# THM – Attacktive Directory

**Objetivos:**

- Recopilar información detallada sobre usuarios, grupos y recursos compartidos.
- Descifrar contraseñas y hashes mediante técnicas como el uso de hashcat y Kerbrute.
- Utilizar técnicas como "pass the hash" para autenticarse como usuarios con mayores privilegios.

**Requisitos:**

- Sistema Operativo Kali Linux
- Software Kerbrute
- Software Impacket
- Software Hashcat
- Software Smbclient
- Software Evil-winrm

**Categoria:**
Windows, Active Directory, Kerberos, SMB

**Dificultad:**
Media

## Comandos y Parámetros a Emplear:

**Linux**

| Comando | Descripción |
|---|---|
| ping | Se utiliza para verificar la conectividad entre dos nodos en una red. |
| cat | Se utiliza para concatenar y mostrar el contenido de archivos. |
| cd | Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos. |
| echo | Imprime mensajes o variables en la pantalla. |
| base64 | Se utiliza para codificar o decodificar datos en formato Base64. |

**Nmap**

| Comando | Descripción |
|---|---|
| -sC | Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo. |
| -sV | Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo. |

**Kerbrute**

| Comando | Descripción |
|---|---|
| -h | Muestra la ayuda o información sobre el uso del programa. |
| --dc | Especifica el controlador de dominio (Domain Controller) al que se dirigirá el ataque de fuerza bruta. |
| -d | Especifica el dominio al que se dirigirá el ataque de fuerza bruta. |

**Hashcat**

| Comando | Descripción |
|---|---|
| -m | Se utiliza para especificar el tipo de hash que se está intentandoatacar. |

**Impacket**

| Comando | Descripción |
|---|---|
| -no-pass | Se utiliza para indicar que no se proporcionará una contraseña al realizar una autenticación. |
| -dc | Especifica el controlador de dominio (Domain Controller) al que se dirigirá la solicitud. |
| -ip | Especifica la dirección IP del objetivo al que se realizarán las operaciones. |
| -just-dc | Indica a la herramienta que solo se debe interactuar con el controlador de dominio. |

**Smbclient**

| Comando | Descripción |
|---|---|
| -L | Se utiliza para listar recursos compartidos disponibles en un servidor SMB sin autenticarse. |
| -U | Se utiliza para especificar el nombre de usuario que se utilizará durante la autenticación en el servidor SMB. |

**Evil-winrm**

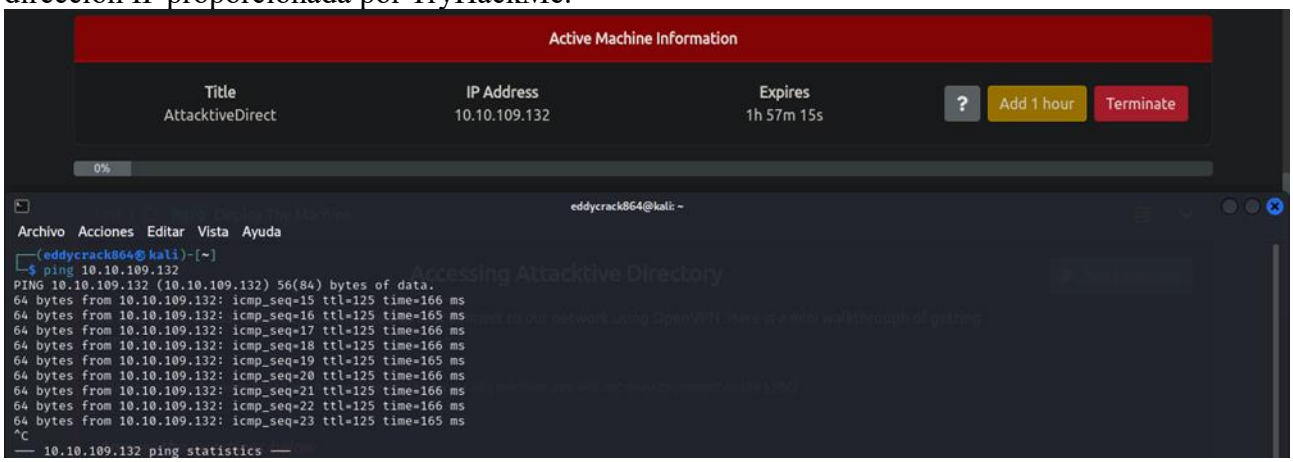
| Comando | Descripción |
|---|---|
| -h | Muestra la ayuda o información sobre el uso del comando. |
| -i | Especifica la dirección IP del sistema Windows al que te estás conectando a través de WinRM. |
| -H | Se utiliza para especificar el host (dirección IP o nombre de host). |

**Windows**

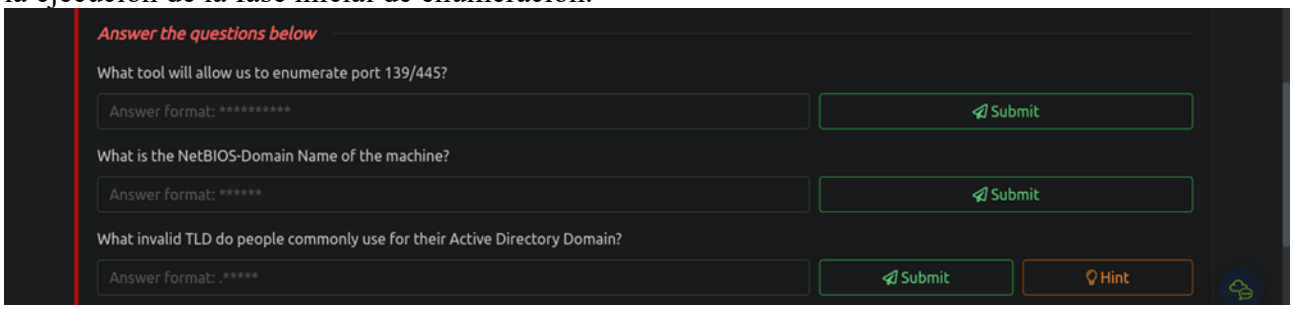
| Comando | Descripción |
|---|---|
| cd | Cambia el directorio actual del usuario en el sistema de archivos. |
| dir | Muestra una lista de archivos y subdirectorios en el directorio actual. |
| type | Muestra el contenido de un archivo de texto en la consola. |

## Desarrollo:

1. Se procede a validar la conectividad mediante la ejecución de un comando de ping dirigido a la dirección IP proporcionada por TryHackMe.



2. En el inicio de la máquina, se despliega un conjunto de tres interrogantes que se abordarán durante la ejecución de la fase inicial de enumeración.



