Task 5 : Capture and Analyze Network Traffic Using Wireshark

**Packet capturing:-**

Packet capture (often abbreviated as PCAP) refers to the process of intercepting and logging network traffic that passes through a computer network. This is commonly done using tools and techniques to analyze network communication for troubleshooting, monitoring, or security purposes.

Packet capture is the recording of data packets that are transmitted across a network. Each "packet" is a small chunk of data sent over the network — such as a web request, an email, or a file transfer.

**Tools used :-**

* Wireshark
* Tcpdump
* Tshark
* Netcat
* Snort

**How to capture the packet:-**

**Step-by-Step:**

1. Download and Install Wireshark
   * Website: <https://www.wireshark.org>
2. Open Wireshark
   * You’ll see a list of network interfaces (e.g., Wi-Fi, Ethernet).
3. Select an Interface
   * Choose the one you want to monitor (e.g., Wi-Fi).
4. Start Capturing
   * Click the blue shark fin button to start.
   * Network traffic will start appearing.
5. Stop the Capture
   * Press the red square to stop the session.
6. Analyze Packets
   * Click on any packet to view detailed protocol info (e.g., IP, TCP/UDP, HTTP).
7. Apply Filters
   * Example: http (shows only HTTP traffic), ip.addr == 192.168.1.1, etc.
8. Save the Capture
   * File → Save As → .pcap file format.

**Why Is Packet Capture Important:-**

* Troubleshooting network issues
* Analyzing performance bottlenecks
* Detecting malicious activities
* Verifying secure communication
* Forensics and incident response

**Protocols Analysis:-**

Protocol analysis is the process of examining the structure and behavior of network communication protocols (like HTTP, TCP, DNS, etc.) by capturing and analyzing network packets.

**Why it's important:**

* Identify malformed or malicious traffic
* Ensure protocol compliance
* Detect network attacks or misconfigurations

**Example:**

When you inspect a packet in **Wireshark**, you can see how a request flows through:

Ethernet → IP → TCP → HTTP

**TCP/IP protocols suite:-**

The TCP/IP model is the foundation of how data travels over the internet and most networks. It has 4 layers, each with specific roles.

**Layers :-**

>Application

>Transport

>Internet

>Network Access

**Key Terms:**

* **TCP (Transmission Control Protocol):**
  + Reliable, ordered delivery
  + Uses acknowledgments (ACK)
  + Example: Web page load
* **UDP (User Datagram Protocol):**
  + Fast, no guarantee of delivery
  + Example: Video streaming, VoIP
* **IP (Internet Protocol):**
  + Handles addressing and routing
  + IPv4 and IPv6

**Network Troubleshooting:-**

Troubleshooting network issues by capturing and analyzing packets lets you diagnose:

* Slow performance
* Connection timeouts
* Packet loss or retransmissions
* Unauthorized access

**Common Problem Detected:**

* **DNS Failure**
* **TCP Retransmissions**
* **High Latency**
* **Duplicate IP**

**Filtering in Packet Capture Tools:-**

Packet captures can contain thousands of packets, so filtering is crucial.

**Types of Filters:**

**In Wireshark, filters can be:**

* **Capture Filters (before capturing):**

Set what to capture (based on IP, port, etc.)

port 80 or host 192.168.1.1

* **Display Filters (after capturing):**

Set what to display from captured data

ip.addr == 192.168.1.100

tcp.port == 443

http.request

dns.qry.name == "example.com"

**Real Example:**

You’re troubleshooting slow loading on a website.

* Filter: http.request
* Check request time vs. response time
* Look for TCP retransmissions or delays
* Validate correct DNS resolution