Exp No 5

WIRESHARK

AIM:

Experiments on packet capture tool: wireshark.

Packet Sniffer

- Sniffs messages being sent/received by computer
- Store & display contents of various protocol
- passive progs
  - never sends packet itself
  - no packet addressed to it
  - receives a copy of all packets

Packet Sniffer Structure diagnostic tools

- Tcpdump

  Eg. tcpdump -enx host 10.129.41.2 -w exe3.out

- wireshark

  Eg. wireshark -r exe 3.out

Wireshark

Formerly Ethereal, wireshark is a powerful network analyzer that captures packets in real-time and displays them in a human-readable format. it supports:

- Packet capture
- protocol decoding
- Filtering
- color coding for packet types
- Statistics & flow graphs
- troubleshooting & protocol debugging

Use cases
- Network administrators for troubleshooting
- Security engineers for analyzing security issues
- Developers for debugging protocols
- Learners for understanding protocol internals.

Getting started with Wireshark

Installation
- Available for windows, macOS & Linux

Capturing packets
- Launch Wireshark & select a network interface
- Start capturing to see packets appear live in the interface.

Wireshark interface
- Packet line pane
  Shows all captured packets line by line
- Packet details pane
- Packet bytes pane
- Color coding
  helps visually identify packet types.

Color Coding
- different colors represent different protocols
- You can view & customize color rules via View > Coloring rules.

Working with captures

. you can view captures to analyze late or open Sample capture files from wireshark's wiki.

. To analyze specific traffic, use filters by typing expressions like dns, tcp or arp.

Filters and Analysis

Filters help focus on specific types of packets, DNP, HTTPS / ARP traffic.

you can right click a packet & select follow > Tcp stream to see the entire conversion between 2 endpoints.

Flow graph

wireshark can display a flow graph under statistics > Flow Graph to visualize communication sequences between hosts.

lab Procedures

. Capture 100 packets on your ethernet interface & Save them.

. Filter Tcp/UDP packets.

Capture 100 packets, filters for Tcp packets using the Search bar, inspect packets & generate a flow graph via Statistics > Flow graph.

. Filter ARP packets

Capture 100 packets, filter for ARP, inspect &

Save.

- Filter DNS packets

  Capture 100 packets, filter for DNS, generate flow graph, Save.

- Filter HTTP packets

  Capture 100 packets, filter for HTTP, inspect & Save.

- Filter IP/ICMP packets

  Capture 100 packets, filter for ICMP/IP, inspect & Save.

- Filter DHCP packets

  Capture 100 packets, filter for DHCP, inspect & Save.

STUDENT OBSERVATION

1. what is promiscous mode?

promiscuous mode is a network interface mode where the adapter captures all packets on the network segment, not just those addressed to its own MAC address. This allows wireshark to see all network traffic, useful for detailed network analysis.

2. Do ARP packets have transport layers header? Explain.

No, ARP packets do not have a transport layer header because ARP operates at the link layer & is used for resolving IP addresses to MAC addresses. It is not encapsulated inside TCP/UDP.

3. Which transport layer protocol is used by DNS.

DNS primarily uses UDP on port 53 for queries because it is faster & has less overhead. It can also use TCP.

4. What is port no. used by HTTP protocol?

80.

5. What is a broadcast IP address?

A broadcast IP address is an address used to send packets to all hosts on a network segment. For IPv4, the broadcast address is typically the highest address in the subnet. All devices in that subnet will receive packets sent to this address.

22/8/25 9/10