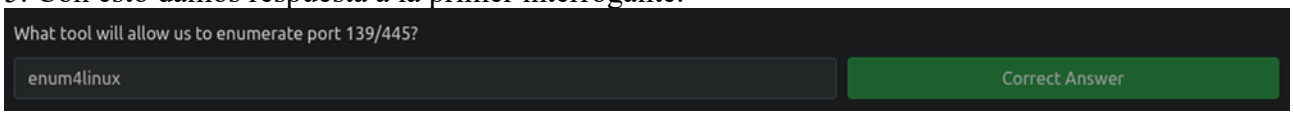

3. Se realizó una enumeración de puertos mediante el empleo de nmap, integrando los parámetros "-sV" y "-sC" para obtener información detallada sobre los servicios y ejecutar scripts de automatización de detección de vulnerabilidades. La salida reveló una gran cantidad de servicios, incluyendo, entre otros, DNS, IIS, Kerberos, RPC, netbios, y Active Directory.

```
┌──(eddycrack864㉿kali)-[~]
└─$ nmap -sC -sV 10.10.109.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:25 -05
Nmap scan report for 10.10.109.132 (10.10.109.132)
Host is up (0.17s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-12-08 13:26:06Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: spookysec.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM-AD
|   NetBIOS_Domain_Name: THM-AD
|   NetBIOS_Computer_Name: ATTACKTIVEDIREC
|   DNS_Domain_Name: spookysec.local
|   DNS_Computer_Name: AttacktiveDirectory.spookysec.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-12-08T13:26:18+00:00
| ssl-cert: Subject: commonName=AttacktiveDirectory.spookysec.local
| Not valid before: 2023-12-07T12:59:17
|_Not valid after:  2024-06-07T12:59:17
|_ssl-date: 2023-12-08T13:26:26+00:00; 0s from scanner time.
Service Info: Host: ATTACKTIVEDIREC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

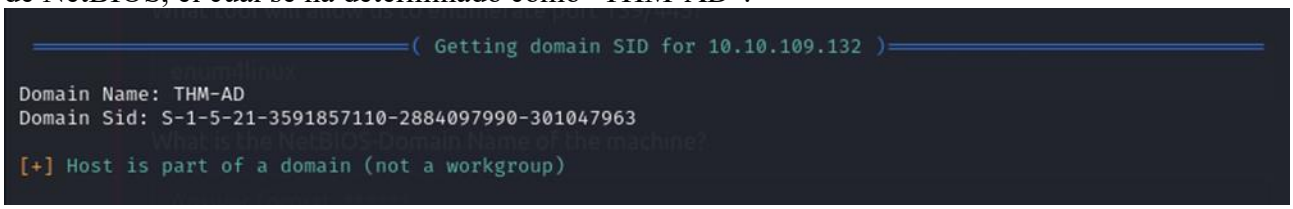
4. El protocolo Server Message Block (SMB) opera a través de los puertos 139 y 445. Para llevar a cabo una enumeración exhaustiva de SMB, se emplea la herramienta especializada enum4linux.

```
┌──(eddycrack864㉿kali)-[~]
└─$ enum4linux 10.10.109.132
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Dec  8 08:29:43 2023

 ========================( Target Information )========================

Target ........... 10.10.109.132
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

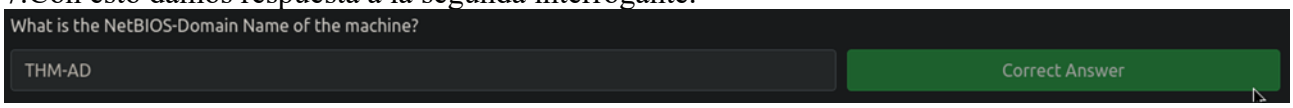
5. Con esto damos respuesta a la primer interrogante.



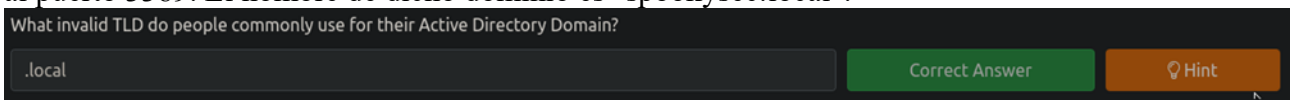
6. Dentro de la salida obtenida tras la aplicación de enum4linux, se identifica el Nombre de Dominio de NetBIOS, el cual se ha determinado como "THM-AD".



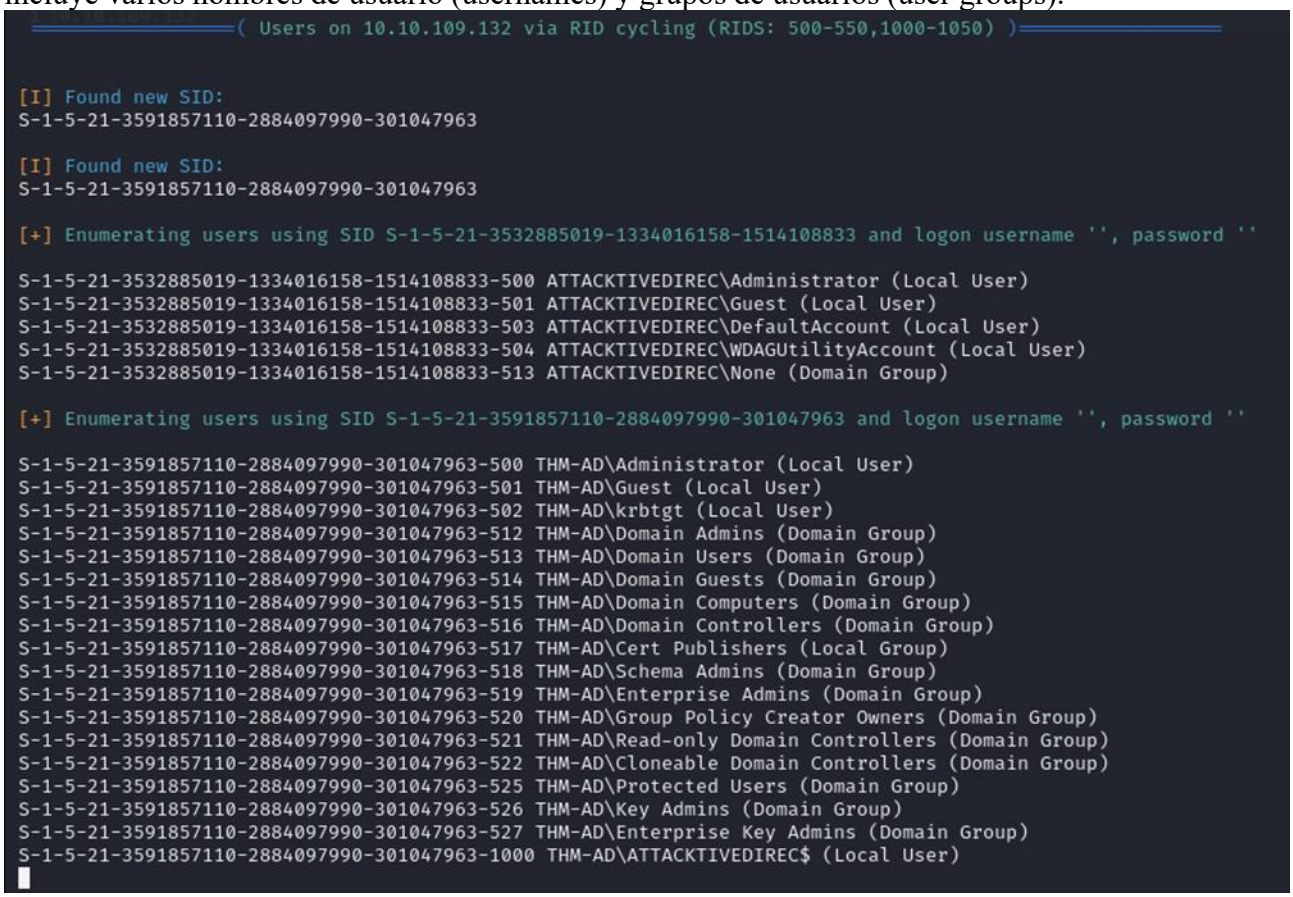

7.Con esto damos respuesta a la segunda interrogante.




