ARP (Address Resolution Protocol) spoofing is a technique used by attackers to manipulate the ARP cache of a network, leading to potential security vulnerabilities. ARP is responsible for mapping IP addresses to MAC addresses, allowing devices on a local network to communicate with each other.

One-Way ARP Spoofing:

Scenario:

In a one-way ARP spoofing attack, the attacker sends false ARP replies to the target device, associating the attacker's MAC address with the IP address of the victim. However, the attacker does not update its own ARP cache.

Process:

The attacker sends forged ARP replies to the target, claiming that it has the IP address of the victim device.

The target device updates its ARP cache, associating the attacker's MAC address with the victim's IP address.

The attacker can intercept or manipulate the traffic between the target and other devices but may not be the final destination for the traffic.

Concerns:

This form of ARP spoofing may be less stealthy compared to two-way ARP spoofing, and the attacker's activities may be more easily detected by network monitoring tools.

Two-Way ARP Spoofing (Man-in-the-Middle - MITM):

Scenario:

In a two-way ARP spoofing attack, the attacker manipulates the ARP cache of both the victim and another device (often a router). This allows the attacker to intercept and manipulate the traffic between the two devices.

Process:

The attacker sends forged ARP replies to the victim, associating the attacker's MAC address with the IP address of the router (default gateway).

Simultaneously, the attacker sends forged ARP replies to the router, associating the attacker's MAC address with the IP address of the victim.

Both the victim and the router update their ARP caches, believing that the attacker's MAC address is associated with the other party's IP address.

The attacker can intercept, modify, or eavesdrop on the communication between the victim and the router.

Concerns:

Two-way ARP spoofing is more sophisticated and can be harder to detect because the attacker actively manipulates the communication between two parties. It enables various attacks, including packet sniffing, session hijacking, and more.

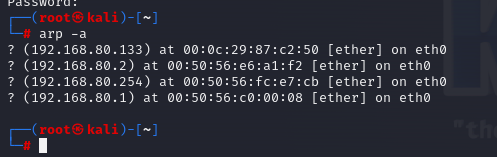
Scenario: My kali m/c is attacker. So I will poison arp entry in victim and gateway.

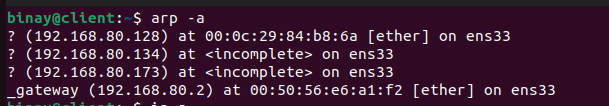
So gateway think, I am victim and Victim think I am gateway.

So in mitm attack, attacker broadcast continously arp msgs to victim and gateway. So victim add entry attacker as a gateway in his arp table and Gateway will add entry attacker as a victim.

So In victim’s arp table, after mitm attack, The ip of gateway will bind to mac addr of Attacker.

And same in gateway’s arp table, ip of victim will bind to attacker’s mac address.

Arp Table of attacker:

Arp table of victim:-

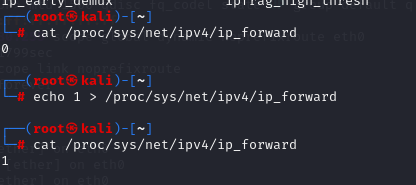
On attacker m/c:

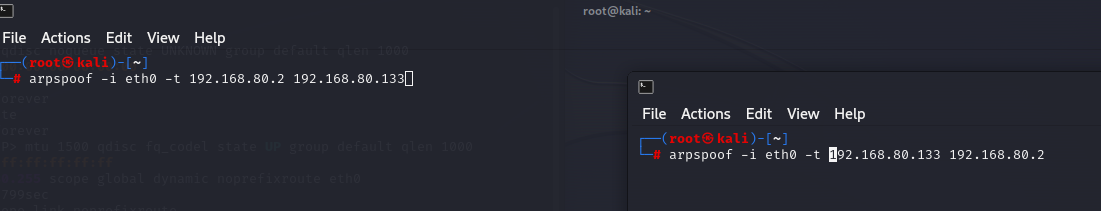
On one terminal, I will continuously broadcast arp msgs for vicitim pretending as a gateway, on 2nd terminal I will continuously broadcast arp msgs for gatway pretending as a victim. On 3rd terminal, I will monitor traffics of victim. And try to modify packets.

