Report On Capture and Analyse Network Traffic Using Wireshark

Report Type: Manual

Performer: Aditya Kamble

Tools: Wireshark (Free) To analyse network traffic using Wireshark

Date: 04/06/2025, Wednesday

Objective: The primary objective of this task was to capture live network packets, analyse them using Wireshark, and identify basic protocols and traffic types.

Tools Used: Wireshark (free) was used for capturing and analysing network traffic.

Methodology:

1. Wireshark was installed and configured for packet capture.
2. Live network traffic was generated by Browse a website and/or pinging a server.
3. Packet capture was initiated and run for approximately one minute.
4. The capture was then stopped, and the collected packets were filtered and analyzed in Wireshark.
5. The captured packets were exported as a .pcap file.

Identified Protocols and Packet Types:

During the analysis, the following protocols and their corresponding packet types were identified within the captured traffic:

TCP (Transmission Control Protocol):

Description: TCP is a core protocol of the Internet Protocol Suite, providing reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating via an IP network.

Packet Types Observed:

- **SYN (Synchronization):** Initial handshake packets used to establish a connection.
- **ACK (Acknowledgement):** Packets used to acknowledge the receipt of data.
- **FIN (Finish):** Packets used to gracefully terminate a connection.
- **PSH (Push):** Packets indicating that the sender wants the application to deliver the data immediately.

 Significance: TCP packets were frequently observed during web Browse activities, signifying the reliable data transfer between the client and web servers for loading web page content.

DNS (Domain Name System):

- **Description:** DNS is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates human-readable domain names (e.g., example.com) into numerical IP addresses.

Packet Types Observed:

- **Standard Query (A record):** Requests to resolve a domain name to an IPv4 address.
- **Standard Query Response (A record):** Responses providing the IP address for a queried domain name.

Significance: DNS queries were observed when initiating connections to websites, as the system needed to resolve the domain names to their respective IP addresses before communication could begin. The document also specifically mentions "What is a DNS query packet?" as an interview question, highlighting its relevance

HTTP (Hypertext Transfer Protocol):

- **Description:** HTTP is an application-layer protocol for transmitting hypermedia documents, such as HTML. It is the foundation of data communication for the World Wide Web.
- **Packet Types Observed:**
  - **GET Requests:** Requests from the client to retrieve information from a web server.
  - **200 OK Responses:** Successful responses from the server indicating the requested resource was found and delivered.
- **Significance:** HTTP packets were prominent during web Browse, demonstrating the client-server interaction for retrieving web pages and their associated resources.

Conclusion: This exercise successfully demonstrated the ability to capture and analyse live network traffic using Wireshark, identifying fundamental protocols like TCP, DNS, and HTTP. Understanding these protocols and their packet types is crucial for network troubleshooting and analysis. The hands-on experience provided valuable insight into packet analysis skills and protocol awareness.