Task 5 Report – Network Packet Analysis using Wireshark

Internship Task Title:

Capture and Analyze Network Traffic Using Wireshark

Tools Used

- Wireshark – For live network packet capture and protocol analysis

- Linux Terminal Commands:

  - ping – ICMP packets
  - dig – DNS traffic
  - curl & browser – HTTP/HTTPS traffic
  - ftp, arping, traceroute– Additional protocols

What Was Done (Steps Followed)

• Installed Wireshark on Linux (dual-boot system).

• Captured live packets using the active network interface.

• Generated traffic using terminal and browser to trigger different protocols.

• Applied filters like icmp, http, dns, tcp, tls, arp, ocsp to analyze specific packet types.

• Identified and documented various protocols and their behavior.

• Exported .pcap file and created a summarized report.

Protocols Captured and Analyzed

DNS (Port 53, UDP)

Tool: dig openai.com
Observed Standard query and Standard response
Resolved domain to IP

TCP (Port 80/443)

Observed 3-way handshake (SYN → SYN-ACK → ACK)
Used for HTTP and TLS communication

HTTP (Port 80)

Accessed: http://neverssl.com
Captured GET requests and 200 OK responses
Found headers like X-XSS-Protection: 0 indicating weak protection

TLS/HTTPS (Port 443)

Accessed: https://google.com
Encrypted traffic; visible Client Hello, Server Hello, Certificate

ICMP (Ping)

Tool: ping google.com
Observed Echo request and reply packets

ARP

Tool: arping 192.168.1.1
Captured ARP request/reply resolving IP to MAC

OCSP (Certificate Status Check)

Observed issuerNameHash, serialNumber and weak SHA-1 algorithm in use
OCSP used by browser to verify certificate validity

Security Observations

• X-XSS-Protection: 0 detected → browser-level XSS filter disabled, may allow reflected XSS if server-side sanitization is weak.

• TLS packets used OCSP with SHA-1, which is deprecated and insecure.

• Encrypted traffic not viewable, but handshake behavior observed.

Outcome / Learning

• Successfully performed live packet capture.

• Understood how different protocols behave in real-time.

• Learned how to filter and inspect packets in detail.

• Developed awareness about security headers, encrypted communication, and protocol usage.

• Explored browser and terminal-based traffic generation for testing.

Skills Gained

• Packet analysis using Wireshark

- Hands-on with multiple network protocols
- Understanding basic vulnerabilities (XSS, insecure headers, SHA-1)
- Use of filters and protocol dissection