8. Las siglas TLD corresponden a "Dominio de Nivel Superior". Al revisar una vez más los resultados de nmap, se observa que el dominio de Active Directory (AD) se menciona en la información relativa al puerto 3389. El nombre de dicho dominio es "spookysec.local".



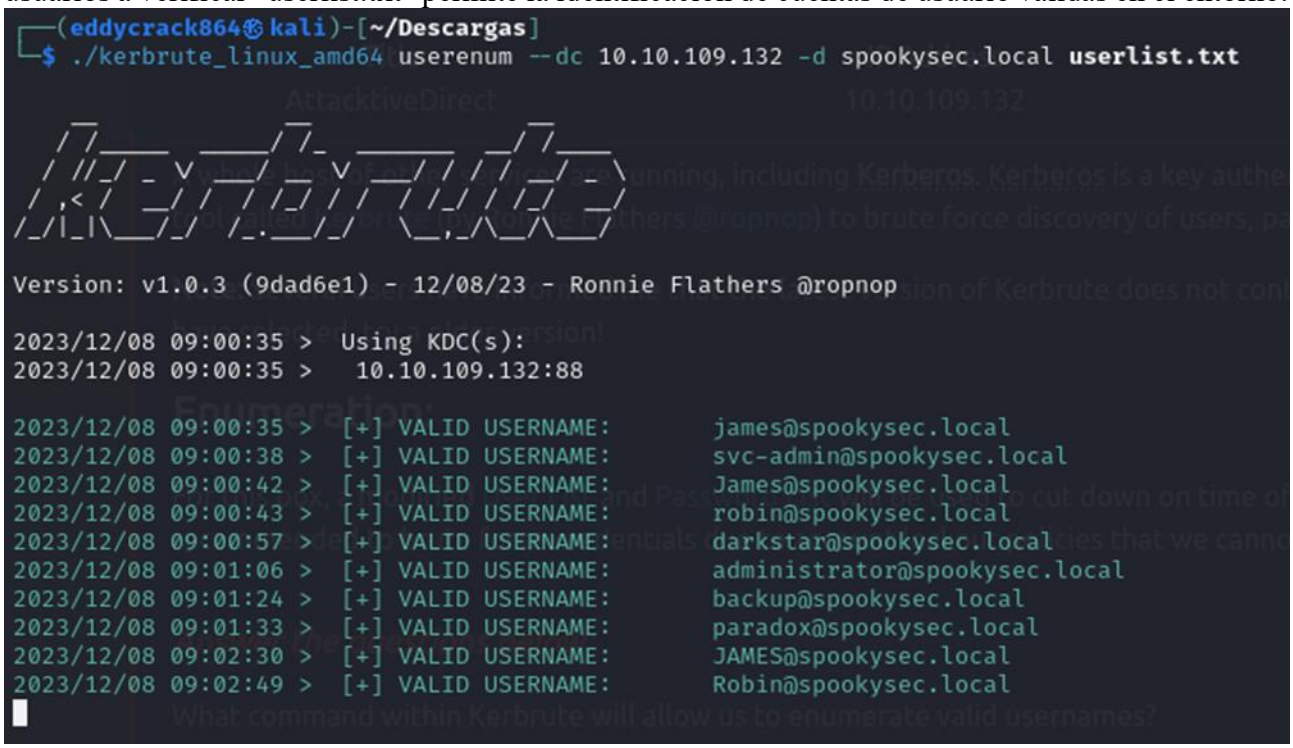

9. Utilizando la herramienta enum4linux, la salida generada proporciona un listado detallado que incluye varios nombres de usuario (usernames) y grupos de usuarios (user groups).



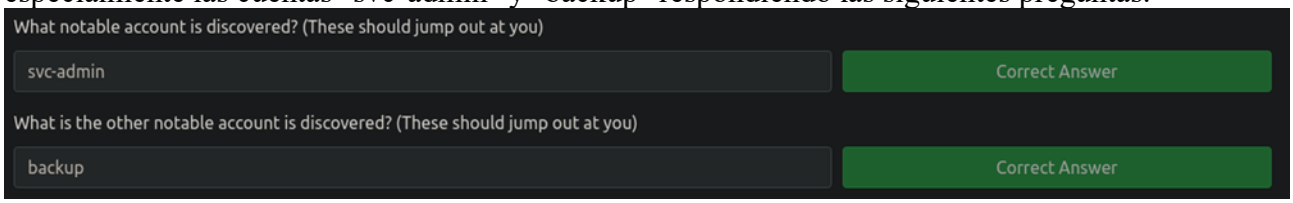
10. Al emplear la aplicación Kerbrute y ejecutarla con el parámetro "-h", se despliega una descripción detallada de su funcionalidad, así como una lista de los comandos disponibles junto con sus respectivas descripciones.


11. Entre los comandos disponibles, destaca "userenum", el cual habilita la capacidad de listar nombres de usuario válidos. De este modo respondemos la primera pregunta de la sección.


12. Posteriormente, se procede a la ejecución de Kerbrute utilizando el ejecutable "./kerbrute_linux_amd64". Con el objetivo de descubrir cuentas de usuario, se emplea el siguiente comando: “userenum --dc <***ip objetivo***> -d spookysec.local userlist.txt”. La especificación del controlador de dominio "--dc <***ip objetivo***>", el dominio objetivo "-d spookysec.local", y la lista de usuarios a verificar "userlist.txt" permite la identificación de cuentas de usuario válidas en el entorno.



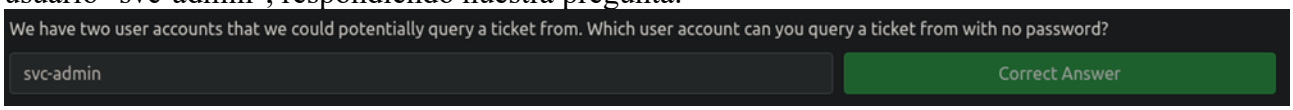
13. Se identifican cuentas de interés significativo en los resultados obtenidos. Entre ellas, se destacan especialmente las cuentas "svc-admin" y "backup" respondiendo las siguientes preguntas.



