PACKET CAPTURE REPORT

Objective

Analyze the captured network traffic data to identify protocols observed, summarize their roles, and detail example packet structures from each protocol based on the sample.

Tools Used

- Wireshark (for packet analysis)

Protocols Identified

Based on the capture, at least three protocols appear commonly in the data:

- **TCP** (Transmission Control Protocol)
- **DNS** (Domain Name System)
- **UDP** (User Datagram Protocol)

Protocol Summaries

TCP (Transmission Control Protocol)

TCP is connection-oriented, ensuring reliable delivery and ordering of packet data between hosts. It is used for operations like loading web pages, file transfers, and more. Several packets in the capture show TCP headers and data exchanges, such as handshake (SYN, ACK) and payload transmission.

UDP (User Datagram Protocol)

UDP provides a fast, connectionless protocol allowing transmission without guarantees of delivery, ordering, or duplicate protection. It appears in the capture, generally related to DNS queries or lightweight data exchange where speed is critical and reliability can be sacrificed.

DNS (Domain Name System)

DNS is an application-layer protocol using UDP (or sometimes TCP for larger payloads) to resolve human-readable domain names to IP addresses. Multiple DNS query and response packets are present in the capture, showing queries to domains and answers facilitating online access.

Packet Examples

TCP Packet Example

One TCP packet from the capture (truncated for illustration):

- Raw Segment: 0800450000478b65400080060000c0a8012514c02c52fcde01bbf1d34298870053db501800fe03190000170303001a243bb4274e344a3f...
    - Header fields include source/destination addresses, protocol type, sequence numbers, and data payload.

UDP Packet Example

UDP-related example used by DNS:

- Segment: 0800450000435ade4000ff117e03c0a80124e00000fb977614e9002f1aac...
    - Contains UDP header, source/destination ports, and embedded DNS payload.

DNS Packet Example

DNS query with domain and corresponding response:

- Segment: 08080808c21f00350028d216769301000001000000000000066173736574730 36d736e03636f6d0000010001
    - Encapsulates a DNS query for a domain, including transaction IDs and flags.

Packet Filtering

To filter packets in Wireshark:

- Apply protocol filters such as tcp, udp, or dns in the display filter box.