Ex! No5
12/9/25

Partical-5

Experiments on Packet Capture tool: Wireshark.

AIM

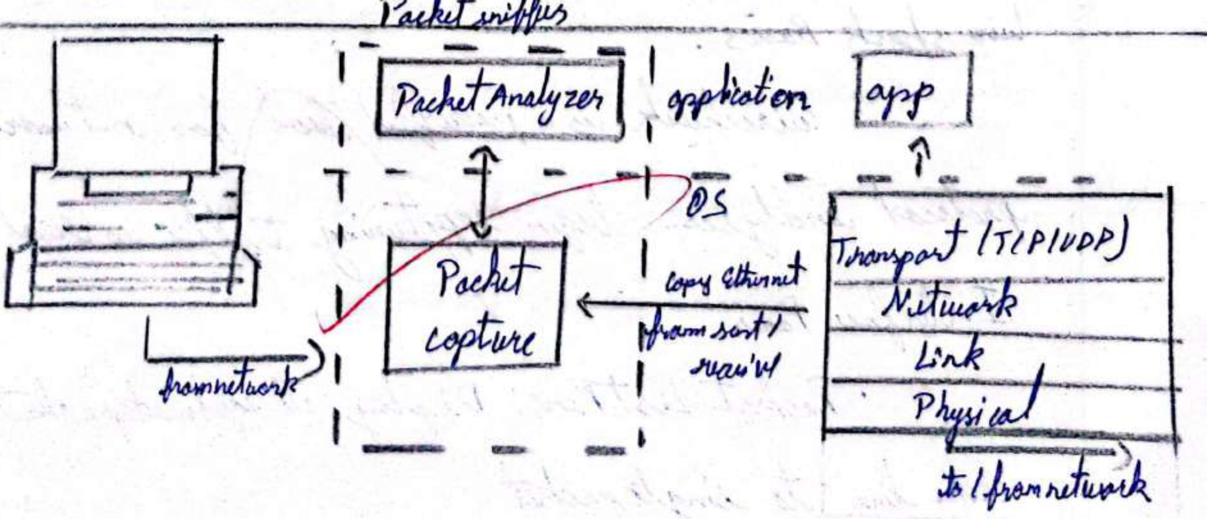
To Experiment on Packet Capture tool : Wireshark.

Packet Sniffer:

- Sniff message being sent/received from/ by your Computer.
- Store and display the contents of various protocal field in messages.
- Passive program
  - never sends packets itself
  - no packets addressed to it
  - receive a copy all packet

Packet Sniffer structure Diagnostic tools

- Tcpdump
  - Eg. tcpdump -enx host 10.129.41.2 -w exe3.out
- Wireshark.
  - wire shark -r exe3.out



Description:

Wireshark

Anetwork analysis tool formerly Knownas Ethereal, captures packets in real time and displays human readable format. includes filters, color code. trouble shoot network Problems

What we can do with wireshark.

- Capture net traffic
- Analyze problem
- watch smart statistics

Wireshark used for

- network administrator: trouble shoot net problems
- Developers: debug protocol implementation
- people: learn network protocol internals.

Getting wireshark:

download from windows - official site.

Wire shark Basics.

Wireshark is a powerful tool for network protocol analysis. begin capturing traffic in real time.

Interface Panes

- Packet List Pane: Display all captured packets, each line to single packet

Packet Pane: shows protocol layers and fields of a selected Pane

Packet Byte: Packet byt pane shows the data of current Packet in hex dump style

Sample Captures:

click file > open wireshark & browse for your downloaded file to open one. open later click file > Save to Save your Captured packets.

filtering Packets:

if trying something specific. close down all other app usind net so can narrow down traffic. still large packets gets sift. so wireshark filter comes in.

DNS packet, when your typing. wire shark will help autocomplit filter

click Analyze > display to chaase filter among the default filter includ wireshark. add your own custom filter & save easily access filter

right click packet. follow > TCP stream - full TCP conversation between client & server, menu to see full conversation for other protocol close window & you'll find a filter has been applied. wireshark shows packet that make conversa

Inspecting Packet

click packet to select it & you can dig down to view its details

you create filter from here - right click one of detail & use Apply as submenu to create filter based on it.

wireshark is powerful tool, scrat the surface of what can do with. debug network protocal implem, examine security problem & inspect network protocal internals

Capturing and Analyse Packet using wireshark tool.

to filter, capture, view, packet capture 100 packet from Ethernet! IEEE 802.3 LAN interface & Save it

1. Create filter to display only TCP/UDP packets, inspect & provide flow graph.

Procedure:

- Select local area Connection in wireshark
- Go to Capture -> option

- Select stop capture automatically 100 packet.
- click start capture
- Search TCP packets in search bar.
- to see flow graph click statistic -> flow graph
- Save packet.

2. create filter to display only ARP packets & inspect packet

Procedure.

- Go capture -> option
- Select stop capture 100 packet
- click start capture
- Search ARP packet in search bar.
- Save packets.

3. Create filter to display only DNS packets & provide flow graph procedure.

- Go capture -> option
- select stop capture automatically 100 pack
- Click start
- Search DNS packet search bar
- flow graph click statistic -> flow graph.
- Save the packet

4. create filter to display only HTTP packet & inspect packet

Procedure.

- select LAN connection in wireshark
- Go capture-> option
- Select stop capture automatically 100 packet
- click start capture.
- Search HTTP packet in search bar
- Save packets

5. Create a filter to display only DHCP packet & inspect

Procedure

- select LAN connection
- Go to capture -> option
- click start capture
- Search DHCP packet in Search bar
- Save packets

<u>student observation:</u>

1. Promiscuous mode is a network interface config in which network card process all packet it sees, this mode is used for packet snif.

2. ARP packet do not contain a transport layer header. ARP Operates directly above data link layer & below network layer in OSI model, and its packet contain header relevant to resolve MAC address from IP.

3. DNS typically uses Datagram Protocol layer at Transport layer for standard query. DNS can use TCP task like Zone packet UDP are too large.

4. The port number used by http protocol is 80.

5. broadcast IP address is special address enable simultaneous message delivery to all device within local network.

Result:

using wireshark the experiment on Packet capture is performed.