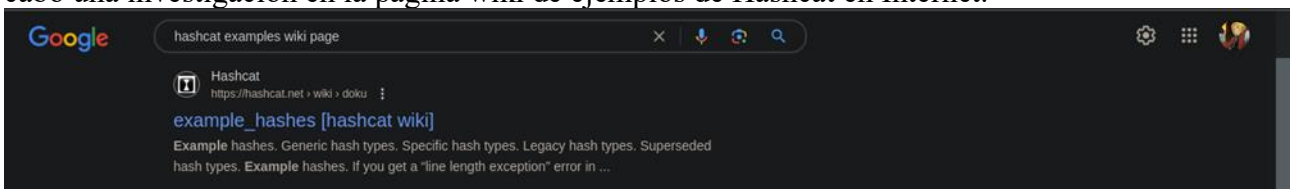

14. Se procede a la navegación hacia el directorio de instalación de Impacket mediante el comando "cd".


15. Habiendo cambiado previamente al directorio "examples" de Impacket, se procede a emplear el script "GetNPUsers.py" mediante el comando: “python3 GetNPUsers.py -no-pass -dc-ip 10.10.109 spookysec.local/svc-admin”. Los resultados revelan que el usuario "svc-admin" cuenta con la capacidad de solicitar un ticket Kerberos sin la necesidad de proporcionar una contraseña. Como consecuencia, se obtiene un hash de Kerberos

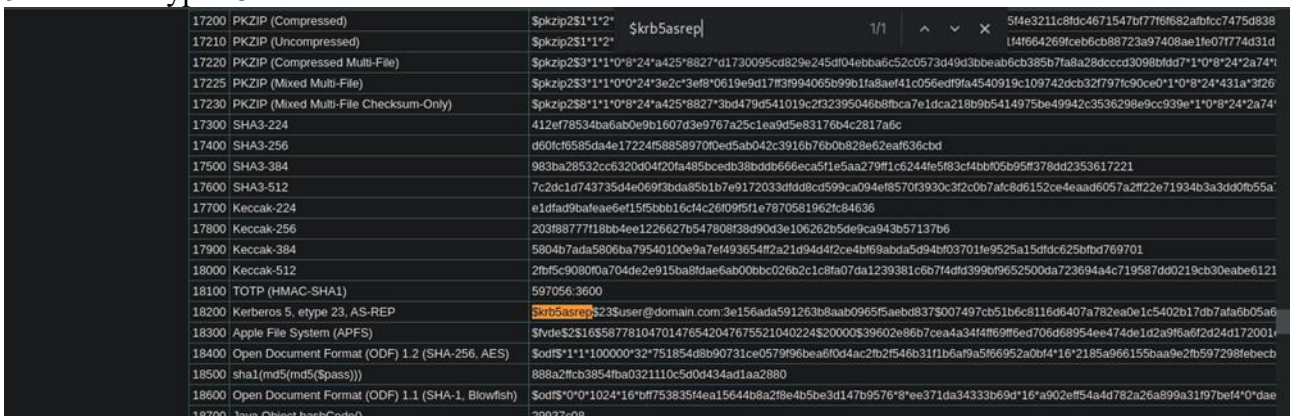

16. El análisis del Ticket-Granting Ticket (TGT) de Kerberos revela la presencia del nombre de usuario "svc-admin", respondiendo nuestra pregunta.



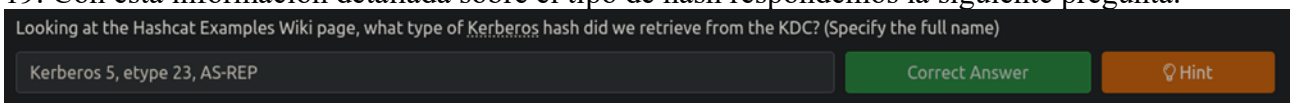

17. Con el propósito de responder a la siguiente pregunta acerca del tipo de hash obtenido, se lleva a cabo una investigación en la página wiki de ejemplos de Hashcat en Internet.



18. La investigación revela que el hash corresponde al modo número 18200 en Hashcat, identificado por la presencia de la cadena inicial ($krb5asrep). Este modo específico es conocido como "Kerberos 5 AS-REP etype 23".

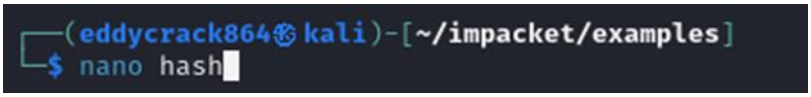



19. Con esta información detallada sobre el tipo de hash respondemos la siguiente pregunta.

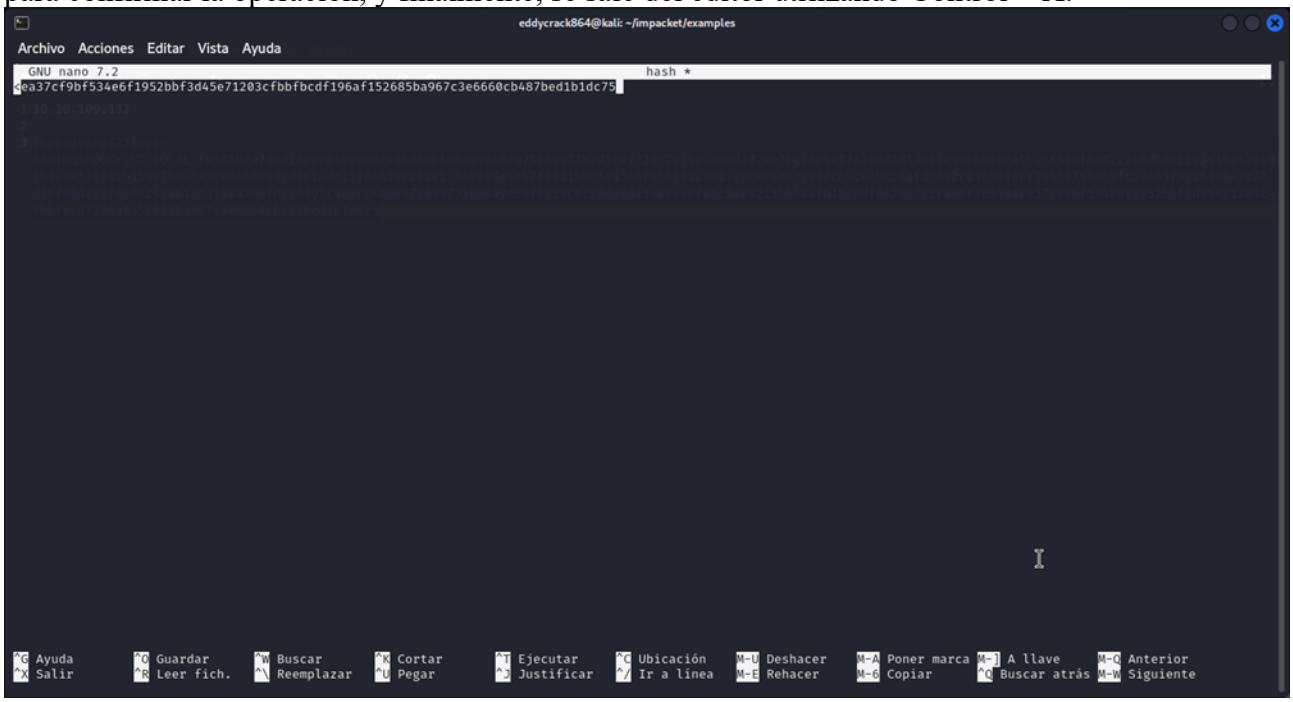



20. Con la información obtenida sobre el modo del hash respondemos la siguiente pregunta.

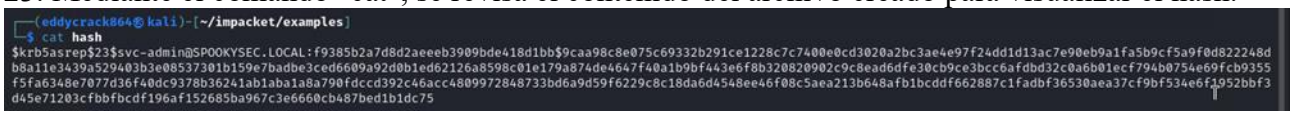

21. Se procede a copiar el hash obtenido en la fase anterior. Posteriormente, se crea un archivo denominado "hash" utilizando el editor de texto nano mediante el comando correspondiente.



