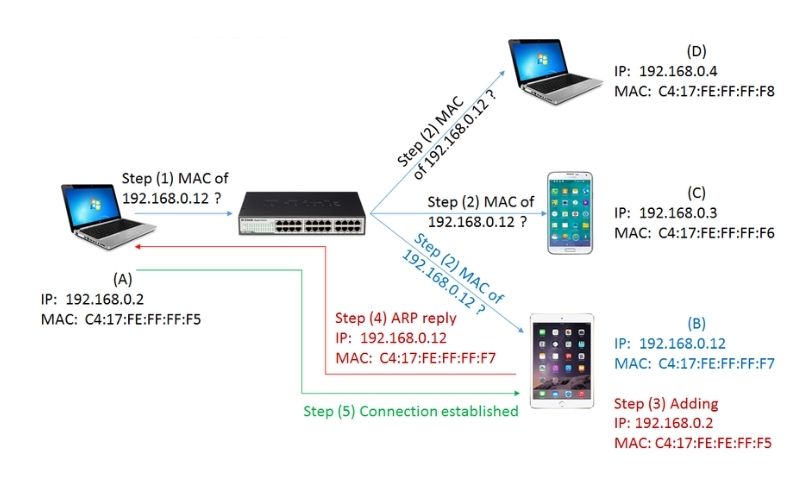
**Experiment 6 :**

Perform the following using appropriate tools:

1. ARP Poisoning
2. DNS Poisoning
3. **ARP Poisoning**

**Aim:**

The primary aim of ARP poisoning (also called ARP spoofing ) is to associate the attacker's MAC address with the IP address of another device on the network, typically the default gateway. This allows the attacker to intercept traffic intended for that device, effectively becoming a man-in-the-middle, and potentially modifying or stopping it.



**Procedure:(here using ettercap tool)**

**Steps:**

1. Open kali-Linux
2. Click on applications
3. Click on sniffing and spoofing
4. Click on ettercap
5. Scan for hosts
6. Open host lists
7. Host1 add to target1
8. Host2 add to target 2
9. Click on MITM(Man-in-the-Middle)menu
10. Click on ARP poisoning
11. Select sniff remote connections
12. Click on OK
13. Poisoned MAC address

**Effects of an ARP Poisoning Attack?**

* **Data Interception:**

ARP poisoning allows an attacker to intercept unencrypted network traffic, potentially revealing sensitive information like login credentials, payment details, or personal data.

* **Data Modification:**

An attacker can modify unencrypted traffic, altering data transmitted between devices and potentially leading to misinformation or corruption.

* **Denial of Service (DoS):**

By redirecting network traffic to an attacker's machine, they can disrupt or block communication, causing network connectivity issues and impacting productivity.

* **Unauthorized Access:**

An attacker can use ARP poisoning to steal login credentials from network traffic and gain unauthorized access to systems and applications.

* **Network Disruption:**

ARP poisoning can disrupt normal network operation by manipulating the network's ARP table, making it difficult or impossible for devices to communicate.

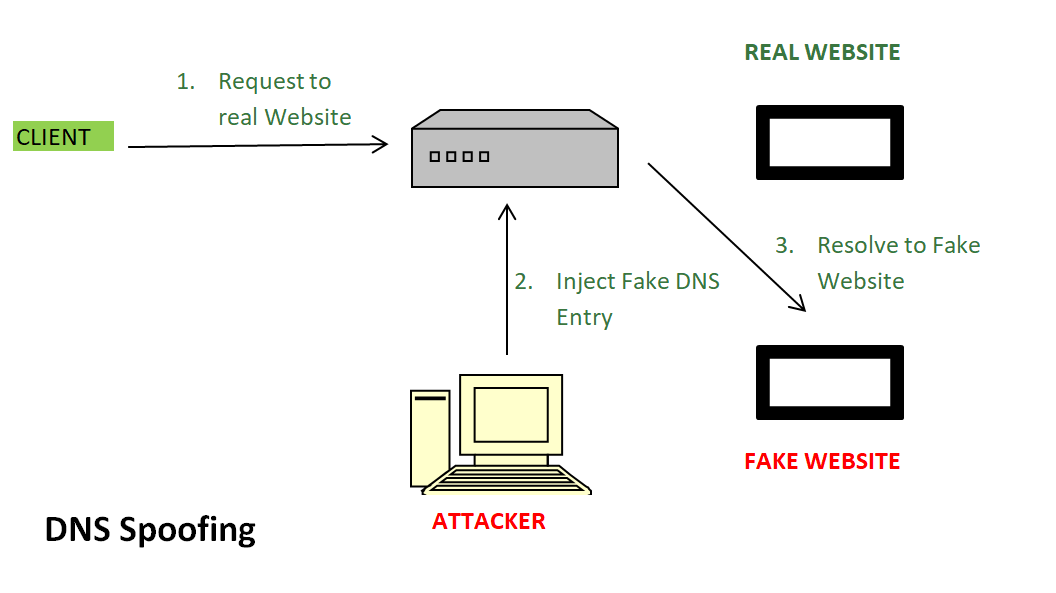
* **Facilitating Other Attacks:**

ARP poisoning is often used as a stepping stone for more sophisticated attacks like man-in-the-middle (MITM) attacks, session hijacking, or malware distribution.

**b) DNS Poisoning**

**Aim:**

The primary goal of DNS poisoning, or DNS spoofing, is to redirect users to malicious or fraudulent websites. By manipulating DNS records attacker gets between the web browser you are using and the DNS . They then use a tool to alter the information in the cache on your device, as well as the information on the DNS server. You then get redirected to a malicious site.



**Procedure:(here using bettercap tool)**

**Steps:**

1. Open kali-Linux
2. Open terminal in root mode (sudo su)
3. Type bettercap(If it is not installed install it with command sudo apt-get install bettercap)
4. Type help
5. Check Module open status
6. Type net.probe on
7. set arp.spoof.fullduplex true
8. set dns.spoof.address kali-Linux IP
9. set dns.spoof.domains ([www.http2demo.io](http://www.http2demo.io))
10. set arp.spoof target windows IP
11. arp.spoof on
12. dns.spoof on

**Protecting Against DNS Poisoning**

* **Implement DNSSEC(DNS security extensions)**

DNSSEC is a suite of security protocols that applies cryptographic validations to DNS

records.

* Always encrypt data

This offers an added layer of protection by preventing hackers who might be able to

intercept that data from doing anything with it.

* Enable secure DNS configurations

you can configure your DNS servers so that they don’t rely heavily on relationships with any other DNS servers. Doing so makes it far more difficult for hackers to establish a connection via their own DNS server

* Regularly run system updates

Making sure you always run these updates so that you use the most recent version of your DNS is extremely important,

* Introduce strong detection protocols

The best detection protocols use regular monitoring to look for certain warning signs

* Use DNS over HTTPS (DoH)

DoH encrypts DNS queries, making it more difficult for attackers to intercept or modify DNS traffic. This added layer of encryption helps protect against attacks that rely on eavesdropping or manipulating DNS responses.