## ****Sniffing Attack Using Wireshark****

### ****1. Overview****

A **sniffing attack** involves intercepting network traffic to analyze packets for sensitive data. **Wireshark**, a powerful packet analyzer, is used for capturing and inspecting network packets in real time.

### ****2. Step-by-Step Guide****

#### ****Step 1: Install Wireshark****

Download and install Wireshark from [Wireshark’s official website](https://www.wireshark.org/).

Follow the installation wizard and ensure necessary permissions are granted.

#### ****Step 2: Select a Network Interface****

Open Wireshark and choose the appropriate network interface (Wi-Fi or Ethernet).

Click **Start Capture** to begin monitoring network traffic.

#### ****Step 3: Capture and Analyze Network Traffic****

Allow network traffic to flow for a few minutes.

Stop the capture and apply filters such as http, tcp, or dns to isolate specific types of packets.

#### ****Step 4: Identify Potential Security Issues****

Look for **unencrypted credentials** in HTTP packets.

Analyze TCP handshakes to detect potential **man-in-the-middle attacks**.

Examine DNS queries for possible **DNS spoofing attempts**.

### ****3. Findings & Observations****

Identified **unencrypted credentials** transmitted over HTTP.

Captured DNS queries and responses.

Observed TCP handshakes and connection details.

### ****4. Mitigation Strategies****

🔹 Use **encrypted communication protocols** like HTTPS and VPNs. 🔹 Implement **firewalls and intrusion detection systems**. 🔹 Restrict **unauthorized access** to network traffic.

