**Experiment No: 5**

**Aim:**

To demonstrate an **ARP Poisoning Attack** using Ettercap and understand how it leads to a **Man-in-the-Middle (MITM)** scenario.

**Step 1: Open Ettercap**

* Launch the Ettercap tool on your system.
* Ettercap is used for network traffic interception and analysis.

**Step 2: Select ‘Unified Sniffing’ from the Sniff Menu**

* Click on the **“Sniff”** menu at the top.
* Choose **“Unified Sniffing”**, which allows you to start monitoring network traffic on a selected interface.

**Step 3: Choose a Network Interface**

* A window will pop up asking which network interface you want to use.
* Select the default option (usually **eth0** or **wlan0**) and click **“OK”**.
* Ettercap starts capturing packets from that network.

**Step 4: Scan for Hosts**

* Go to the **“Hosts”** menu.
* Select **“Scan for Hosts”** to detect all devices currently connected to the same network.

**Step 5: View Hosts List**

* Again, under the **“Hosts”** menu, click on **“Hosts List”**.
* This displays the list of IP addresses and MAC addresses of all discovered devices.

**Step 6: Set Targets for the Attack**

* In the hosts list window:
  + Click on a device (like a victim's computer) and choose **“Add to Target 1”**.
  + Then select another device (usually the router or gateway) and choose **“Add to Target 2”**.
* This setup allows you to intercept communication between these two devices.

**Step 7: Launch ARP Poisoning**

* Go to the **“MITM”** (Man-In-The-Middle) menu.
* Select **“ARP Poisoning”** from the dropdown.
* This will launch the attack that tricks both devices into thinking your system is the other one.

**Step 8: Sniff Remote Connections**

* A small window will appear.
* Tick the checkbox **“Sniff remote connections”** and click **“OK”**.
* Ettercap will now intercept and display any data (such as passwords or messages) being exchanged between the two target devices.

This attack demonstrates how **ARP spoofing** can redirect traffic through an attacker’s system, showing the importance of encryption and secure protocols in network communication.