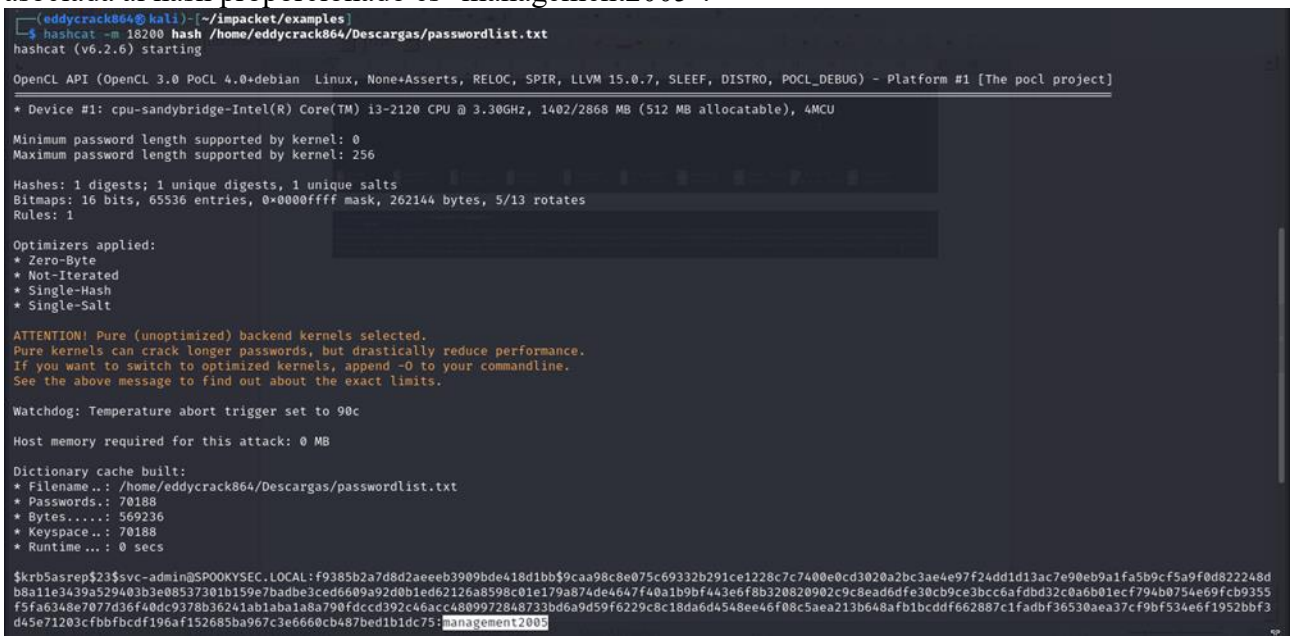

22. Se procede a pegar el hash previamente obtenido dentro del editor de texto. Posteriormente, se guarda el contenido del archivo utilizando la combinación de teclas Control + O, se presiona Enter para confirmar la operación, y finalmente, se sale del editor utilizando Control + X.



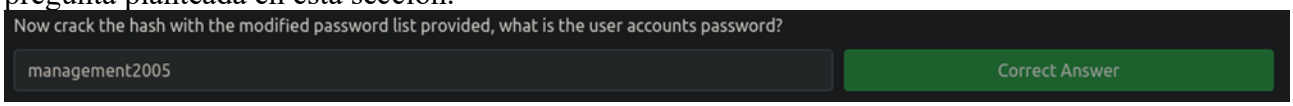
23. Mediante el comando "cat", se revisa el contenido del archivo creado para visualizar el hash.



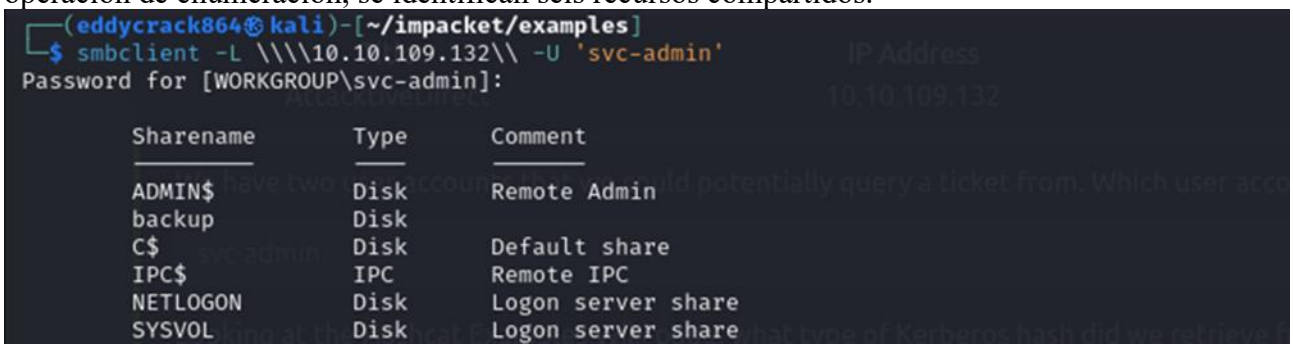

24. El proceso de descifrado se lleva a cabo mediante la herramienta hashcat utilizando el comando: “hashcat -m 18200 hash <ruta al archivo passwordlist.txt>”. Los resultados indican que la contraseña asociada al hash proporcionado es "management2005".



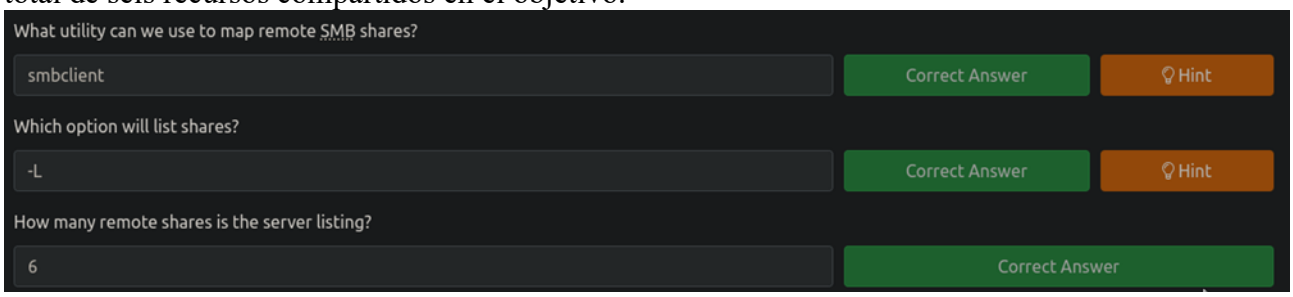

25. Con la contraseña identificada como "management2005", se encuentra la respuesta a la última pregunta planteada en esta sección.



