Wireshark Packet Analysis Report

Name: Hemant Singh Chouhan

Task: Cyber Security Internship - Task 5

Objective: Capture and analyze network packets using Wireshark.

Protocols Identified

1. DNS (Domain Name System)

• Purpose: Resolves human-friendly domain names (e.g., google.com) to IP addresses.
• Examples:
  - Standard query A google.com
  - Response: A google.com A 142.250.76.78
• Port: UDP 53
• Packet Info: Source – 192.168.186.4 | Destination – 192.168.186.83 | Length – 70–202 bytes

2. ICMPv6 (Internet Control Message Protocol v6)

• Purpose: Used for diagnostics and neighbor discovery in IPv6.
• Examples:
  - Echo (ping) request and reply
  - Neighbor Solicitation/Advertisement
• Packet Info: Various source/destination IPv6 addresses, length ~118 bytes.

3. ARP (Address Resolution Protocol)

• Purpose: Resolves IP addresses to MAC addresses within local networks.
• Examples:
  - Who has 192.168.186.83? Tell 192.168.186.4
  - 192.168.186.83 is at f6:20:ef:e0:e6:05
• Packet Info: Source – VMware_5b:f3:81 | Destination – Broadcast | Length – 42–60 bytes

Additional Observed Protocol: UDP

• Purpose: Used in DNS, DHCP, MDNS, and other lightweight protocols.
• Port Examples: 53 (DNS), 67/68 (DHCP)
• Nature: Connectionless and faster, but less reliable than TCP.

Summary of Findings

Packets were captured on the eth0 interface of Kali Linux using Wireshark. Filters were applied for DNS, ARP, ICMPv6, and UDP. The analysis revealed typical local network communication such as domain resolution, ping activity, and address resolution. No suspicious or abnormal activity was observed.