Day 113

Topic: Sniffing & Spoofing

Objective: To intercept network data and impersonate other machines using Man-in-the-Middle (MitM) techniques.

Theoretical Concepts:
We explained ARP Spoofing (poisoning the ARP cache of a target to route their traffic through the attacker's machine) and DNS Spoofing. This allows an attacker to sniff passwords even on a switched network.

Practical Work:
We used **Ettercap** to perform ARP Poisoning between a Windows VM (victim) and the Gateway. Once the MitM position was established, we opened **Wireshark** and captured the traffic. We could see the victim's HTTP requests. We also demonstrated DNS spoofing, redirecting the victim's request for "facebook.com" to our malicious IP.

Tools Used: Wireshark, Ettercap.

Outcome: Successfully executed a Man-in-the-Middle attack and captured data flow on a local network.