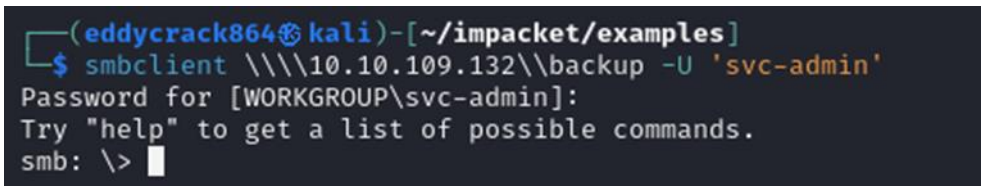

26. A través del programa smbclient, se realiza la enumeración de los recursos compartidos mediante el uso del parámetro -L seguido de la dirección IP del objetivo. Además, se emplea el parámetro -U para suministrar el nombre de usuario, que en este caso es "svc-admin". Como consecuencia de esta operación de enumeración, se identifican seis recursos compartidos.



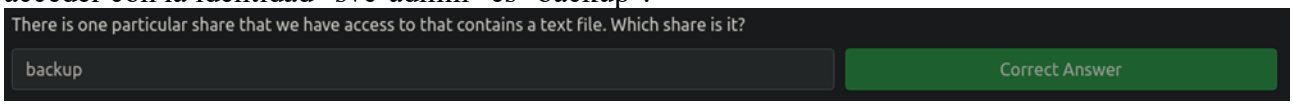
27. Se procede a responder las preguntas correspondientes. La aplicación utilizada para esta tarea fue smbclient, el parámetro empleado fue -L para listar los recursos compartidos, y se identificaron un total de seis recursos compartidos en el objetivo.



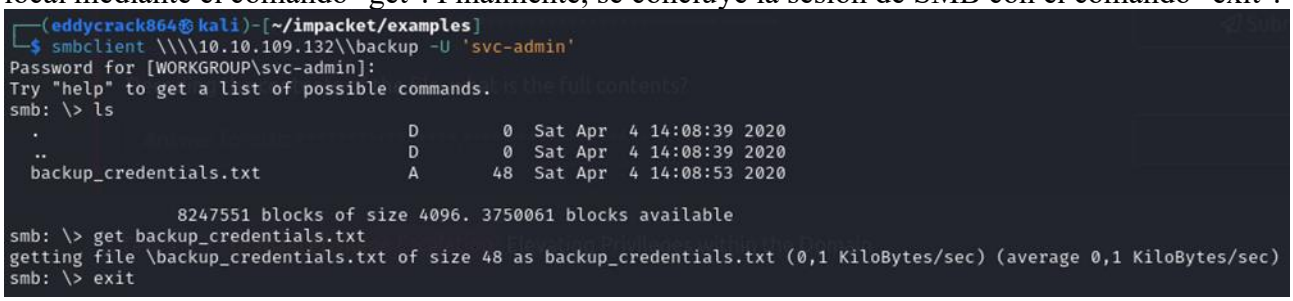

28. Mediante el programa smbclient, se realiza una conexión específica a un recurso compartido determinado. Se fija la IP del objetivo y se añade el recurso compartido deseado, en este caso, "backup". Se utiliza el parámetro -U para especificar el nombre de usuario, que en este contexto es "svc-admin". Posteriormente, el sistema solicitará una contraseña, la cual se suministra utilizando la que fue obtenida al descifrar el hash con hashcat.



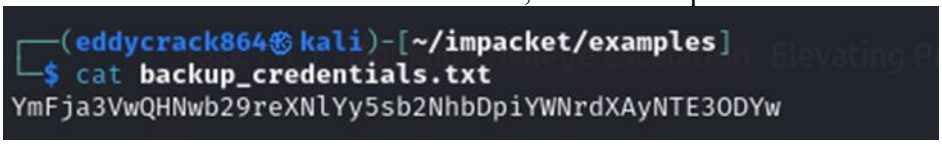

29. Este proceso nos proporciona la respuesta a la pregunta planteada: el recurso al cual se puede acceder con la identidad "svc-admin" es "backup".



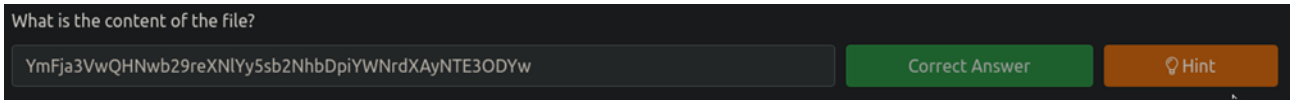

30. Después de haber ingresado al recurso compartido "backups", se ejecuta el comando "ls" para listar el contenido, revelando la presencia de un archivo de texto. Este archivo se transfiere al sistema local mediante el comando "get". Finalmente, se concluye la sesión de SMB con el comando "exit".




31. Inmediatamente después, se procede a visualizar el contenido del archivo de texto transferido utilizando el comando "cat". Al examinar el contenido, se observa que el texto está cifrado.

