" PANE:

Shows the data of the current packet in a hexdump style.

COLOR CODING:

Wireshark uses colors to help you identify the types of traffic at a glance. By default light purple is TCP traffic, light blue is UDP traffic & black identifies packet error.

FILTERING PACKETS:

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other application using the network so you can narrow down traffic.

INSPECTING PACKETS:

Click a packet to select it & you can dig down to its details.

Wireshark is an extremly powerful tool. It is used to debug network protocol implementation, examine security problems.

CAPTURING AND ANALYSING PACKETS:

To filter, capture, view, packets in Wireshark Tool. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface & save it.

PROCEDURE:

- Select Local Area Connection
- 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, inspects the packets and provide the flow

PROCEDURE:

⇒ Select Local Area Connection
⇒ Go to capture → option
⇒ Select stop capture automatically after 100 packet
⇒ 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
⇒ Select stop capture automatically after 100 packets
⇒ Search ARP packets in search bar
⇒ Save the packets

3) Create a Filter to display only DNS packets & provide the flow graph.

PROCEDURE:

⇒ Go to capture → option
⇒ Then click start capture
⇒ Search DNS packets in search bar.
⇒ To see flow graph click statistics → Flow graphs

4) Create a Filter to display only DHCP packets & inspect the packets.

PROCEDURE:

⇒ Select Local Area Connection
⇒ Go to capture → option
⇒ Then click start capture
⇒ Search DHCP packets in search bar
⇒ Save the packets.

RESULT:

Experiment on Packet capture tool done successfully.