

❖ **Assignment No: 4**

❖ **Problem Statement:** Configure and demonstrate use of vulnerability assessment tool like Wireshark or Snort

❖ **Objectives:**

- To capture and analyze network traffic using Wireshark.
- To identify potential vulnerabilities or suspicious activities in the network.
- To learn how network protocols work and how to filter and inspect packets for forensic investigation.

❖ **Hardware Requirements:** Intel Core i3 or higher Processor, 4 GB RAM, 250 GB Hard Disk, Network interface card capable of packet capture (Wi-Fi or Ethernet)

❖ **Software Requirements:** Windows 10 / Linux / macOS Operating System, Wireshark Application

❖ **Theory:**

• **Network Traffic and Vulnerability Assessment**

Wireshark is a network protocol analyzer that allows the capture and detailed inspection of network packets. It is a key tool for vulnerability assessment because it helps identify misconfigurations, suspicious activity, and protocol-level security weaknesses.

i. Packet Capture

- Wireshark captures all traffic passing through the selected network interface.
- Each packet contains metadata including source/destination IPs, ports, protocol type, and payload data.
- Captured packets can be filtered by protocol (http, tcp, icmp, etc.) or by IP addresses to focus on relevant traffic.

ii. Packet Analysis

- Packets can be analyzed to detect:

- Unauthorized or suspicious connections
 - Open ports or unusual services
 - Malformed packets or protocol violations
- Packet inspection is useful in cybersecurity investigations and network troubleshooting.

iii. Filtering and Protocol Analysis

- Filters help narrow down captured traffic:
 - Example: `ip.addr == 192.168.1.10` (traffic to/from a specific host)
 - `tcp.port == 80` (HTTP traffic)
- Protocol analysis helps understand application behavior, network efficiency, and detect anomalies.

iv. Applications in Cybersecurity

- Detecting unauthorized access attempts
- Monitoring malicious traffic
- Performing penetration testing and vulnerability assessment
- Supporting network forensic investigations

❖ Conclusion:

Wireshark allows real-time capture and analysis of network packets, helping identify vulnerabilities and suspicious activity in a network. By using filters, protocol analysis, and inspection of packet details, network administrators and cybersecurity professionals can investigate network issues, detect attacks, and secure the network effectively.

❖ Wireshark Captures:



