# LAB-03

1. **As part of a penetration testing engagement for a client, you're tasked with evaluating the security of their internal network. You suspect that sensitive data might be leaking from one of their development servers due to a potential misconfiguration or a compromised machine within their network. To investigate further, you plan to intercept network traffic using Wireshark to identify any unauthorized data transfers.**

   Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security. Networks must be monitored to ensure smooth operations and security. Popular with academic institutions, government agencies, corporations and nonprofits, Wireshark is one such tool that can offer an in-depth view into network activities, diagnose network performance issues or identify potential security threats.

   Wireshark -Snipping
   Intercept target machine traffic(Metaspoiltable2 VM) with Wireshark
   • Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.
   • Open Kali Linux and navigate to Applications -> Snipping & Spoofing -> Wireshark.
   • Select the interface (eth0) to capture network traffic.
   • Access the browser on Kali Linux and enter the IP address of the Metasploitable2 VM (e.g., 192.168.62.129) to open the Mutillidae website.
   • Navigate to Mutillidae page and proceed to the login page.
   • Enter random credentials (e.g., username: admin, password: 12345) and attempt to log in, resulting in a login failure message.
   • Switch to Wireshark, where traffic interception has begun.
   • In the filter bar, type "http" and select the http with post stream contains login.php page.
   • Right-click on HTTP traffic, choose "Follow," then "HTTP stream" to open a new window.
   • The new window displays intercepted traffic containing the username and password entered on the DVWA login page, showcasing successful traffic interception using Wireshark.