MITM – ETTERCAP

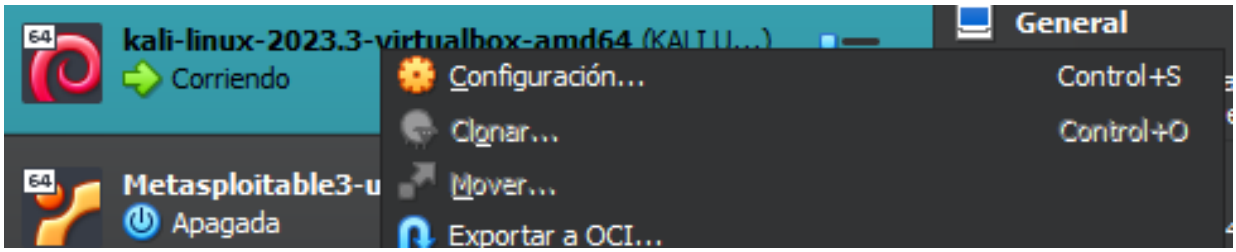
ARP POISONING.

PROTOCOLO FTP.

Requerimientos:

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

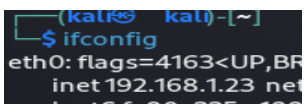
Lo podemos hacer clonando la máquina main de Kali en el VirtualBox. Además de cambiar las direcciones MAC en ajustes de red>Avanzado.

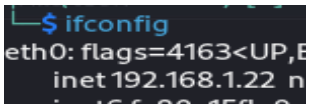


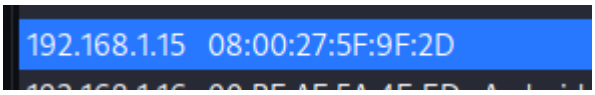
Hacemos click derecho en la máquina a clonar. IMPORTANTE: tiene que estar apagada.

Pasos.

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

   IP Máquina MITM. 

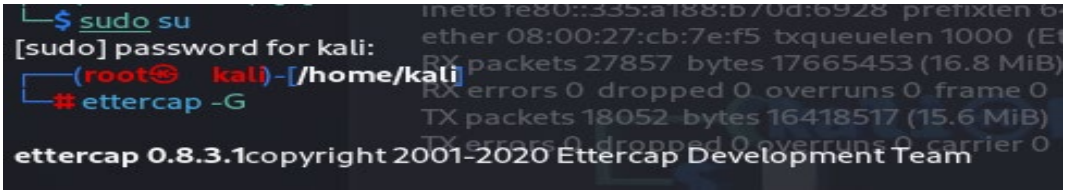
IP Máquina servidor. 

IP Máquina cliente. 

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.

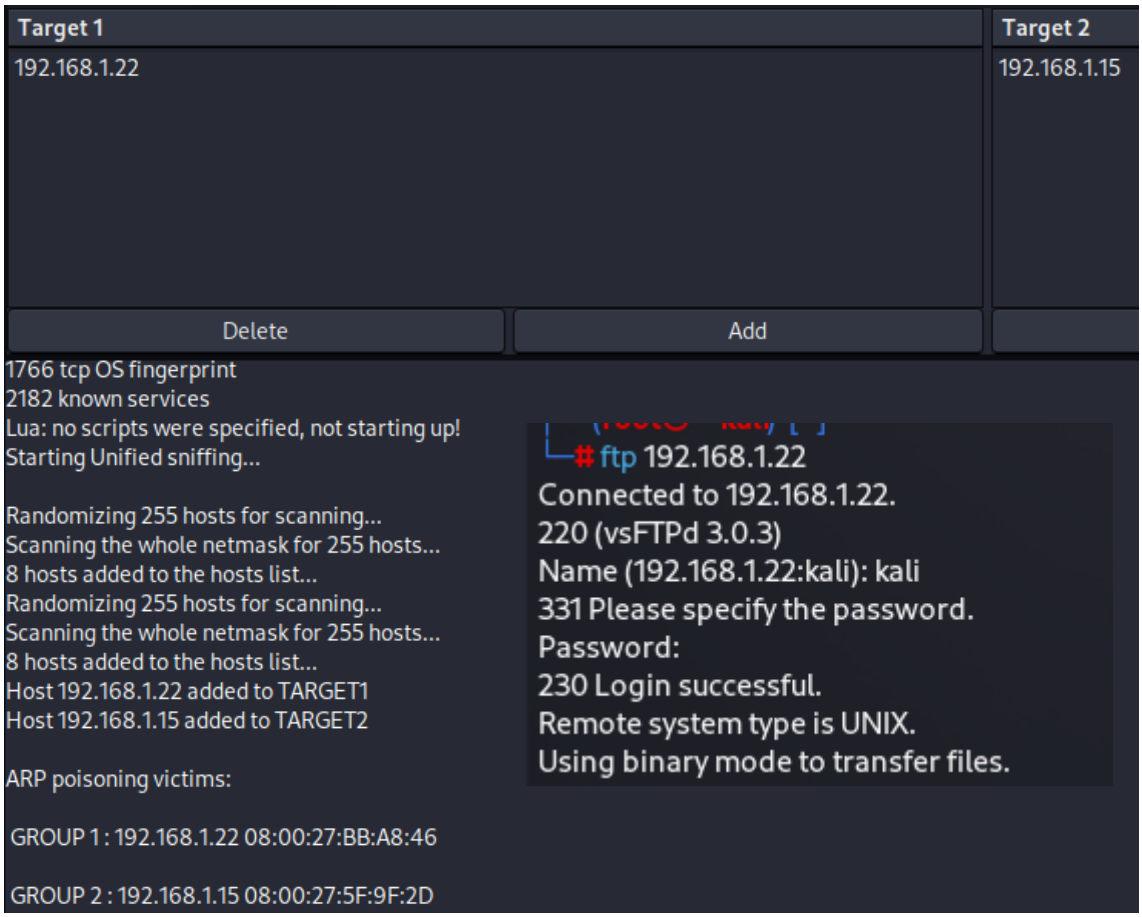


   En la siguiente imagen podemos ver:

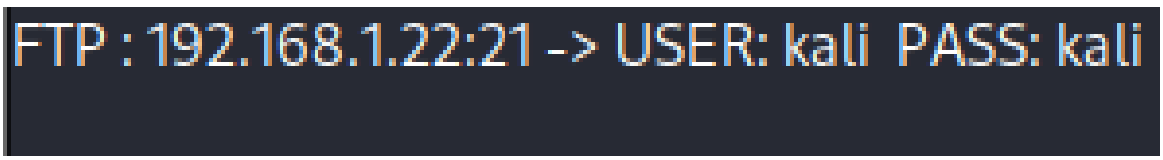
   TARGET1 – IP DEL SERVIDOR

   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.



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



JCN