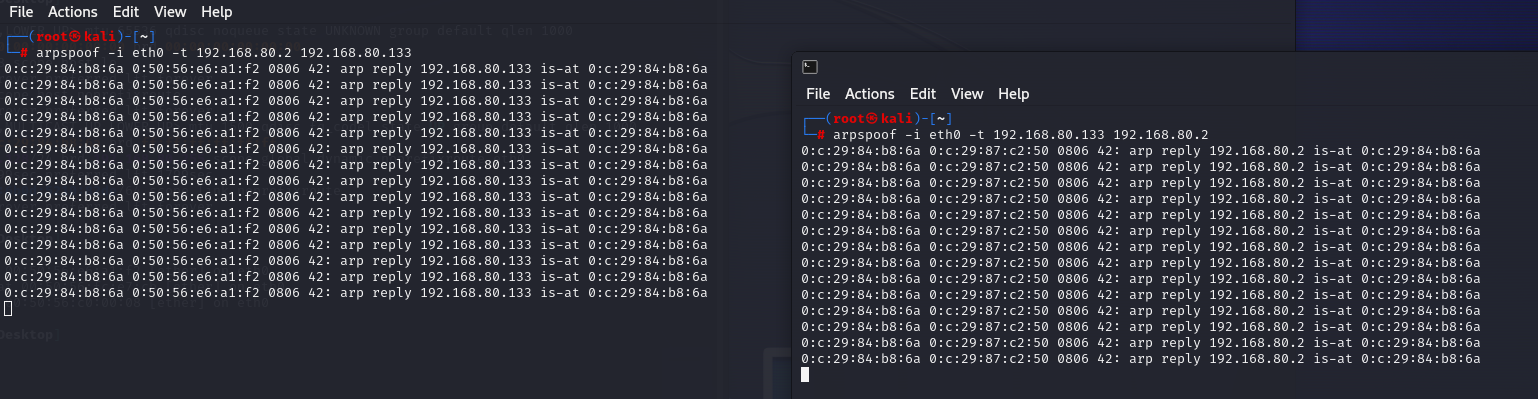
In this practical, we can see only http traffic.

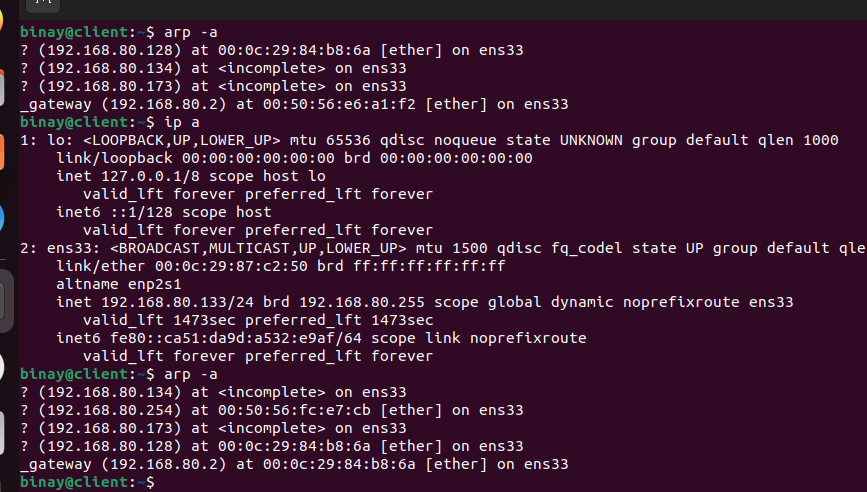
Install dsniff

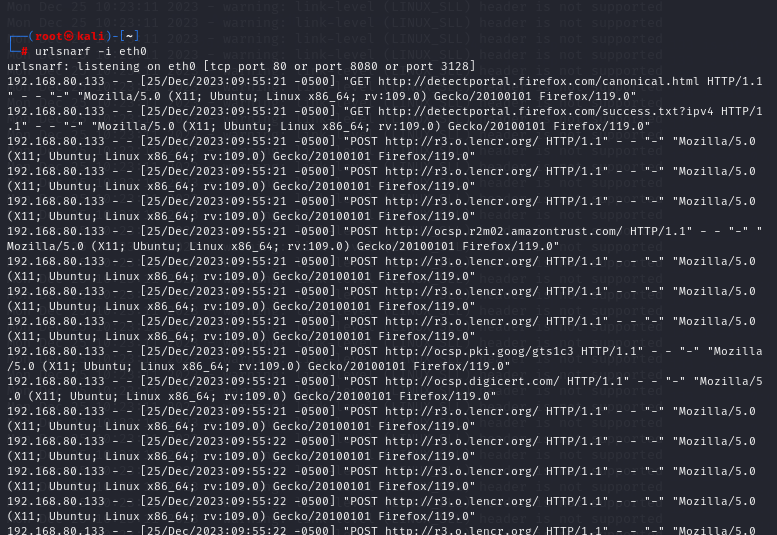
#apt install dsniff -y

Enable ip forwarding:-





See the mac address before and after mitm

Using urlsnarf, we can see which websites victim is visiting and using driftnet we can capture http websites’s images.

We can use Ettercap tool too for mitm