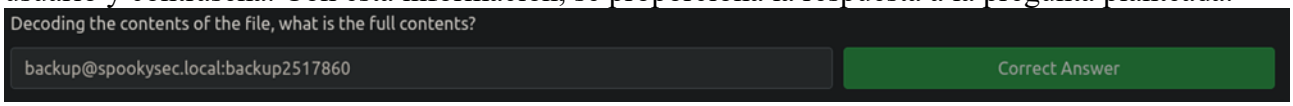



32. La respuesta a la pregunta planteada se proporciona ingresando el texto encontrado en el archivo cifrado.

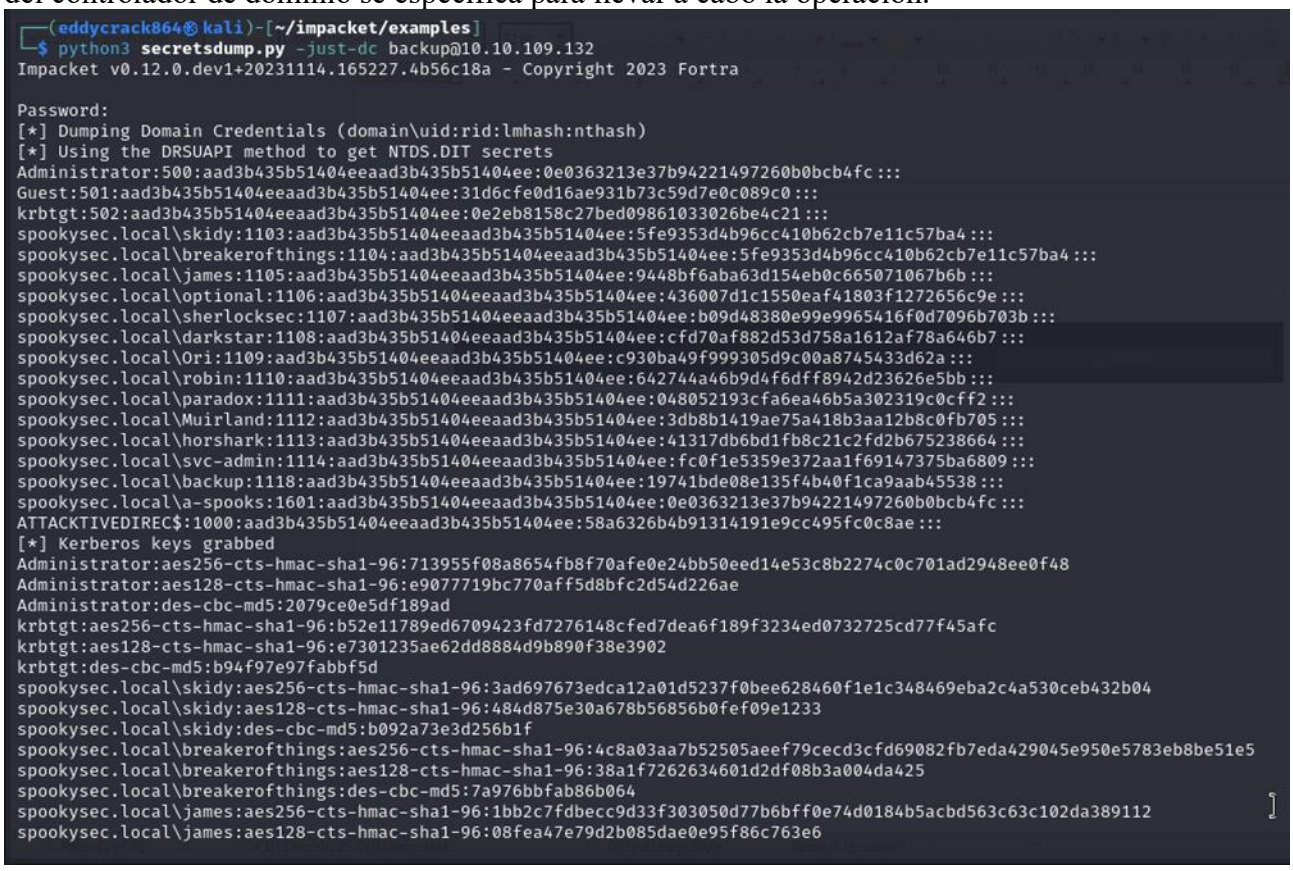


33. A continuación, se procede a desencriptar el texto identificado. Se utiliza el comando "echo" junto con el texto cifrado. Además, se destaca que el texto estaba encriptado en base64, por lo que se aplica el comando "base64 -d" para llevar a cabo la desencriptación.

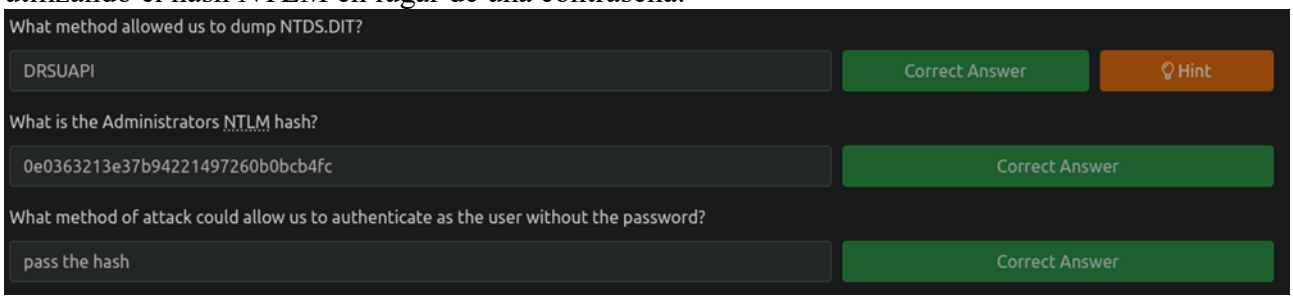

34. Como consecuencia del proceso de desencriptación, se obtiene lo que parece ser un conjunto de usuario y contraseña. Con esta información, se proporciona la respuesta a la pregunta planteada.



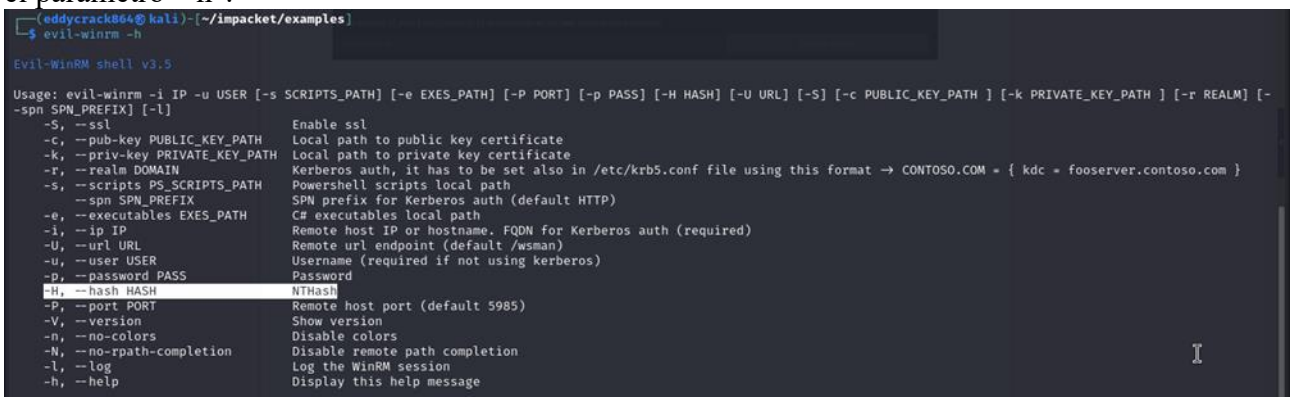

35. Con las nuevas credenciales de cuenta de usuario en nuestro poder, podemos emplear la herramienta "secretsdump.py" de Impacket. Esta utilidad nos posibilita recuperar todos los hashes de contraseña que la cuenta de usuario posea sincronizados. Mediante el uso del parámetro "-just-dc", indicamos que deseamos realizar el volcado de credenciales desde el controlador de dominio, utilizando el nombre de usuario "backup" para autenticarnos en dicho controlador. La dirección IP del controlador de dominio se especifica para llevar a cabo la operación.



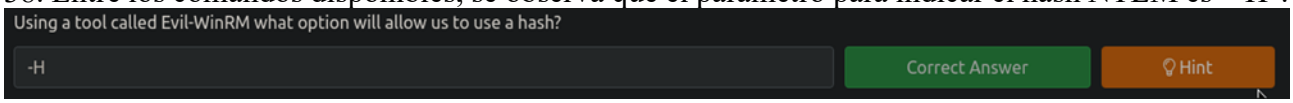
36. La salida del comando anterior revela información valiosa. Se identifica que el método utilizado para obtener el archivo de base de datos principal de Active Directory fue DRSUAPI. Además, se obtiene el hash NTLM del administrador, para esto se empleó la técnica conocida como "pass the hash". Esta técnica de hacking permite a un atacante autenticarse en un servidor o servicio remoto utilizando el hash NTLM en lugar de una contraseña.



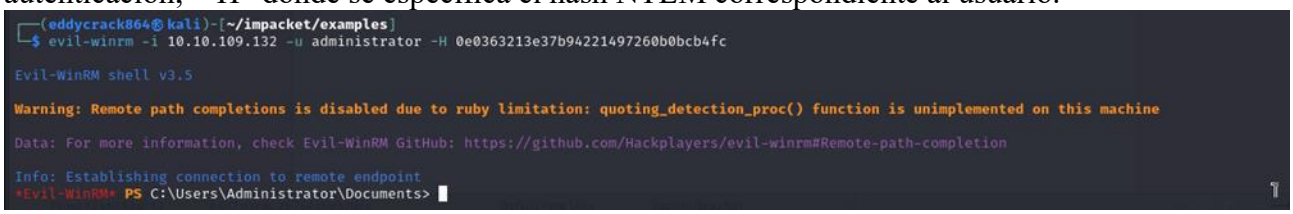

37. Con el hash NTLM del administrador en nuestra posesión, procederemos a utilizar la herramienta "evil-winrm". Como primer paso, exploraremos detalladamente los comandos disponibles utilizando el parámetro "-h".



