

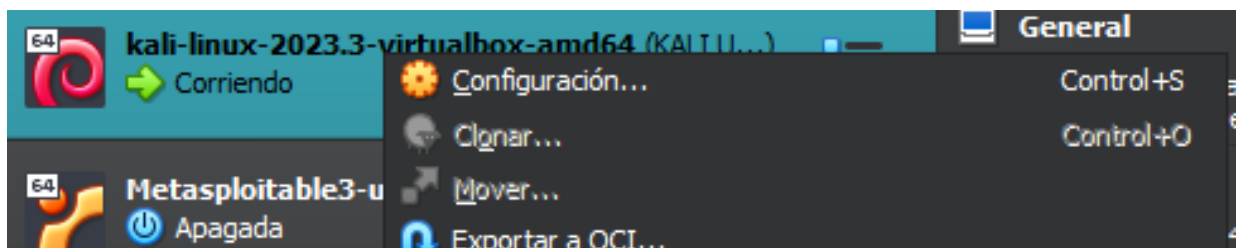
MITM – ETTERCAP

ARP POISONING.

Requerimientos:

Dos máquinas; Víctima y la que usaremos como la Man in the middle (MITM)

Lo podemos hacer clonando la máquina main de Kali en el VirtualBox.



Hacemos click derecho en la máquina a clonar. IMPORTANTE: tiene que estar apagada.

Pasos.

1. Encender ambas máquinas y hacerles sus correspondiente ifconfig para averiguar la IP de cada una.

IP Máquina MITM.

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BR
inet 192.168.1.23 net
```

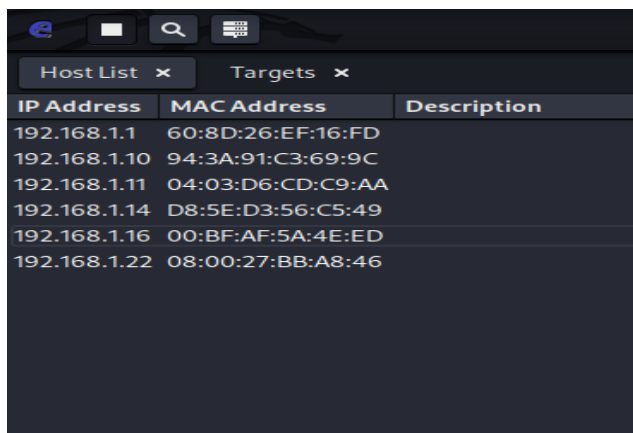
IP Máquina víctima.

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,B
inet 192.168.1.22 n
```

2. Iniciamos Ettercap en la máquina donde haremos de MITM, en mi caso, en mi máquina principal (main) con el usuario root.

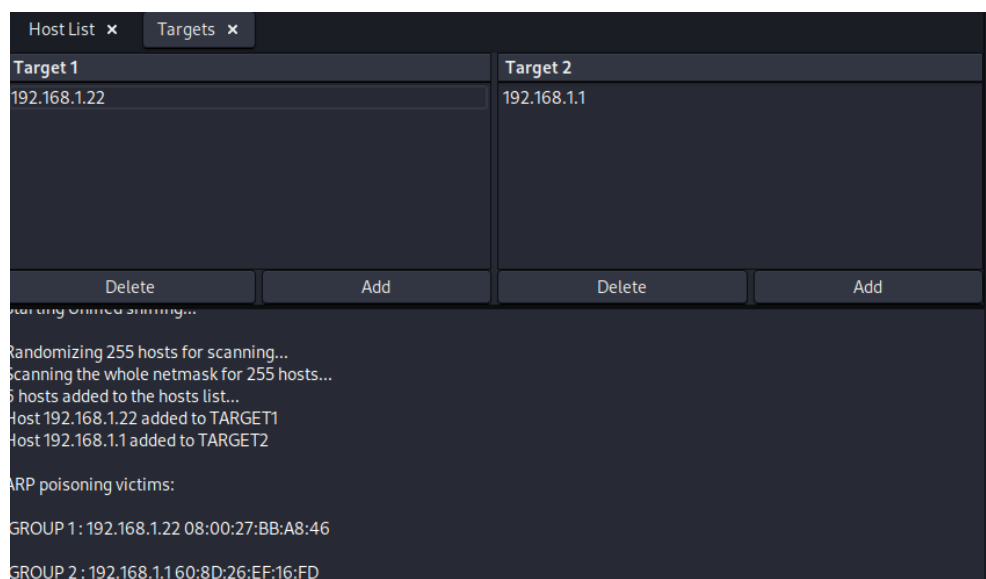
```
$ sudo su
[sudo] password for kali:
(root@kali)~# ettercap -G
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

3. Fijamos como objetivo (target1) la víctima y la dirección del router (target2) para hacer el Sniffing.



IP Address	MAC Address	Description
192.168.1.1	60:8D:26:EF:16:FD	
192.168.1.10	94:3A:91:C3:69:9C	
192.168.1.11	04:03:D6:CD:C9:AA	
192.168.1.14	D8:5E:D3:56:C5:49	
192.168.1.16	00:BF:AF:5A:4E:ED	
192.168.1.22	08:00:27:BB:A8:46	

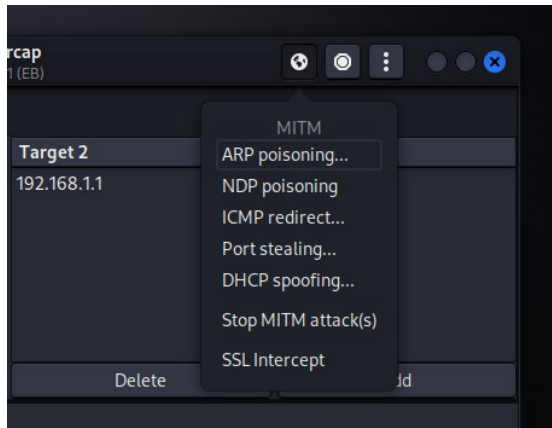
En este caso, seleccionaremos como target1 la ip 192.168.1.22 y como target2 la dirección del router 192.168.1.1.



Target 1	Target 2
192.168.1.22	192.168.1.1

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
\$ hosts added to the hosts list...
Host 192.168.1.22 added to TARGET1
Host 192.168.1.1 added to TARGET2
ARP poisoning victims:
GROUP 1 : 192.168.1.22 08:00:27:BB:A8:46
GROUP 2 : 192.168.1.1 60:8D:26:EF:16:FD

4. Después de seleccionarlal, ejecutamos el ataque ARP POISONING.



Click en ok para iniciar el ataque.

5. Para observar que lo hemos hecho adecuadamente ejecutamos cualquier página con el protocolo HTTP en el que pida una autenticación. He elegido esta:

<http://httpbin.org/basic-auth/foo/bar>

```
HTTP : 34.235.39.169:80 -> USER: foo PASS: bar INFO: httpbin.org/basic-auth/foo/bar
```

Nos muestra las credenciales con las que accedemos a la página HTTP.

JCN