Network Traffic Scanning Using Wireshark

Presented by *: Pankaj Singh*

Roll no *: 2023A7R058*

Department: *CSE cyber security*

What is Wireshark?

Wireshark is a free and open-source packet analyzer used for network troubleshooting, analysis, and education.

Key Features:

Captures live traffic from network interfaces

Deep packet inspection (OSI Layer 2–7)

Filters, decodes, and analyzes hundreds of protocols

Setting Up and Capturing Traffic

Steps to Capture Traffic:

Select correct network interface

Apply capture filters (optional)

Stop capture after desired time

Capture Filters vs Display Filters:

Capture Filter: Limits data being collected

Display Filter: Focuses view after capture

Analyzing Captured Packets

Analyzing Captured Packets

Common Protocols to Analyze:

HTTP/HTTPS: Web traffic

DNS: Domain name lookups

TCP/UDP: Transport-layer traffic

ICMP: Ping and diagnostics

Real-World Use

Cases

1

Use Case 1:
Detecting malicious traffic (e.g., malware callbacks)

2

Use Case 2:
Troubleshooting slow network performance

3

Use Case 3:
Verifying encrypted vs unencrypted data flow

Conclusion:

Wireshark is a powerful tool for seeing inside your network. Mastering it strengthens both defense and troubleshooting.

Best Practices:

Use filters to reduce noise

Save capture files for analysis

Always capture with legal permission

Mask sensitive info if sharing