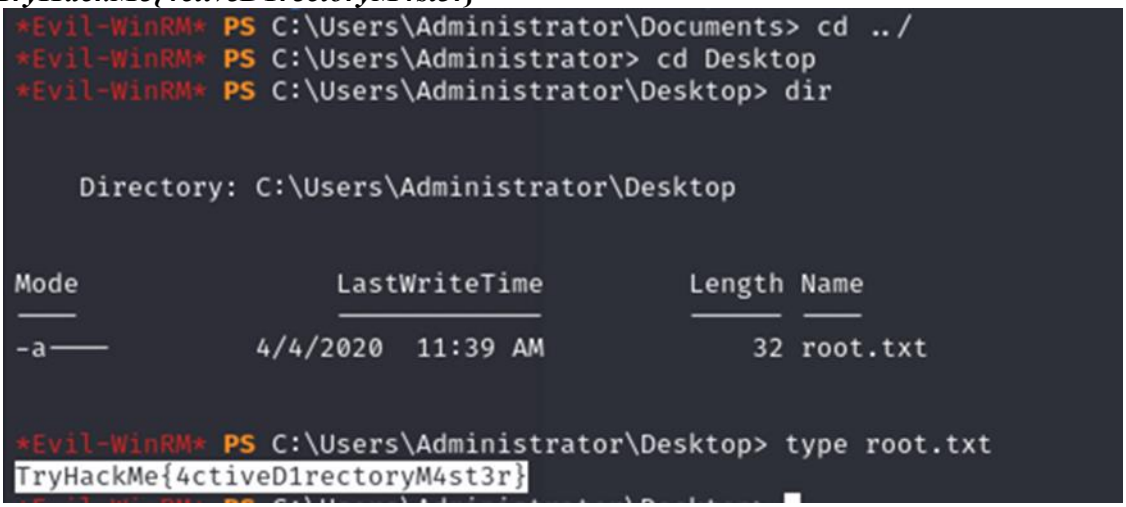

38. Entre los comandos disponibles, se observa que el parámetro para indicar el hash NTLM es "-H".



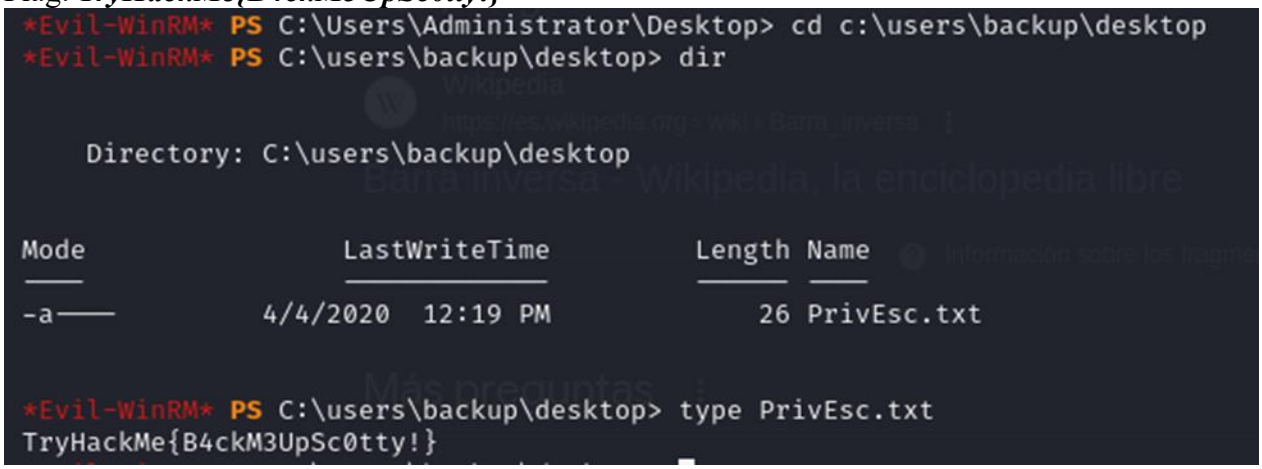

39. Finalmente, para obtener acceso como administrador en la máquina objetivo, se emplea la herramienta "evil-winrm". Usando los parámetros: “-i” para especificar la dirección IP del sistema de destino al que se intenta acceder; “-u” para indicar el nombre de usuario que se utilizará para la autenticación; “-H” donde se especifica el hash NTLM correspondiente al usuario.



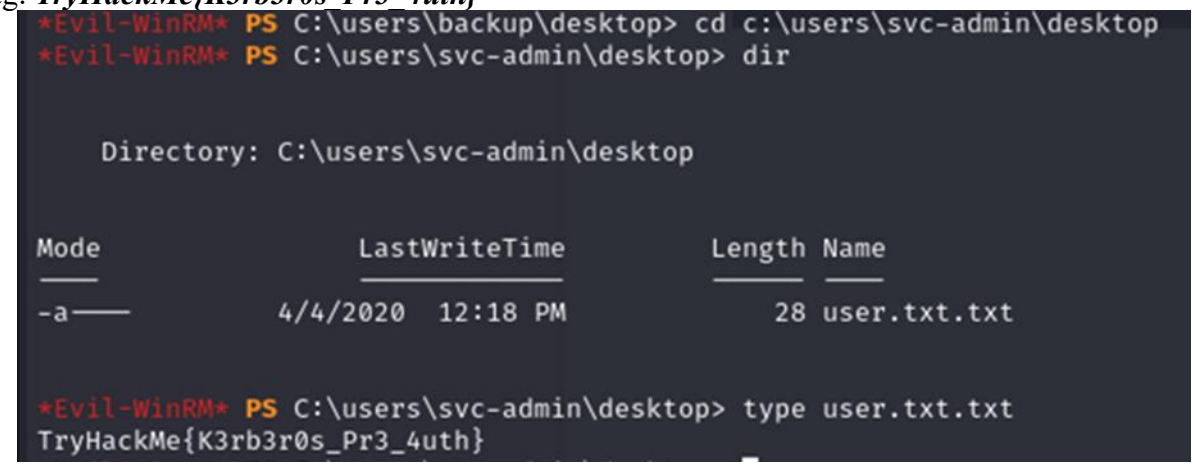
40. Una vez que hemos obtenido privilegios de administrador, nos dirigimos al directorio principal y posteriormente al escritorio. Al listar el contenido, identificamos la flag del administrador, la cual visualizamos utilizando el comando "type".
Flag: ***TryHackMe{4ctiveD1rectoryM4st3r}***




41. Procedemos a navegar hacia el escritorio de la carpeta del usuario "backup". Luego, al listar el contenido, identificamos la bandera correspondiente a este usuario. Finalmente, visualizamos la flag utilizando el comando "type".
Flag: ***TryHackMe{B4ckM3UpSc0tty!}***




42. Siguiendo los pasos anteriores, repetimos el proceso para el último usuario y obtenemos la última flag.
Flag: ***TryHackMe{K3rb3r0s_Pr3_4uth}***



43. Al subir correctamente las tres flags a TryHackMe, la plataforma mostrará un mensaje indicando que se ha completado exitosamente esta instancia en su totalidad.